SECURITY-INTEGRATED NUCLEAR PROCESS ACCESS CONTROL

by

Helen Cheung

M.A.Sc., Ryerson University, 2008

A dissertation
presented to Ryerson University

in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in the Program of
Electrical and Computer Engineering

Toronto, Ontario, Canada, 2015

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A DISSERTATION

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

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

I further authorize Ryerson University to reproduce this dissertation 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 dissertation may be made electronically available to the public.

ABSTRACT

SECURITY-INTEGRATED NUCLEAR PROCESS ACCESS CONTROL

Doctor of Philosophy in the Program of Electrical and Computer Engineering 2015
Helen Cheung
Ryerson University

The intent of this thesis research is to develop a concept/methodology to advance technologies for controls of network accesses to the industrial processes of safety/operation-critical and to contribute to the nuclear process control modernization with improved nuclear operation security and consequently increased nuclear safety and cost savings. This thesis is focused on the security-integrated nuclear process network-access controls for modernizing nuclear operations.

This thesis research commenced with assessments of the current states of nuclear processes in the live nuclear generating stations and identified improvements on the current nuclear practices and security concerns of using the network-based intelligent features of modern process controls for nuclear operations.

This thesis has created SNP - *Security-integrated Nuclear Process*, OBAC - *Operation Based Access Control*, NOAA - *Nuclear Operation Access Authentication*, CSM - *Cost Savings Model*, etc. as the fundamental developments for contributions to the nuclear operations modernization with improved operation security and subsequently increased nuclear safety and cost savings in daily nuclear operations.

The *SNP* is to transform the current nuclear practices into network-based nuclear operations that include equipment performance monitoring, nuclear data processing, nuclear equipment control and maintenance. The *OBAC* is an operation-based access control built upon the core nuclear operations and facilitates the security and quality controls of network accesses to nuclear operations. The *NOAA* is to provide user security authentication for access to nuclear operation network, which is composed of *APP* for access pre-access authentication and *AQP* for access qualification authentication. The *CSM* is designed for evaluations of the *SNP* and associated designs in terms of cost savings opportunity.

The feasibility and practicality of these new designs are illustrated in the thesis, by analytical and numerical methods. The significance of these new designs is tremendous, resulting in potentially significant cost savings in daily nuclear generation, in addition with increased nuclear operation network security and subsequently the nuclear safety that is priceless.

ACKNOWLEDGEMENTS

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

I would like to express special thanks to my father Dr. Richard Cheung, my mother Mrs. Linda Cheung, and my brother Mr. Herman Cheung for their continuous encouragement and support.

TABLE OF CONTENTS

Part 3: NUCLEAR PRACTICES TRANSFORMATION AND SNP DATA BASE

LIST OF TABLES page

LIST OF FIGURES page

LIST OF ILLUSTRATIONS page

Chapter 1

INTRODUCTION

The intent of this thesis research has two aspects: *technical* and *practical*. In the general technical aspect, the intent is to develop a concept/methodology to advance the technology used for the control of network accesses to the industrial processes of safety-critical, infrastructure-critical, economic-critical, operation-critical, availability-critical, etc. In the specific practical aspect, the intent of this thesis research is to create a new nuclear operation network base and a new network access control for contributions to the nuclear process control modernization with improved nuclear operation security and consequently, with increased nuclear safety and operation cost savings.

This thesis research started with assessments of the current state of the nuclear process in the live nuclear generating stations and has identified the weakness in the current nuclear process practices and the security concerns for nuclear operation modernization with the use of the network-based intelligent (smart) features of modern control process equipment. There has not been absence of instances that many conceptual designs had failed and can never be implementable successfully with significant impacts on economic and technology advances, because they do not consolidate with practical details. Therefore, this thesis emphasizes on details, augmented with practical experiences accumulated from working in the industrial sites, in order to enhance the practicality of the conceptual design/methodology developed in the early stage of this thesis research.

This thesis research develops a new concept and practical innovative methodology for improved nuclear practices, supported with practically feasible and secure network access controls, in order to break a serious gridlock largely due to nuclear safety concerns in the progression of nuclear process modernization. This thesis research drives to a ground-breaking development, termed as the *Security-integrated Nuclear Process* ***SNP*** for advancement of nuclear operation modernization.

This thesis presents two new designs, termed as the *Operation-Based Access Control* ***OBAC***, and the *Nuclear Operation Access Authentication* ***NOAA***. The goal of these designs is to contribute to the network-based nuclear operations, satisfying the most essential requirement of ensuring the cyber-secure nuclear operations. The feasibility and practicality of these new initiations (*SNP*, *OBAC*, and *NOAA*) have been thoughtfully evaluated. The significance of new initiations is tremendous, resulting in potentially huge cost savings in addition to increased operation network security and subsequently nuclear safety that is priceless.

This thesis research is to carry out the development of a fundamental transformation of current nuclear practices, being first-of-the-kind creation of total network-based nuclear operations. Since after exhaustive research, there are no particularly suitable methods available for the evaluation of this first-of-the-kind transformation of nuclear practices, this thesis research creates a cost model termed ***NCM***, the *Nuclear Cost Model* for the current nuclear practices and establishes it as a reference base for the *SNP* design performance analysis, and creates another model termed ***CSM***, the *Cost Saving Models* for the analytical evaluation of the new *SNP* designs in terms of cost savings opportunity.

This thesis presents:

Chapter 1: This chapter presents an introduction of this thesis research.

Chapter 2: This chapter first presents a conceptual development and methodology for the control of accesses to a safety-critical process with network-based operations and second, this chapter presents the new design of ***OBAC***, as the first step in this thesis research for finding a new security-integrated access control to the new formation of the network-based nuclear process.

Chapter 3: This chapter presents a new authentication design for the network-based nuclear process access controls termed as ***NOAA***, the *Nuclear Operation Access Authentication*, consisting of two new protocols ***APP*** **-** the *Authentication Pre-access Protocol* and ***AQP*** **-** the *Authentication Qualification Protocol*.

Chapter 4: This chapter first presents the *SNP* transformation of the current nuclear practices on equipment performance monitoring, nuclear data processing, and equipment control and maintenance. Second, this chapter presents a case study for illustration of the *SNP* transformation of nuclear practices. Third, this chapter presents the creation of the nuclear network data base for the support of the *SNP* transformation.

Chapter 5: This chapter presents the performance analysis of the *SNP* designs developed in this thesis. This chapter creates the *nuclear cost models* ***NCM*** for a measure of the cost aspect of the current nuclear practices to establish a reference base for the *SNP* designs analysis. This chapter also creates the nuclear *cost saving models* ***CSM*** for an analytical evaluation of the new *SNP* designs in terms of cost savings opportunity. This chapter also presents the numerical analysis of the performance of the *SNP* designs and the numerical assessment of the network pre-access authentication process.

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 nuclear power generation realities and prevailing nuclear practices issues, and identifies targets of this thesis research and development for promotion of nuclear process modernization with increased operation security, nuclear safety, radiation free working environment, and significant cost savings in the daily nuclear operations.

Section 1.2: This section introduces the basic nuclear power electricity generation, a new nuclear process network base, and a new nuclear process access.

Section 1.3: This section presents this thesis research findings on the assessment of the current state of smart industrial control systems, information technology systems, and nuclear process control systems, which is to lay out the background to establish benchmarks for this thesis' development of a new *Security-integrated Nuclear Process* (*SNP*). This section also presents this thesis research findings on the assessment of state-of-the-art network access controls, which is to lay out the background to establish benchmarks for this thesis to develop a new access control.

Section 1.4: This section introduces a new design developed in this thesis research for the controls of access to the nuclear process operations, termed as the *Operation-Based Access Control* (OBAC).

Section 1.5: This section presents this thesis research findings of the current state of current states of authentication and protocols for network access, access security concerns and resolutions using authentication.

Section 1.6: This section introduces a new design developed in this thesis research for nuclear process access authentication, termed the *Nuclear Operation Access Authentication* (NOAA).

Section 1.7: This section presents an overview of the *SNP* designs analysis.

Section 1.8: This section lists the acronyms and abbreviations used in this thesis.

1.1 Thesis Research Targets

This section presents a review of the current nuclear power generation realities and prevailing nuclear practices issues, and identifies *targets* of this thesis research and development for promotion of nuclear process modernization with increased operation security, and subsequently enhanced nuclear safety and radiation-free working environment, and significant cost savings in the daily nuclear operations.

1.1.1 *Security Concern for Nuclear Process Modernization*

With years of on-the-nuclear-site working experiences in weighty positions of nuclear engineering management, system design and field supervision, it has reached a deduction that the nuclear process *security concern* is the major roadblock in the progression of nuclear process operations modernization.

Intelligent (smart) process control equipment of various kinds from simple devices to complex systems, such as from standalone smart valve positioners to state-of-the-art ≈1,000MW generator automatic control systems are available for modernization of nuclear process operations, and many of them are already physically installed in the nuclear generating stations. These smart process control equipment have networking capability with intelligent features for central data processing, devices/equipment/ systems operations optimizing and coordinating, predictive maintenance scheduling, etc.

Unfortunately, the nonobvious reality learnt from the on-nuclear-site experiences is that most of intelligent features in these equipment are deliberately disabled or their capabilities are severely limited intentionally due to security concerns in the nuclear operating environment. Security concerns, if ignored, will have extremely serious consequences to public and employees' health and safety. Therefore millions dollars of yearly potential savings from utilizing these intelligent equipment capabilities and associated benefits cannot be realized.

Target 1: Develop a novel concept and implementable method for effectively eliminating the security concerns for access to nuclear process in the nuclear operations modernization.

1.1.2 *Obsolescence of Nuclear Units and Obscuration of Nuclear Refurbishment*

Ontario nuclear power generating stations that were built about thirty or forty years ago have become obsolete, and they are now due for refurbishment in order to continue their safe operations for another life cycle of thirty years. The refurbishment of a nuclear generating station is very expensive and to put it in a proper perspective, the first Ontario nuclear refurbishment project for 2 units of an eight-unit nuclear plant has cost a huge amount of money, multiple billions of dollars. With this first-of-the-kind worldwide massive scale of expenses in the nuclear unit refurbishment, it is certainly expected the refurbished nuclear units to be modernized with tremendous benefits and the investment payback period as short as possible.

However, the nonobvious reality as experienced on the nuclear site, with respect to the refurbishment of nuclear process controls, the obsolete devices/equipment/systems were replaced, as a first priority, with ones of the same form, fit, and function. The replacement with newer devices/equipment/systems having intelligent (smart) features with networking capability is not necessary a preference, unless no equivalence to the obsolete ones can be found. Should it be in such situation with exhausted searches resulting in no equivalent replacement be found, then replacement with modern intelligent equipment are to be considered. Even though the modern smart equipment are adopted, their intelligent features with networking capability were mostly either disabled or substantially limited due to security concerns and therefore, the potential benefits are severely reduced. Although the extremely expensive refurbishment and severely limited replacement practices were the recent past reality, the situation will stay unchanged in the foreseeable future as the existing nuclear units are aging and safety concerns are unsolved for full use of network-based smart features.

Target 2: Develop a new effective methodology of secure deployment of modern smart equipment for nuclear process upgrades particularly in the multibillions-dollars refurbishment projects, aiming for increased operation access security.

1.1.3 *Inefficiency and Expensive of Existing Nuclear Operation Practices*

Safety is paramount in all nuclear power plants, as senior managements in nuclear industry always emphasize “no safety ⟹ no nuclear business”. Safety in the nuclear plant is non-negotiable and must be well understood and implemented.

Ontario nuclear power generating stations were built about thirty or forty years ago with the best technologies of that time or earlier. In general, the nuclear process controls were designed and implemented in traditional discrete and analog forms and with redundancy for satisfying requirements of safety and operation reliability. Of this traditional setting, the existing nuclear process controls are sluggish, bulky, maintenance intensive, etc. compared to today’s process control technology.

With years of research and working experiences on the nuclear site, it has come to a unique conclusion that now it is time to research, develop, and implement a revolutionary-type of changes for the nuclear generating practices, under the non-negotiable condition of satisfying the supreme requirement of nuclear *Safety*. The key objective of this thesis research is to significantly reduce the current human-intensive maintenance and operation practices in the existing nuclear plants, with the use of today's available intelligent (smart) technologies.

The current human-intensive nuclear practice has serious consequences, of which the major one is the costs, both labour cost and operational cost. There are three aspects affecting the nuclear labour cost: the nuclear workers in general have a higher-than-average salary due to the nature of nuclear radioactive-related work; the nuclear workers require intensive trainings plus regularly repetitive trainings because of radiation safety requirements; the nuclear workers have a tightly-regulated limit on radiation exposure. The major operational cost is the cost of outage, with the nuclear unit being shut down for extensive maintenance.

With respect to the nuclear process controls, not considering others outside of this thesis focus such as radiation dose controls, the traditional discrete and analog devices/equipment/systems require intensive human care for monitoring, operation, and maintenance. In addition, these traditional setups generally were not equipped with online diagnosis and online adjustments, and their essential maintenance must wait until the scheduled outage when the nuclear unit is planned to be completely shut down, or the forced outage when there is a considerable event preventing the nuclear operation. The outage is very costly, often to be a million dollars a day per nuclear unit for the loss of revenue and overtime payments.

Target 3: *Develop a revolutionary-type of changes for the nuclear generating practices to significantly reduce the current human-intensive maintenance and operation practices in the existing nuclear plants, with the use of today's available intelligent (smart) technologies.*

Target 4: *Develop a practical innovative access control to new smart nuclear processers with networking capability for online diagnosis and online adjustments, in order to shorten the outage requirements that directly render to tremendous savings.*

1.1.4 *Old-fashioned Nuclear Practices*

At the time of this thesis research, many hundreds of devices in one nuclear station are obsolete, in addition with their original manufacturers either out of business or no longer supporting the production of these devices. These devices are near or at the end of their life expectation and their performance is deteriorating quickly due to aging. Because the current practices these devices are to be replaced with ones of the same form, fit, and functions, as the priority, the replacements have become difficult and expensive. Even such devices of the equivalent form, fit and function can be found, these devices are in general inefficient from the standard of today's technology.

Smart process control equipment of various levels from simple standalone smart valve positioners to advanced generator automatic control systems are commercially available and in fact, many have already been installed in the nuclear generating stations. These smart equipment has networking capability with intelligent features for central data processing, equipment operations optimizing and coordinating, predictive maintenance scheduling, etc. However most of intelligent features in these equipment are deliberately disabled or their capabilities are severely limited intentionally due to security concerns in nuclear operating environment and therefore, millions dollars of potential savings and associated benefits are lost.

Target 5: Develop an innovative security-integrated system for nuclear process controls that facilities the functioning of state-of-the-art intelligent features of modern process controlling equipment with networking capability for central data processing, operations optimizing and coordinating, and predictive maintenance scheduling.

1.1.5 *Challenge in Nuclear Process Modernization*

The nuclear electricity generation is not new at all. However, it is considerably challenging to be able to dig out any tangible data including any significant nuclear process deficiencies, issues, events and their causes in the real nuclear generating facilities, because the nuclear industry is substantially "*closed*" that is virtually isolated from the external world due to their conservative ways of handling public safety concerns, particularly with respect to radiation exposures and nuclear events/accidents, in additional to risks inherent in the operating nuclear systems. With years of research and on-the-nuclear-site working experiences, it has learnt the culture and daily practices of the nuclear industry, of which the nuclear workers are repeatedly trained to be absolutely careful for handling anything with relation to nuclear matters, from design, installation, commissioning, operation, monitoring and maintenance, to even out-of-site chats that nuclear workers will not casually release any tangible information or touching topics of their own-site nuclear events excepting for those already announced publicly.

Nevertheless information about the general aspects of the nuclear industry can be found in the literature. An attempt to gather information for carrying out any fundamental ground-breaking research in the nuclear industry, with significant improvement on nuclear practices and significant potential economic benefits, would be a different story. Researchers, particularly academic researchers if without nuclear working experiences or with no connections to nuclear industry, are hardly able to obtain any essential on-site data about the real deficiencies in nuclear practices or events happened in the nuclear plant.

Target 6: Develop a new security-integrated nuclear practice that can significantly benefit the nuclear industry as well as can be accepted by this "closed" industry.

1.2 Introduction of Nuclear Generation and Scope of Nuclear Process Access Design

This section introduces the basic nuclear power electricity generation, new nuclear process network base, and scope of new nuclear process access.

1.2.1 *Introduction of CANDU Nuclear Generation*

a) *CANDU Reactor*: CANDU (CANada Deuterium Uranium) reactor is used in Ontario nuclear power stations for electricity generation. The CANDU reactor is a Canadian invented pressurized heavy water (deuterium-oxide) reactor. The fuel used in CANDU is natural uranium that consists of mainly ^{238}U, and a small amount of fissile ^{235}U that generates nuclear power. The CANDU reactor is operated to sustain a steady rate of fission that the neutrons released by ^{235}U fission cause an equal number of fissions in other ^{235}U atoms, achieving an equilibrium condition known as criticality. However, the neutrons released by fission are fairly energetic and are not readily captured by other sparse fissile ^{235}U. The neutrons must have their energy moderated to sustain the chain reaction of fission. Light water is a too good moderator of which the light hydrogen atoms can absorb a lot of energy in a single collision. Since the light hydrogen can absorb neutrons effectively, this however leaves too few neutrons to react with the other sparse fissile ^{235}U contained in natural uranium, and therefore this prevents the condition of criticality for sustained chain reaction of fission for electricity generation. Heavy water has advantage over light water in terms of non-absorption of neutrons, as the heavy hydrogen (deuterium) 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 and therefore allow the use of unenriched natural uranium as fuel in the CANDU reactor.

b) *Ontario CANDU Nuclear Generating Unit*: In a typical Ontario nuclear generating unit, the fission reaction in the reactor core heats the pressurized heavy water in the calandria and 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 (that is the calandria-moderator division, one of the four divisions created in this thesis). The pressurized heavy water is circulated between reactor fuel channels and steam generators (the primary heat transport division). The steam generator transfers the heat to the light water in the secondary cooling loop (the boiler-steam division). The stream from the boiler powers a stream turbine that run an electricity generator (the turbine-generator division). 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 (the condenser and light water division).

1.2.2 *Creation of Nuclear Process Real-Time Operation Network Base*

In the current state due to pending nuclear safety concerns, *first*, millions dollars of potential savings every year from utilizing modern intelligent equipment's networking and computing capabilities and associated benefits cannot be realized; *second*, in the expensive nuclear refurbishment the replacement of obsolete equipment with new equipment having smart networking features is not necessary a preference unless no equivalence to the obsolete ones can be found and the equivalent equipment are in general of older technology; *third*, the continued use of equipment of old technology leads to sluggish performance, bulky and inefficiency, non/limited on-line diagnosis, intensive maintenance, etc. This results in labour intensive and costly in operating and maintaining equipment of older technologies. This thesis research is to contribute to the secure use of equipment of today's technology with networking capability for on-line diagnosis, operations coordinating, predictive maintenance scheduling, etc.

In order to fully utilize the intelligent features of smart equipment for the real-time nuclear operations, a secure computer network must be established. The basic requirement for a secure network is the control of its access that is the focus of this thesis research. Firstly the network for the safe nuclear process operations must be configured, starting from the network access point of view.

This thesis design divides the access to the nuclear process network into four (4) *SNP* access levels. Each access level is defined according to a typical physical CANDU nuclear process operations in the real on-line Ontario nuclear power plants producing hundreds of MW electricity. The four levels form the nuclear real-time operation network base.

Division-level nuclear process: $SNP\_\boldsymbol{D_n}$
System-level nuclear process: $SNP\_D_n\_\boldsymbol{S_n}$
Equipment-level nuclear process: $SNP\_D_n\_S_n\_\boldsymbol{E_n}$
Function-level nuclear process: $SNP\_D_n\_S_n\_E_n\_\boldsymbol{F_n}$

This thesis design divides the nuclear process of a typical CANDU nuclear unit in the Ontario NGS into five (5) divisions:

Calandria-moderator division: $SNP\_\boldsymbol{D_1}$
Primary heat transport-heavy water division: $SNP\_\boldsymbol{D_2}$
Boiler-steam division: $SNP\_\boldsymbol{D_3}$
Turbine-generator division: $SNP\_\boldsymbol{D_4}$
Condenser-light water division: $SNP\_\boldsymbol{D_5}$

1.2.3 *Cooling of Nuclear Fuel – the prime importance of nuclear operations*

This thesis research develops the five *SNP* divisions first, to facilitate the fulfillment of the prime importance of the operating nuclear unit that is cooling of the fuel whether or not the unit generates electricity and second, to enhance the safe and uninterrupted production of electricity. Safe electricity generation is the basic justification for the existence of a nuclear power plant.

This thesis develops the *SNP* access to expedite the overall control of the nuclear unit and to achieve a balance between the rate of heat being produced by the fuel and the rate of heat being removed from the fuel. The following summarizes the basic heat controlling process for a typical CANDU nuclear unit and its relationship with the new *SNP* divisional access proposed in this thesis research:

1) Heat produced in the *fuel* is controlled by reactor regulating systems, moderating systems, and shutdown systems – SNP_D_1 facilitates these heat controls.
2) Heat transferred from the fuel to the *primary heat transport* systems is controlled by inventory controls, pressure controls, and circulating controls – SNP_D_2 facilitates this heat transfer.
3) Heat transferred from primary heat transport system to the *boilers* is controlled by boiler level controls and boiler pressure controls – SNP_D_3 facilitates this heat transfer.
4) Heat transferred from boilers to the *turbine* is controlled by boiler pressure controls and main steam governing controls – SNP_D_4 facilities this heat transfer.

   Heat energy is converted by the turbine into mechanical energy that runs the *electrical generator* to produce electricity – SNP_D_4 facilitates this energy conversion.
5) Heat energy is converted from the turbine exhausted steam to condenser – SNP_D_5 facilitates this energy conversion.

SNP scope for nuclear heat controls:

The SNP expedites the above-mentioned heat controlling process to achieve a balanced conversion of nuclear energy to electrical energy (the final product and lifeline of the nuclear plant), utilizing modern IT-network-based devices/systems of which the use is to be secured by this thesis' SNP designs of access control and network data base.

1.2.4 *Scope of Functions of SNP Access to Nuclear Division*

There are 10 systems in the SNP_D1 the calandria-moderator division:

Reactor flux/power monitoring system	$SNP\_D_1\_\boldsymbol{S}_1$
Main moderator control system	$SNP\_D_1\_\boldsymbol{S}_2$
Liquid zone control system	$SNP\_D_1\_\boldsymbol{S}_3$
Reactivity adjuster control system	$SNP\_D_1\_\boldsymbol{S}_4$
Moderator liquid poison control system	$SNP\_D_1\_\boldsymbol{S}_5$
Reactor shutdown control system	$SNP\_D_1\_\boldsymbol{S}_6$
Moderator purification control system	$SNP\_D_1\_\boldsymbol{S}_7$
Cover gas control system	$SNP\_D_1\_\boldsymbol{S}_8$
Moderator heavy water sampling system	$SNP\_D_1\_\boldsymbol{S}_9$
Moderator heavy water collection system	$SNP\_D_1\_\boldsymbol{S}_{10}$

The following describes the scope of the *SNP* access to first five of the ten calandria-moderator divisional systems, for the illustration purpose:

- $SNP\_D_1\_\boldsymbol{S}_1$: reactor flux/power monitoring system SNP access

There are two independent methods/equipment used to monitor the CANDU reactor flux: Ion Chamber Flux Detectors and In-Core Flux Detectors. The ion chamber detectors are used to monitor the reactor flux of low range. These detectors are installed outside of the calandria and they measure the neutron flux leaked out from the CANDU reactor. A signal is then generated from the flux measurement and the signal is proportional to the average reactor power only in the region of the reactor core that the flux is measured, but the signal cannot represent the reactor power in other regions of the reactor core. The in-core flux detectors are used to monitor the reactor flux of high range. Signals are then generated from these flux measurements and they are proportional to the neutron flux in the immediate areas of the detectors. These signals however will decrease with time, as these detectors continually absorb neutron from the reactor. The correction of the reactor power signals derived from the in-core flux detectors with the use of the reactor thermal power measurements.

The scope for $SNP\_D_1\_\mathbf{S}_1$ is to facilitate the monitoring of the CANDU reactor flux/power from ion-chamber flux detector and in-core flux detector, utilizing modern network-based signal processing devices of which the use is to be secured by this thesis' SNP access control and data base, and with significant reduction of proximity to the nuclear reactor for radiation measurements and signal processing, resulting with improved nuclear work environment.

- $SNP\_D_1\_\boldsymbol{S}_2$: main moderator control system SNP access

During normal reactor operation, the hot heavy water is pumped from the bottom of the calandria through two parallel heat exchangers to remove heat in the moderator. The cooled heavy water is returned to the calandria at the horizontal centerline in order to augment convection currents in the moderator inside the calandria. The controls of the main moderator system are: to slow down energetic neutrons released by fission to an energy level required to cause further fission; to remove heat in the moderator; to serve as a medium for diffusing chemicals for reactivity control in the reactor core; to provide heat sink for the reactor fuel in the event of a design basis earthquake induced steam main break and emergency power supply or emergency water supply failure; and to provide heat sink to ensure fuel channel integrity following a large loss of coolant accident and loss of emergency coolant injection.

The scope for $\mathrm{SNP\_D}_1\_\mathbf{S}_2$ is to facilitate the operation of the main heavy-water moderator for a typical CANDU reactor, utilizing modern network-based signal processing devices of which the use is to be secured by this thesis' SNP designs, resulting in improved moderator level control and enhanced nuclear safety.

- $SNP\_D_1\_\boldsymbol{S}_3$: liquid zone control system SNP access

The liquid zone control provides fine control of reactivity in the moderator using light water as absorber. The moderator is divided into 14 zone-control compartments, containing variable amount of light water. The cover gas over the light water is helium. The system is designed to circulate and condition the light water and gas flows. The control of the liquid zone are: to keep reactor critical for steady operation; to provide small positive or negative reactivity to increase or decrease the reactor power; to shape three-dimension power distribution; achieve bulk neutron flux control; and to achieve spatial neutron flux control.

The scope for $\mathrm{SNP\_D}_1\_\mathbf{S}_3$ is to facilitate the operation of the liquid zone system for a typical CANDU nuclear unit.

- $SNP\_D_1\_\boldsymbol{S}_4$: reactivity adjuster control system SNP access

The reactivity adjuster system provides adjustment of the CANDU reactivity in the moderator. This system consists of motor drive, thimble, thimble adapter, guide tube, guide tube extension, shield plugs, and adjusters. If natural cobalt is installed in the adjusters, after one or two years of irradiation the cobalt will be sufficiently transformed to Cobalt-60 to be of economic value. The cobalt is removed from the reactor and replaced with a fresh one for further cobalt irradiation. Cobalt-60 is utilized in radiography, therapy equipment, sterilization processes, etc. The controls of the reactivity adjuster system are: to shape the neutron flux to optimize reactor power and fuel burn-up; to provide excess reactivity needed to overcome Xenon-135 poisoning following reduction of power; and to develop full power output with all 21 adjusters inserted in the core.

The scope for SNP_D$_1$_**S**$_4$ is to facilitate the operation of the reactivity adjuster system for a typical CANDU nuclear unit.

- *SNP_D$_1$_**S**$_5$*: moderator liquid poison control system SNP access

The moderator liquid poison system regulates the reactivity of the CANDU moderator heavy water by adding soluble neutron poisons to it in a controlled manner. These poisons have large neutron capture cross-sections, are boron and gadolinium. The liquid poison system consists of a heavy water supply line from the main moderator system connected at the downstream of the moderator heat exchangers. Two mixing tanks, one for boron and one for gadolinium, both are equipped with ports for manual addition of boron and gadolinium. A separate line from each tank transports the liquid poison to the suction of the moderator pumps. Each tank is provided with a canned centrifugal pump to add these solutions to the moderator system to recirculate and mix the poison solutions and to permit sampling. The controls of the moderator liquid poison system are: to add negative reactivity to the moderator for excess reactivity in new fuel; to add negative reactivity for loss of xenon reactivity after a poison out or long shutdown; decrease reactivity along with other reactivity control devices; to guarantee enough poison in the moderator to prevent criticality during shutdown; and to automatically add gadolinium to the moderator when reactivity level rises above normal equilibrium.

The scope for SNP_D$_1$_**S**$_5$ is to facilitate the operation of the moderator liquid poison system for a typical CANDU nuclear unit.

1.3 Current States of Smart IT-based Industrial Controls and Process Access Controls

The nuclear process control system falls into the general category of industrial control systems, but the nuclear system has additional unique requirements due to nuclear safety operations and concerns.

First, this section presents this thesis research findings on the assessment of the current state of smart industrial control systems (section 1.3.1), information technology (IT) systems (section 1.3.2), and nuclear process control systems (section 1.3.3). This assessment is to lay out the background to establish the *BenchMarks* (*BM*) for this thesis' development of a new *Security-integrated Nuclear Process* (*SNP*).

Second, this section presents this thesis research findings on the assessment of state-of-the-art network access controls (sections 1.3.4). This assessment is to lay out the background to establish *Benchmarks* for this thesis' development of a new *Operation Based Access Control (OBAC)*.

1.3.1. Benchmarks for SNP over current state of smart industrial control systems

This thesis research identifies the NIST 800-82 *Guide to industrial control systems security* [1] to be a good source for the study of the security of industrial control systems, specifically for the nuclear process control systems. This NIST 800-82 is to be utilized to establish the benchmarks for the *SNP* development, as illustrated below:

BM-1: *SNP shall be free from the below-mentioned potential risks and conflicts.*

Potential risks and conflicts: The industrial control systems were originally isolated systems running proprietary control protocols using specialized hardware and software. They are being replaced by widely available low-cost internet protocol devices that increases the possibility of cyber security vulnerabilities and incidents. As industrial control systems are adopting information technology (IT) solutions to increase connectivity and remote access capabilities and are being designed and implemented using industry standard computers, operating systems and network protocols, they are starting to resemble Information Technology (IT) systems. This integration supports new IT capabilities, but it provides significantly less isolation for industrial control systems from the outside world than predecessor systems, creating a greater need to secure these systems. The industrial control systems have characteristics that differ from traditional IT systems. The logic executing in industrial control systems has a direct effect on the physical world. If the industrial control system is faulted, significant risks to the health and safety of human lives and serious damage to the environment and serious financial issues such as production losses, negative impact to nation economy, and compromised proprietary information. Therefore, industrial control systems have their unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. The nuclear control system is a typical industrial control system with strict safety requirements and if the nuclear system is faulted, it causes serious consequences of nuclear safety.

Efficiency and safety may conflict with security in the design and operation of industrial control systems. Extensive procedures may need to be executed to achieve guaranteed security for the industrial systems, and such execution may slow down the system operation that affects the system efficiency and may delay the system response to an event that affects the system safety. Any influence on the safety of the nuclear control system is not acceptable, as a basic requirement for the design of security-integrated nuclear process controls in this thesis.

BM-2: *SNP shall be free from the below-mentioned security concerns.*

Security Concerns: The industrial control systems were originally susceptible primarily to local threats because many of their components were in physically secured areas and the system components were not connected to IT networks. However the trend toward integrating industrial control systems with IT networks provides significantly less isolation for industrial control systems from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats. The increasing use of wireless networking places industrial control systems implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Also threats to the control systems can come from numerous sources including terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters and malicious insider, accidental actions by insiders, etc.

Potential security concerns on modern industrial control systems include: Flow of information through industrial control systems networks is blocked or delayed, causing disruption on the industrial control systems operation; Instructions, commands, or alarm thresholds are changed without authorization, causing damage to equipment, disabling or shutting down of equipment, creating environmental impacts, endangering human life, etc.; Inaccurate information is sent to system operators to mask unauthorized changes, to cause the operators to initiate inappropriate actions, etc.; Industrial control systems software or configuration settings are modified, or industrial control systems software are infected with malware, etc.; Interference with the operation of safety systems could cause direct danger to human life.

BM-3: *SNP shall embrace the below-mentioned security strategies.*

Security Strategies: The industrial control system security strategies include: restrict software access to the industrial control systems network using a demilitarized zone network architecture with firewalls to prevent network traffic from passing directly between the corporate and industrial control systems networks, and having separate authentication mechanisms and credentials for users of the corporate and industrial control systems networks; restrict physical access to the industrial control systems network and devices as unauthorized physical access could cause serious disruption of the industrial control systems functionality; protect individual industrial control systems from exploitation, deploying security patches speedy after testing them under field conditions, disabling all unused ports and services, restricting systems user privileges to only those as required for their roles, tracking audit trails, and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware; maintain functionality during adverse conditions, designing the industrial control systems with each critical component having a redundant counterpart and with fail safe mechanism to ensure any failure does not generate unnecessary traffic on the industrial control systems; restore system rapidly after an incident.

BM-4: *SNP shall embrace the below-mentioned defense-in-depth strategies.*

Defense-in-depth strategies: The industrial control system security defense-in-depth strategies include: develop security policies, procedures, training for access to the industrial control systems; address security throughout the lifecycle of the industrial control systems from architecture design to procurement to installation to maintenance to decommissioning; implement a network topology for the industrial control systems with multiple layers and with the most critical communications occurring in the most secure and reliable layer; provide software separation between the corporate and industrial control systems networks; employ a demilitarized zone network architecture to prevent direct traffic between the corporate and industrial control systems networks; ensure that critical components are redundant and are on redundant networks; design critical systems for fault tolerant to prevent catastrophic cascading events; disable unused ports and services on industrial control systems devices after testing to assure this will not impact industrial control systems operation; restrict physical access to the industrial control systems; restrict industrial control systems user privileges to only those as required to perform their roles, establishing role-based access control, and configuring each role based on the principle of least privilege; use separate authentication mechanisms and credentials for users of the industrial control systems network and the corporate network; use modern technology such as smart cards for personal identity verification; implement security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the industrial control systems; apply security techniques such as encryption and cryptographic hashes to industrial control systems data storage and communications where determined appropriate; deploy security patches speedy after testing all patches under field conditions; track audit trails on critical areas of the industrial control systems.

1.3.2. Benchmarks for SNP over current state of IT systems

Smart industrial control systems have adopted many features of the IT systems to increase their connectivity and remote access capabilities. Due to possible risks to the health and safety of human lives, serious damage to the environment, and loss of production/revenue, the industrial control systems have unique performance, reliability, and security requirements/features, in comparison with the general IT systems, as listed below.

BM-5: *SNP shall embrace the below-mentioned time-critical performance and availability.*

Time-critical Performance and System Availability: Industrial control systems are generally time-critical with limited acceptable delays as per individual applications; industrial control systems require deterministic responses for predictable controls; high throughput is usually not essential to industrial control systems. Conversely the IT systems require high throughput but they can tolerate considerable delays.

The industrial control systems are continuous in operation, and unexpected outages of these systems are not acceptable. Outages are often to be planned and scheduled weeks or months in advance. Exhaustive pre-deployment testing is essential to ensure high availability for the industrial control systems. Some IT strategies, such as rebooting a component as it becomes unavailable, are usually not acceptable due to the adverse impact on the requirements for high availability, reliability and maintainability of the industrial control systems. The industrial control systems employ redundant components to provide continuity when any system component becomes unavailable.

BM-6: *SNP shall embrace the below-mentioned risks management.*

Risks Management and Security Architecture: The data confidentiality and integrity are typically the primary concerns for IT systems. On the other hand, 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, or lost or damaged products are the primary concerns for the industrial control systems. The personnel responsible for operating, securing, and maintaining industrial control systems must understand the important link between safety and security.

The primary security focus for the industrial control systems is to protect the operations of control components as they affect the end processes, but the primary security focus for the IT systems is to protect the information stored/transmitted. This affects the design of security architecture for the industrial control networks.

BM-7: *SNP shall embrace the below-mentioned physical interactions and responsiveness.*

Physical Interactions and Responsiveness: The IT systems have virtually no physical interactions with the environment. Conversely industrial control systems can have complex interactions with physical processes. All security functions integrated into the industrial control systems must be tested off-line in comparable environment to prove that they do not compromise normal control systems functionality.

The access control for the IT systems can be implemented without significant regard for data flow. Conversely for the industrial control systems, automated response time or system response to human interaction may be critical. The processing of authentication and authorization on a human-machine interface must not interfere with emergency actions for industrial control systems, and the data flow must not be interrupted or compromised. Access to the industrial control systems should be restricted by rigorous physical security controls.

BM-8: *SNP shall embrace the below-mentioned operation tolerances and resources constraints.*

Operation tolerances and resource constraints: The operating systems for the industrial control systems and their applications may not tolerate typical IT system security practices. The legacy systems are especially vulnerable to resource unavailability and timing disruptions. Control networks are often more complex and require a different level of expertise, as control networks are typically managed by control engineers, not IT personnel. Software and hardware are more difficult to upgrade in an operational control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection.

The industrial control systems and their real time operating systems are often resource-constrained systems that usually do not include typical IT security capabilities. There may not be computing resources available on industrial control systems components to retrofit these systems with current security capabilities. The third-party security solutions may not be allowed due to industrial control systems vendor license and service agreements, and loss of service support can occur if third-party applications are installed without vendor acknowledgement or approval.

BM-9: *SNP shall embrace the below-mentioned communication and software constraints.*

Communication and software Constraints: The communication protocols and media used by the industrial control systems environments for field device control are typically different from the generic IT systems environments, and they may be proprietary.

Unpatched software represents a serious vulnerability to a system. Software updates on IT systems including security patches are typically applied in a timely fashion based on appropriate security policy and procedures, and the procedures are often automated using server-based tools. However, software updates on the industrial control systems cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the vendor of the industrial control application and the end user of the application before being implemented and industrial control systems outages often must be planned and scheduled days or weeks in advance. The industrial control systems require revalidation as part of the update process. The change management process for the industrial control systems requires careful assessment by industrial control systems experts/engineers working in conjunction with security and IT personnel.

BM-10: *SNP shall embrace the below-mentioned diversification and components accessibility.*

Diversification and components accessibility: The IT systems allow for diversified support styles, supporting disparate but interconnected technology architectures. However for industrial control systems, service support is usually via a single vendor, which may not have a diversified and interoperable support solutions from other vendors.

The typical IT components have a lifetime of 3 to 5 years due to the quick evolution of technology. However for industrial control systems where technology was often developed for very specific use and implementation, the lifetime of the deployed technology is of 15 to 20 years and sometimes longer. The typical IT system components are usually local and easy to access, while the industrial control systems may be isolated, remote, and require extensive physical effort to gain access.

1.3.3. Benchmarks for SNP established over Current State of Nuclear Process

Intelligent (smart) process control equipment of various kinds from simple devices to complex systems, such as from standalone smart valve positioners to state-of-the-art 800MW generator automatic control systems are available for modernization of nuclear process operations, and many of them are already physically installed in the nuclear generating stations. These smart process control equipment have networking capability with intelligent features for central data processing, systems operations optimizing and coordinating, predictive maintenance scheduling, etc.

Unfortunately, the untold reality learnt from on-nuclear-site experiences, is that most of intelligent features in these equipment are deliberately disabled or their capabilities are severely limited intentionally due to security concerns in the nuclear operating environment and therefore, millions dollars of potential savings and associated benefits are lost. With respect to the process control refurbishment, the obsoleted devices/equipment/systems were replaced, as a first priority with ones of the same form, fit, and function.

The replacement with newer devices/equipment/systems having intelligent features with networking capability is not necessary a priority, unless no equivalence to the obsoleted ones can be found. Should it be in such situation with exhausted search resulting in no equivalent replacement found, then replacement with modern smart equipment will be considered but their intelligent features with networking capability were either disabled or substantially limited due to security concerns and therefore, the potential benefits are severely reduced. Even the need for nuclear unit refurbishment and the huge cost for refurbishment were the recent past reality, the situation will stay unchanged in the foreseeable future as the existing nuclear units are aging.

BM-11: *SNP shall fully utilize the embedded features in the modern nuclear devices/systems already installed in the nuclear process and released the benefits of these features.*

1.3.4. Benchmarks for SNP Access over state-of-the-art network access controls

The first defense for the new *SNP* operation network is the secure control of the access to the *SNP* network. This thesis research identifies the *ANSI INCITS 359: Role Based Access Control* (RBAC) [2] to be a good source for the study of network access controls, particularly in an effort to implement security measures for nuclear process access.

1.3.4-1 Role Based Access Control

The RBAC consists of the *reference model* and the *system and administrative functional specification*:

The *reference model* defines the sets of basic elements (users, roles, permissions, operations and objects) and relations. The reference model identifies the minimum set of features, aspects of role hierarchies, aspects of static constraint relations, and aspects of dynamic constraint relations. Also the reference model provides a precise and consistent language, in terms of element sets and functions for use in defining the functional specification. The *system and administrative functional specification* 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 (users, roles and permissions) and relations (user-role assignments). 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.

The *reference model* can be defined in terms of: *Core RBAC* defines a minimum collection of RBAC elements (users, roles, permissions, operations, and objects) and relations (user-role and permission-role assignments); *Hierarchical RBAC* adds relations to support role hierarchies. A hierarchy is a partial order defining a seniority relation between roles, whereby senor roles acquire the permissions of their juniors and junior roles acquire users of their seniors; *SSD relation* adds exclusivity relations among roles with respect to user assignments in the presence and absence of role hierarchies; *DSD relation* defines exclusivity relations with respect to roles that are activated as part of a user session.

Core RBAC Model: The core model includes sets of five basic data elements called users, roles, objects, operations, and permissions. The model is defined in terms of individual users being assigned to roles and permissions being assigned to roles. A role is a means for naming many-to-many relationships among individual users and permissions. The core model includes a set of sessions where each session is a mapping between a user and an activated subset of roles that are assigned to the user. *User* is defined as a human being in this standard (the concept of a user is extended to include nuclear process machines in this thesis). *Role* is a job function with the authority and responsibility conferred on users assigned to the role. *Permission* is an approval to perform an operation on RBAC objects. *Operation* executes some functions for the user, for example within a file system, operations might include read, write, and execute and within a database management system, operations might include insert, delete, append and update. *Object* is an entity that contains or receives information.

Role relations: RBAC defines two relations: *user assignment* and *permission assignment*. They are a many-to-many relations that a user can be assigned to one or more roles and a role can be assigned to one or more users. This arrangement provides flexibility of assigning permissions to roles and users to roles, but without it a user may be granted more access to resources than is needed, because of limited control over the type of access that can be associated with users and resources. Any increase in the flexibility of controlling access to resources also strengthens the application of the principle of least privilege.

Sessions: Each session is a mapping of one user to possibly many roles. A user establishes a session to activate some subset of roles that the user is assigned. Each session is associated with a single user and each user is associated with one or more sessions. The function *session_roles* activates the roles and the function *session_users* activates the sessions. The permissions available to the user are the permissions assigned to the roles that are currently active across all the user's sessions.

Role hierarchy means structuring roles to reflect an organization's lines of authority and responsibility. It defines an inheritance relation among roles. Inheritance can be described in terms of permissions as r_1 inherits role r_2 if all privileges of r_2 are also privileges of r_1. Alternatively, role hierarchy can be managed in terms of user containment relations as role r_1 contains role r_2 if all users authorized for r_1 are also authorized for r_2. However, the user containment implies that a user of r_1 has at least all the privileges of r_2, while the permission inheritance for r_1 and r_2 does not imply anything about user assignment. The standard recognizes two types of role hierarchies: general role hierarchies and limited role hierarchies. The general role hierarchies provide support for an arbitrary partial order to serve as the role hierarchy, to include the concept of multiple inheritances of permissions and user membership among roles. The limited role hierarchies impose restrictions resulting in a simpler tree structure, where a role may have one or more immediate ascendants, but is restricted to a single immediate descendent.

General role hierarchies support the concept of multiple inheritance that enables to inherit permission and user membership from two or more role sources. The multiple inheritance provides two hierarchy properties: the ability to compose a role from multiple subordinate roles with fewer permissions in defining roles and relations; the ability to provide uniform treatment of user/role assignment relations and role/role inheritance relations.

Limited role hierarchies are restricted to a single immediate descendent. They provide clear administrative advantages over Core RBAC. The limited role hierarchy can be defined as a restriction on the immediate descendants of the general role hierarchy.

Constrained RBAC adds separation of duty relations to the RBAC model. The separation of duty relations enforce conflict of interest policies to prevent users from exceeding a reasonable level of authority for their positions. In order to minimize the likelihood of collusion, individuals of different skills or divergent interests are assigned to separate tasks required in the performance of a function. This is to ensure that fraud and major errors cannot occur without deliberate collusion of multiple users. The RBAC standard allows for both static and dynamic separation of duty as defined below.

Static Separation of Duty (SSD) Relations: The conflict of interest in a role-based system may be as a result of a user gaining authorization for permissions associated with conflicting roles. One way of preventing this conflict is through the SSD to enforce constraints on the assignment of users to roles. The SSD defines the mutually disjoint user assignments with respect to sets of roles. The SSD constraints defined in this model are limited to those relations that place restrictions on sets of roles to form user assignment relations. An SSD policy can be centrally specified and then uniformly imposed on specific roles. The SSD relations can enforce conflict of interest and other separation rules over sets of RBAC elements. The SSD place restrictions on administrative operations that may undermine higher-level organizational SSD policies.

SSD on User-Role Assignments: The RBAC models define the SSD relations with respect to constraints on user-role assignments over pairs of roles such that no user can be simultaneously assigned to both roles in SSD. This is overly restrictive in two aspects: the size of the set of roles in the SSD and the combination of roles in the set for which user assignment is restricted.

SSD on Hierarchical RBAC: When applying the SSD relations in a role hierarchy RBAC, care is needed to ensure that user inheritance does not undermine the SSD policies, because role hierarchies have been defined to include the inheritance of SSD constraints. In order to address this inconsistency, the SSD is defined as a constraint on the authorized users of the roles that have an SSD relation.

Dynamic Separation of Duty (DSD) Relations: The DSD relations, like the SSD relations, limit the permissions available to a user. However the DSD relations differ from SSD relations by the context in which these limitations are imposed. The SSD relations place constraints on a user’s total permission space. The DSD relations place constraints on the roles that can be activated within or across a user’s sessions. The DSD properties provide extended support for the principle of least privilege in that each user has different levels of permission at different times, depending on the role being performed. These properties ensure that permissions do not persist beyond the time that they are required for performance of duty. This aspect of least privilege is often referred to as timely revocation of trust. The dynamic revocation of permissions can be a rather complex issue without the facilities of the DSD, and it generally ignored in the past for reasons of expediency.

The SSD relations address potential conflict-of-interest issues at the time a user is assigned to a role. The DSD allows a user to be authorized for two or more roles that do not create a conflict of interest when acted in independently, but produce policy concerns when activated simultaneously. As long as the same user is not allowed to assume both of these roles at the same time, a conflict of interest situation will not arise. Although this effect could be achieved through the SSD, the DSD generally provides the organizations with greater operational flexibility.

RBAC System and Administrative Functional Specification defines functions and semantics to create, delete and maintain RBAC users, roles and permissions and relations, as well as defines the creation of user sessions to perform role activation/deactivation, enforcement of constraints on role activation, and access decision.

1.3.4-2 Limitations of RBAC for Nuclear Operations

As it is named the "*Role Based*", the RBAC is centred on the *ROLES*, as such how to relate *"ROLES* and *USERS"* (e.g. mapping a role onto a set of users), or relate *"ROLES* and *PERMISSIONS"* (e.g. mapping a role onto a set of permissions). The following illustrates the limitations of RBAC when it is used for access to the nuclear process operations:

a) The *Core RBAC* deals with the role-user assignments and the role-permission assignments. Simply, if a user is assigned with a role, then the user will have all the permissions/privileges of that role, and then the user can execute all the operations or can access all the objects associated with the permissions assigned to that role.

   However, this *Core RBAC* cannot cover the strict and detailed requirement for access to the nuclear process operations. The reasons are: first the operation of each of the thousands of devices in a nuclear plant may be fairly unique for the conditions that a particular device being operated and any mis-operations could cause tremendous serious nuclear consequences/casualties; second the roles are practically limited to a certain number, but the devices to be operated are thousands in a nuclear plant; third the nuclear devices operations require the operators' currency of technologies that the operators can only be accredited with constant trainings. Therefore, not simply with an assigned role, the user will have the privileges of that role to carry out all the nuclear operations.

b) The *Hierarchal RBAC* structures roles to reflect an organization's lines of authority and responsibility. It defines an inheritance relation among roles that can simply described in terms of permissions that if a role of higher inheritance level (e.g. a senior role) inherits a role of lower inheritance level (e.g. a junior role) then all the privileges of the junior role are also the privileges of the senior role. This *Hierarchal RBAC* structure works well for office information/data access that is most of the access controls are designed for, as such that junior staff roles have certain privileges to access/handle certain information/data, and their senior manager role who inherits their roles will certain have all their privileges to access/handle those information/data.

However, this *Hierarchal RBAC* structure cannot directly be applied as the control of access to the nuclear operations. This can be illustrated with a simple case for access to a nuclear pressure-transmitter operation that a nuclear chief engineer has an official position of much higher seniority than a nuclear technician, but the technician possessing required pressure-transmitters trainings with proof-of-currency certificates can be authorized by the chief engineer to access/handle the pressure-transmitter operation however, the chief engineer himself/herself cannot be authorized to do that job without the proper valid certificates.

c) The *Constrained RBAC* adds separation of duty relations to the RBAC model, and the separation of duty relations are to enforce conflict of interest policies to prevent users from exceeding a reasonable level of authority for their positions. This *Constrained RBAC* basically imposes constrains on the assignments of roles to the users, whether in *Core RBAC* or in *Hierarchal RBAC*,

However, this *Constrained RBAC* is definitely not enough for covering the qualifications requirements for the operations of nuclear process. As described above, the operation of each of the thousands of devices in a nuclear plant may be fairly unique for the conditions that a particular device being operated and any mis-operations could cause tremendous serious nuclear consequences, and therefore merely imposing constrains on the roles is obvious far from adequacy. The access to the nuclear process should be constrained on the nuclear systems/equipment/devices operations themselves, and this is targeted in this thesis research.

d) The *RBAC Specification* defines functions and semantics to create, delete and maintain RBAC users, roles and permissions and relations. The *RBAC Specification* is considerably involved. Even with such an involved specification process, it still cannot meet the qualifications requirements for the access to the nuclear operations. A new design for the access to nuclear operations is needed.

BM-12: *SNP access control shall be free from the above-mentioned limitations and shall develop a suitable access control for nuclear operations application.*

1.4 Introduction of New Operation-Based Access Control to Nuclear Process

This thesis develops a new design for the controls of access to the nuclear process operations. The architecture of this new nuclear operations access control is shown in Figure 1.1. This figure shows that the operation is the focus of this new access control design, and therefore it is termed as "*Operation-Based Access Control*", the **OBAC**.

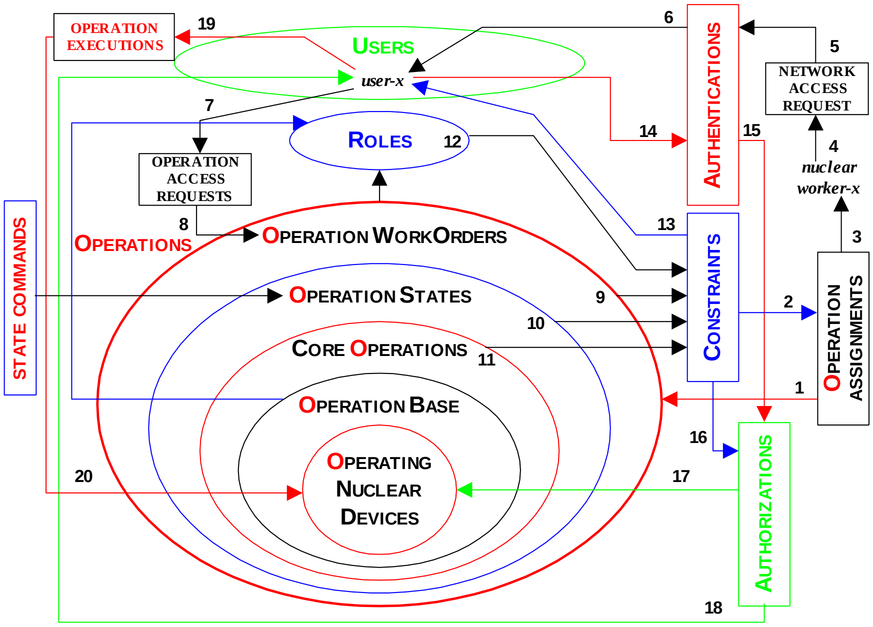


Figure 1.1: **OBAC** design

The following provides an introduction of this new access control (details are given in chapter 2).

1.4.1 *Overall View of OBAC*

The flow of the access control in *OBAC* is numbered in Figure 1.1. Starting with the assignment of operation work orders, the operation network may be checked (1) to get information of the current constraints/requirements for the work order to be assigned (2). The operation work order is to assign to the nuclear worker-*x* (3). The nuclear worker-*x* makes a network access request (4) and carries out pre-access authentication (see chapter 3) to validate the worker's access legitimacy (5) and then the worker-*x* enter into the nuclear operation access network and becomes an authorized nuclear network user-*x* (6). The user-*x* makes an operation access request (7) to check the operation work-order access control (8) that generates the work-order validation and feedbacks as constraints (9). The operation work order access is mapped to the operation states that controls the work order access to the nuclear core operations and feedbacks as constraints (10). The work order is then mapped to the core operation access and generates the technical, field-experience and role-experience qualification requirements and feedbacks as constraints (11) and (12). Then all the access constraints/requirements are sent back to the user-*x* (13) to request for satisfying these access requirements. The user-*x* sends his/her qualification certificates for satisfying the access requirements to the authentication server (14). The server verifies the user-*x*' certificates and if they are verified (15), the authenticated certificates are sent to the authorization server where they are checked against the operation access requirements (16). If the check is passed, the authorization server informs the core nuclear operation control (17) and sends an operation-access permit to the user-*x* (18). The permit allows user-*x* to make work order operation execution (19) and finally user-*x* can access to the nuclear operation network to execute their assigned work orders (20).

1.4.2 *Comparison of OBAC with standard RBAC*

The following provides a brief comparison of the new design *OBAC* and the standard network access control *RBAC* using the function specifications for both access control for illustration.

The *RBAC Specification* defines functions and semantics to create, delete and maintain RBAC users, roles and permissions and relations. The following is taken from the RBAC standard *ANSI INCITS 359* [2] for illustration of the RBAC specification for assigning a user with the Static Separation of Duty SSD constrain.

$$AssignUser(user, role\colon NAME)$$

$$\begin{aligned}
&AssignUser(user, role\colon NAME)\\
&user \in USERS; role \in ROLES; (user \mapsto role) \notin UA\\
&\forall ssd \in SSD \circ \bigcap_{\substack{r \in subset \\ subset \subseteq ssd_{set(ssd)} \\ |subset| = ssd_{card(ssd)} \\ au = if\ r = role\ then\ \{user\}\ else \emptyset}} (authorized\_users(r) \cup au) = \emptyset\\
&UA' = UA \cup \{user \mapsto role\}\\
&assigned\_user' = asssigned\_users \setminus \{role \mapsto assigned\_users(role)\} \cup\\
&\{role \mapsto (assigned\_users(role) \cup \{user\})\}
\end{aligned}$$

It can be recognized that this *RBAC Specification* is considerably involved. Even with such an involved specification process, it still cannot meet the qualifications requirements for the controls of access to the nuclear operations. Therefore, a new design for the access to the nuclear operations is needed.

As to be demonstrated in chapter 2, the ***OBAC*** designed in this thesis has special features and advantages for the application on the nuclear process access controls, for example:

- ***OBAC*** is "simple" of one pattern of specifications, which can easily be reapplied for different access elements and functions such as for adding an element, deleting an element, assigning/authorizing an element, etc. The simple specification pattern is particularly important for nuclear process access controls, which offers confident safety routine validations for nuclear operations, as compared with the complex specifications used in the role-based access controls, of which illustrations are provided in chapter 2.
- ***OBAC*** is a "single" layer control for different access-specification sessions to carry out various mappings or authorizations. For the reason of capable of offering confident safety routine validations, this OBAC single-layer feature is essential for nuclear applications, as compared with the multiple layers of specifications used in the role-based access controls.
- ***OBAC*** is "robust" for access controls execution with one-pattern and one-layer access control architecture. Whenever a possible not-immediately-known nuclear event occurs, the paths for searching for the causes should be as short as practically possible. The OBAC's robust access control architecture offers this critically needed feature for nuclear event causes searching, of which the role-based access controls cannot offer.
- ***OBAC*** is "efficient" for processing the access specifications and access control implementations due to simple access architecture.
- ***OBAC*** is "reliable" for access control security executions as the access security is simply embedded in the access qualification requirements. This qualifications embedment offers absolutely-simple security assurance, as it does not leave the determination of whether all qualification requirements are met to the layers of access control checks. In the nuclear environment, the simpler is the better for all nuclear processes, as any mis-operations could cause tremendous serious nuclear consequences or casualties.

1.5 Introduction of Network Access Authentication and Protocols

This section presents this thesis research's findings of the current state of current states of authentication and protocols for network access, access security concerns and resolutions using authentication.

Authentication is a procedure of verifying the identity of a user as a prerequisite for granting access to a communication network as well as a necessary measure for preventing or rejecting unauthorized network access. Many authentication protocols have been proposed for general wired or wireless network applications and a few authentication protocols designed for power systems mainly for smart grid meter authentications. There is none specifically for the nuclear applications.

An overview of authentication basics and applications is given below:

Authentication Protocols for Wired Networks: As a typical protocol for wired network, Kerberos [27] works on the basis of *tickets* to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aim primarily at a client-server model and it provides mutual authentication that both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Authentication with Hardware for Wired Networks: The RSA SecurID [28] employs hardware tokens to authenticate user. The hardware token stores secrets in a tamper-resistant module carried by the user. The simplest dedicated-hardware version has only a display and no buttons.

Authentication Protocols for Wireless Networks: As a typical protocol for wireless network, PANA [29] enables authentication between clients and access networks in wireless local area networks. PANA runs between a client and a server to perform authentication and authorization for the network access.

Authentication Protocols for Smart Grids: For smart grids application, a light-weight and secure message authentication mechanism [32] is proposed based on Diffie-Hellman key establishment protocol and hash-based message authentication code. This allows various smart meters at different points of the smart grids to make mutual authentication and achieve message authentication with low latency and few signal message exchanges.

Authentication Protocols using Public-Key Cryptography: The authentication protocol to be designed in this thesis for users of a nuclear site to access critical process with nuclear safety requirements needs high level of security as well as high efficiency for real-time nuclear operations. The protocol is therefore based on public key cryptography.

Transport Layer Security: The International Electrotechnical Commission (IEC) standard IEC61850 [2] is developed for power substation automation, and this IEC standard recommends Transport Layer Security [5], a public-key based authentication protocol, to achieve secure communications. However, transport layer security has two weaknesses: 1) it is not efficient, and 2) the key updates are vulnerable.

Authentication Protocols for Power Systems: The authentication protocol for the power system applications shall meet the following requirements [3]: *High Efficiency* - efficiency is crucial to achieve the high availability requirement in real-time power system applications; *Resilient to Attacks* - authentication schemes are required to resist malicious attacks, such as forgery attack, replay attack, and denial-of-service attack; *Mutual Authentication* - this authentication is a two-way authentication process between a user and the authentication server. The users ensure that they are not communicating with a malicious authentication server by authenticating the server.

Authentication Protocol Standard: The Federal Information Processing Standards *FIPS-196* [23] specifies two challenge-response protocols by which the user and the verifier may authenticate their identities to one another. The authentication uses public key cryptography, digital signatures, and random number challengers.

The protocol can be designed to address threats including masquerade, password compromise, replay attacks, etc. by the following means:

Use of challenges and digital signatures for authentication eliminates the need for transmitting passwords and therefore to reduce the passwords being compromised. Passwords however may still be used for users to access their private keys, and thus passwords must be kept secure.

Use of public key cryptography eliminates the need for the authenticating individuals to share their secret values, and therefore it is extremely important to always keep the private keys secure and under the owners' sole control.

Use of random number challenges prevents an intruder from copying an authentication token signed by another user and replaying it successfully at a later time. However, a new random number challenge should be generated for each authentication exchange. The security of replay prevention hinges on the generation of random number challenges that have a low probability of being duplicated.

Use of a random number of its own in an authentication token allows the user to preclude the signing of only data that is pre-defined by the verifier. If a user uses its private key for more than just signing authentication tokens, then a verifier could maliciously create a challenge consisting of information which is meaningful in another context. This can be prevented when the user signs both the challenge and unpredictable, meaningless data - a random number.

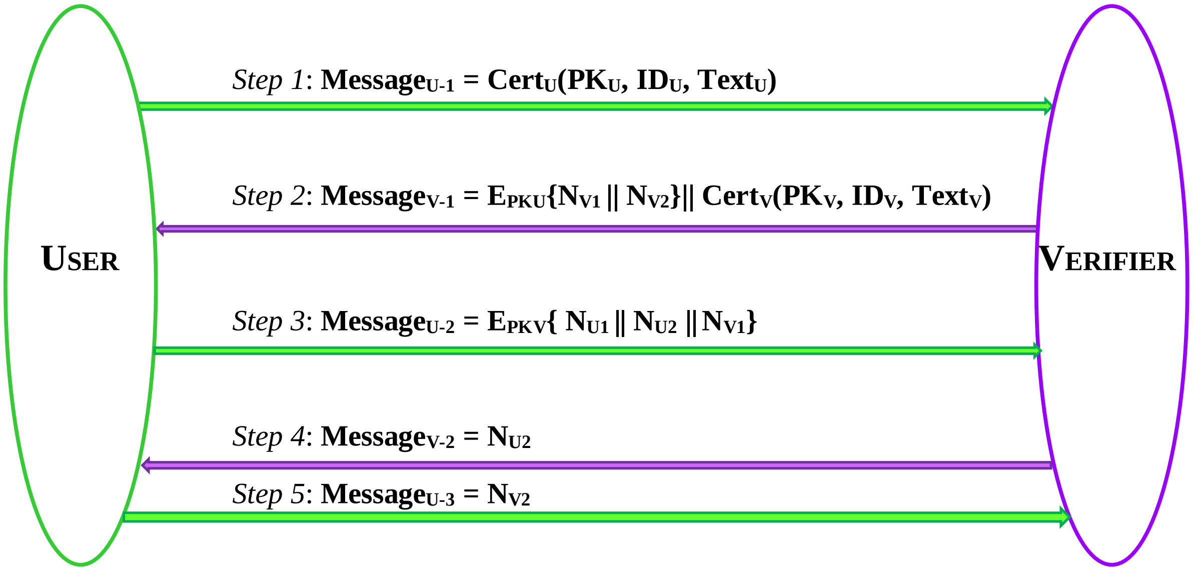
Other threats include denial of service, session capture, transmission modification, and compromised private key. No aspect of the authentication tokens or protocols preclude another entity from rerouting or modifying authentication transmissions. Maintaining the secrecy of the private key is of extreme importance and failure to do so may result in an attacker masquerading as the legitimate user by using the user's private key for authentication.

1.6 Introduction of New Operation-based Access Authentication for Nuclear Process

This thesis research develops a new design for nuclear process access authentication, termed the *Nuclear Operation Access Authentication* (**NOAA**). The design development has considered the authentication application requirements, concerns, resolutions, etc. discussed in the previous section.

The design of nuclear process access authentication must be, for real-time nuclear operations that are critical due to nuclear safety, high efficient and resilient to attacks. A design objective is to minimize the latency of the authentication protocol, specifically to minimize the burden of message exchanges between the user and the verifier and key operations by the user and the verifier while achieving high resilience to all kinds of possible attacks.

Figure 1.2 shows a new protocol termed the *Authentication Pre-access Protocol* (***APP***) that is developed for the ***NOAA*** system (detailed in section 3.2). As shown in the figure, there are five (5) steps in the ***APP*** that is used to determine the person (or device) requesting to access the nuclear process is legitimate and authorized user. This is the first and most important defense for the security of the nuclear process network and subsequently the safety of the nuclear operations.



USER
VERIFIER
Step 1: $\mathbf{Message_{U\text{-}1} = Cert_U(PK_U, ID_U, Text_U)}$
Step 2: $\mathbf{Message_{V\text{-}1} = E_{PKU}\{N_{V1} \| N_{V2}\} \| Cert_V(PK_V, ID_V, Text_V)}$
Step 3: $\mathbf{Message_{U\text{-}2} = E_{PKV}\{ N_{U1} \| N_{U2} \| N_{V1}\}}$
Step 4: $\mathbf{Message_{V\text{-}2} = N_{U2}}$
Step 5: $\mathbf{Message_{U\text{-}3} = N_{V2}}$

Figure 1.2: ***APP*** - a 5 step protocol for nuclear process pre-access authentication

Simultaneously, the verifier is authenticated by the user to ensure that the verifier is the legitimate verifier. This mutual authentication that further confirms the security of access to the nuclear process consists of 5 steps (see section 3.2 for details):

Step 1: User sends its digital certificate to Verifier, for authentication.

Step 2: Verifier encrypts its two nonces and sends to User, with its digital certificate.

Step 3: User encrypts its two nonces and sends to verifier, with one of verifier's nonce.

Step 4: Verifier sends one of the user's nonce to announce the success of user authentication.

Step 5: User sends one of the verifier's nonce to announce the success of verifier authentication.

The new design of ***NOAA*** authentication is resilient to cyber-attacks, in particular the forgery attacks and replay attacks and the analysis is given in section 3.5.

1.7 Overview of SNP Designs Analysis

This section presents an overview of the *SNP* designs analysis.

The best measure of the merit of a practical process/design change for performing the same or better functions as the existing ones in the industry is the *cost saving* that the new design can bring in and for the nuclear industry specifically, the *safety* and *security* that the new design can enhance. This thesis research creates the cost models for the current nuclear practices to establish a reference base for the *SNP* designs analysis.

Table 1.1 summarizes the cost models for the current nuclear equipment maintenances, where the cost *NCM_1* is the base cost, and *NCM_2* and *NCM_3* and *NCM_4* are additional costs above the base cost, due to on-line maintenance, forced-outage maintenance, and delayed maintenance, respectively (see section 5.1 for details).

Table 1.1: Cost models for current maintenance

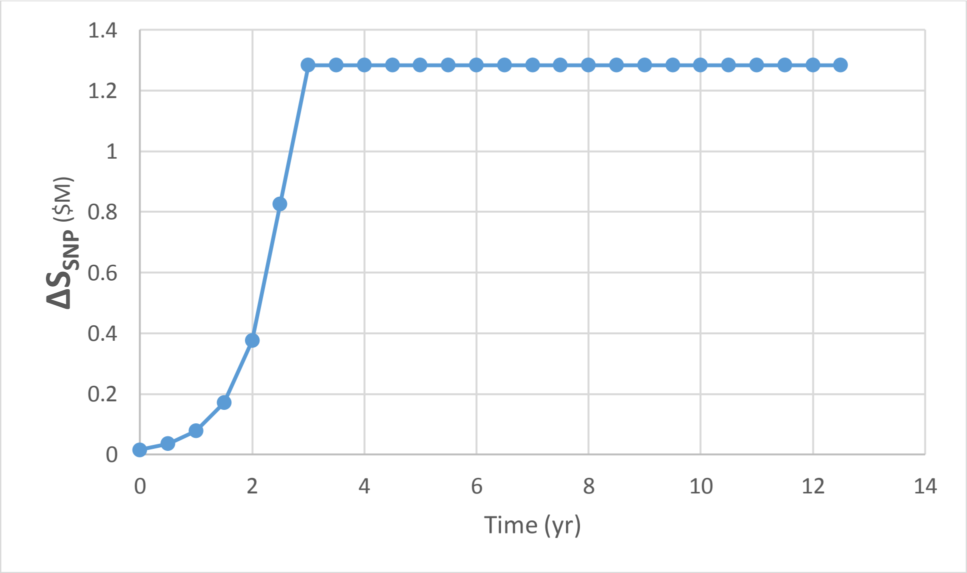
NCM_1 =	*Base Cost for Scheduled-outage Maintenance* $Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so} + Tm_{so} \times Rrev + C_{eam}$
NCM_2 =	*Additional Cost due to On-line Maintenance* $(Tp_{on} \times Np_{on} + Tm_{on} \times Nm_{on}) \times R_{on} + Ceam$
NCM_3 =	*Additional Cost due to Forced-outage Maintenance* $(Tp_{fo} \times Np_{fo} + Tm_{fo} \times Nm_{fo}) \times Rm_{fo} + Tm_{fo} \times Rrev + C_{eam}$
NCM_4 =	*Additional Cost due to Delayed Maintenance* $(T_{ed} + T_{md}) \times N_{em} \times R_{em}$
NCM_5 =	*Average Annual Cost for Maintenance* $F_{so} \times NCM\_1 + F_{on} \times NCM\_2 + F_{fo} \times NCM\_3 + F_{de} \times NCM\_4$

This thesis research also creates the cost saving models for the implementation of the *SNP* designs as well as for the installation of smart process control (SPC).

Table 1.2 shows the cost saving models and these models represent that the accumulative cost savings as benefited from the *SNP* and *SPC* implementations increase at an accelerative speed initially and then at constant speed after the limit is reached, as shown in Graph 1.1 (see section 5.4 for details).

Table 1.2: Cost savings models

S_{SNP}	$= \sum_{i=0} \left\{ R_{SNP} \times \left[limit\,{}_{0}^{P_{max}} P_0 \left(e^{\frac{i \times \Delta t_{SNP}}{\tau_{SNP}}} \right) \right] \times \Delta t_{SNP} \right\}$
S_{SPC}	$= \sum_{j=0} \left\{ R_{SPC} \times \left[limit\,{}_{0}^{D_{max}} D_0 \left(e^{\frac{j \times \Delta t_{SPC}}{\tau_{SPC}}} \right) \right] \times \Delta t_{SPC} \right\}$
S_{Total}	$= S_{SNP} + S_{SPC}$
A_S_{final}	$= CF_{combined} \times A\_COST_{Model}5_{Annual}$



Graph 1.1: Incremental cost saving contributed by SNP

1.8 Acronyms and Abbreviations

ANO	Authorized Nuclear Operators
ANSI	American National Standards Institute
APP	Authentication Pre-access Protocol
AQP	Authentication Qualification Protocol
BC	Basic Criteria
BP	Basic Proposition
CANDU	CANada Deuterium Uranium
CF	Contributing Factor
CM	Control and Maintenance
COMS	Constructable, Operable, Maintainable, and Safety
CSM	Cost Saving Model
DB	Design Basics
DSD	Dynamic Separation of Duty
FIPS	Federal Information Processing Standards
FLM	First Line Managers
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
IT	Information Technology
NCM	Nuclear Cost Model
NOAA	Nuclear Operation Access Authentication
OBAC	Operation-Based Access Control
RBAC	Role Based Access Control
RSA	Rivest Shamir Adleman public-key cryptosystems
SNP	Security-integrated Nuclear Process
SPC	Smart Process Controller
SRM	System-Responsible Managers
SSD	Static Separation of Duty
UOA	Unit Operating Authority

Chapter 2

SECURITY-INTEGRATED NUCLEAR PROCESS

Part 1: CONCEPTUAL DESIGN AND OPERATION-BASED ACCESS CONTROL

This chapter first presents a conceptual development and methodology for the control of accesses to a safety-critical process with network-based operations and second, presents a new design for secure and efficient access control to the safety-critical operation network.

There has not been absence of instances that many conceptual designs had failed or can never be implementable successfully with significant impacts on economic and technology advances, because they do not consolidate with practical details. In order to enhance the conceptual development and enrich the practicality of the methodology with details, the nuclear operations of safety-critical, infrastructure-critical, economic-critical, availability-critical, etc. are used for the evidence of its significances of the conceptual development presented in this chapter. This leads to the innovative development of ***SNP***, the *Security-integrated Nuclear Process* design and its key associated designs of ***OBAC*** - the *Operation-Based Access Control*, ***NOAA*** - the *Nuclear Operation Access Authentication*, ***APP*** - the *Authentication Pre-access Protocol*, ***AQP*** - the *Authentication Qualification Protocol*, etc.

This chapter presents the new design of ***OBAC***, as the first step in this thesis research for finding a new security-integrated access control to the new formation of the network-based nuclear process. The network-based process can be significantly benefited from the use of modern smart process control equipment with inter-networking capability for operation improvement, but simultaneously it can be challenged with network-induced cyber security risks leading to nuclear safety concerns. Any development related to the nuclear subject cannot be proceeded if there is any chance of affecting the nuclear safety even in a very minor and remote manner. For the objective of nuclear safety concerns-free and nuclear practices large scale improvement, this thesis develops the concept of the security-integrated network-based intelligent nuclear process termed as ***SNP***, the *Security-integrated Nuclear Process*. In this new SNP, any access to the operations and resources in the nuclear generating unit must pass two checks: the access authentication security check and the user experience and technical qualifications check. This chapter presents the specifications for the user experience and technical qualification check as part of the overall access control in the *OBAC*.

The *OBAC* is designed for the access control to the new network-based nuclear operations as created in this thesis research, first for the *CANDU* nuclear power electricity generating process as an essential step for realization of nuclear operations modernization. This is to provide the first tangible illustration of the implementable of this thesis' new design series (*SNP*, *OBAC*, *NOAA*, *etc.*) when the evaluation is with respect to a live nuclear environment, as a step advanced from the conceptual development because of carrying out any experiments in the live nuclear facilities is usually very limited. The base and the concept of these designs are not limited to *CANDU* nuclear application and the designs have a general architecture and a general network base structure, and therefore they are applicable for other nuclear facilities of using different nuclear technologies.

This chapter presents:

Section 2.1:	This section presents the conceptual development of a methodology for the control of access to a critical safety process with network-based operations.
Section 2.2:	This section presents the basic criteria and theories for the creation of the OBAC, and the architecture for the OBAC.
Section 2.3:	This presents nine modules for the OBAC access controls to the network-based nuclear operations, which include operation base module, core operations module, technical qualifications module, field-experience qualifications module, role-experience qualifications module, operation states module, work-orders module, nuclear users module and overall OBAC flow control module
Section 2.4:	This section presents the base specifications for the nuclear operation base, the core operations, the technical qualifications, the field experience qualifications, the role experience qualifications, the operation states, the work orders, and the nuclear users.
Section 2.5:	This section presents the *Hierarchies Specification* the OBAC Specifications, which include the *technical* qualification hierarchies, *field*-experience qualification hierarchies, and *role*-experience qualification hierarchies.
Section 2.6:	This section presents the specifications of *assignments* in the OBAC Specifications, which include role qualifications assignment, field qualifications assignment, and technical qualifications assignment.
Section 2.7:	This section presents the specifications for the mappings in the OBAC Specifications, which include the user-work mapping, the user-role qualifications mapping, the user-field qualifications mapping, and the user-technical qualifications mapping.

2.1 Conceptual Development for Safety-Critical Process Control Advancement

Objective:

Develop a methodology for the control of access to a safety-critical process operations network.

Circumstances:

The circumstances to be targeted are challenging, for example:

- Any error in the control of accesses to the safety-critical process would cause extremely serious consequences to public's health and safety and/or huge economical/infrastructure loss.
- Any error occurred in the control of the accesses is non-recoverable, as the accesses directly go to the live critical operations.
- The control of the accesses must be maintainable, modifiable, and upgradeable in practical terms as the operation conditions or the means for the operations may change in various magnitudes.
- The access control elements must be precisely defined in details, and the access specifications must be verifiable under all live operation conditions.
- Access controls to the live operations must be reliable, quality-controllable and clearly understandable to all network users so that the users will not make wrong accesses that possibly lead to disaster operations.
- Operation access controls must be reconfigurable and constructable under the real complex live operation environments. Otherwise the access controls may still stay in the conceptual stage or may not be practical at all and may never be implementable.

Exhaustive Research:

This thesis research has carried out exhaustive searches for the access control methodology that can satisfy the above-mentioned challenging circumstances. The findings with respect to the existing methodologies, standards, procedures, etc. partially have been mentioned in chapter 1 and are to be presented in this and subsequent chapters matching to the flow of materials presented in this thesis. Below is a highlight:

- RBAC, the *Role Based Access Control* would be the closest one for meeting the above-mentioned challenges, but it is still not able to satisfy the challenges in the targeted circumstances, with some typical reasons given below for illustration.
- RBAC, similar to most of the standard available access controls, are designed with the focus on the role base, as its name implies, primarily for data access and/or information management access, but not readily for live operations access principally lacking of guarantees in practical terms of verifiable, reconfigurable, reliable, quality-controllable, clearly understandable, maintainable, constructable, modifiable, upgradeable, etc. as challenged above.
- The role-based access controls, in general, if without enforcement through complex control loops of static separations of duty, dynamic separations of duty, layers of hierarchy, etc., would lead to users granted with over-privileges or lead to loose access control in the live operations. On the other hand, the role-based access controls when enforced with complex control loops would result in unaffordable time delays for live operations/during an operation event, or would result in some undiscovered/untestable grey operation areas due to complex control loops. This thesis recommends that complex access controls shall not be used.
- The role-based access controls for live operation applications if not to be stretched back to the lengthy access list form, seems unavoidable to be implemented with complex control loops in order to be sufficiently able to handle the real live operations. Access controls implemented with complex control loops may not comply with the safety-critical industries standard of requiring control systems/equipment to be *COMS* (Constructable, Operable, Maintainable, and Safety) due to complex control loops. However, the weakness of the access list approach has been demonstrated in the literatures.
- The role-based access controls, regardless of the complexity that may be involved, would not sufficient and not quite appropriate for live operation applications, because having a higher-hierarchy role, the users may not be appropriate or allowed to access the same live operations as some users with low hierarchy role, for example engineering authority personnel of much higher hierarchy role than a pump technician can authorize any pump operation for the technician but themselves may not be permitted to access the operation network for carrying out the pump work if they do not have pump-work qualifications or their qualifications are not current.

Design Basics:

This thesis research carries out a conceptual development and methodology for the control of access to a safety-critical process with network-based operations. The following lays out the design concepts, the development strategies, and the Design Basics (***DB***):

1. *Modularization of safety-critical operations*

In order to efficiently execute the safety-critical operations and effectively make error-free accesses to the operations, the core operations are classified into modules. The classifications of industrial control processes may encounter various degrees of difficulties if this applies to legacy process control equipment and systems as these systems may be specifically designed and some of their functions are merged together. For these legacy equipment and systems, apply the modular classifications to the best possible level. Fortunately, these legacy equipment and systems are obsolete and being replaced with smart systems with networking and configurable capabilities that are readily available to be transformed by modular classifications.

DB-1: *Classify the safety-critical operations into Modules: for typical complex facilities that may be divided downwards from process divisions, to divisional systems, system equipment, control devices, etc. down to device functions.*

2. *Classification of Core operations and functions*

Even though most of the industrial control processes are of various levels of complexities, the core operations of the control processer however have various degrees of similarities that can be classified into groups. The control process core operations can be, in general, classified into 5 groups, as follows:

DB-2: *Classify the safety-critical operations into 5 groups: Monitoring, Processing, Controlling, Verifying, and Supervising Core Operation Functions.*

The monitoring core operation is to monitor the industrial process systems/equipment/devices performance; the processing core operation is to analyze the data collected from the industrial process controls; the controlling core operation is to control and adjust the operations of the facilities; the verifying core operation is to verify/approve the changes of the facilities; and the supervising core operation is to observe/supervise all key operations in the facilities.

3. *Static constraints for accesses to network-based core operations*

Access to the direct core operations of safety-critical, infrastructure/economical critical, and time-of-operation critical facilities must be precisely controlled with well-defined constraints. The constraints can be grouped into static or dynamic/transient constraints. The constraints of both static and dynamic are to be continuously updated according to the changes of the operating conditions or elements. The static access constraints can be classified as follows:

DB-3: *Classify the static access constraints into 3 typical requirement groups of Technical qualifications, Field experience qualifications, and Role operating experience qualifications. Identify the levels of qualifications required for specific operations.*

Users who are qualified to make accesses directly to the core operations of the critical facilities must in general have sound credentials, up-to-date technical trainings, sufficient field experiences, ample role operating experiences, etc. However, the level of qualifications requirement depends on the kind of live operations are accessed to perform.

4. *Operating states and dynamic constraints for accesses to live operations*

As the operating conditions change, the restrictions of the access to the direct core operations have to be changed. The dynamic constraints for core operation accessed depend on the states of the operations of the facilities, defined as follows:

DB-4: *Monitor the state of the live operation of the facilities and then determine which accesses to the core operations are allowed as well as their corresponding dynamic constraints.*

5. *Pre-access authentication to live operation network*

Any access to the live operations must pass two checks: one is the pre-access authentication security check; the other is the user pre-operation authentication experience and technical qualifications check. The pre-access authentication is the first and the most important security control as a necessary measure for preventing or rejecting unauthorized network access, which is defined as follows:

DB-5: *A mutual (two-way) authentication shall be used between the users and the network authentication server for the pre-access authentication to prevent unauthorized accesses. The users can ensure that they are not communicating with a malicious authentication server by authenticating the server, and the authentication server can ensure that it is not communicating* *with a malicious user by authenticating the user. Public-private key-based authentication shall be used in the pre-access authentication, and authentication shall use random number challenges and digital signatures.*

6. *User qualifications authentication for accesses to core operations*

The user qualifications authentication takes action after the user passed the pre-access authentication and already entered the core operation network, then a quick authentication process is carried out, as follows:

DB-6: *A unilateral authentication shall be used between the users and the operation network authentication server for the users' technical, field-experience, and role-experience qualifications authentication. Authentication shall be high efficient for authentication of qualifications and data transmissions to minimize the delays during the live operations.*

Conceptual Design Realization:

The conceptual design according to the design basics can be realized as shown in Figure 2.1.

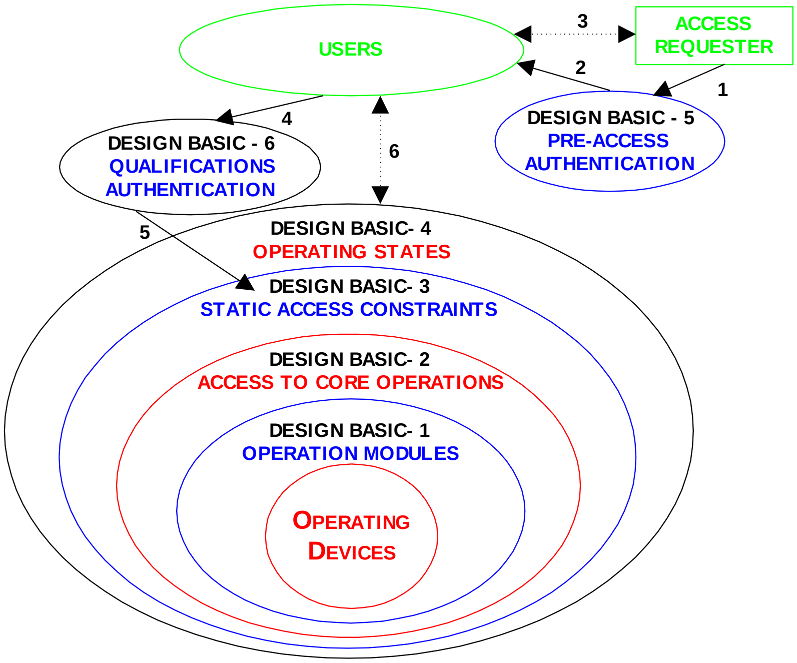


Figure 2.1: Conceptual design

Figure 2.1 shows that a requester for access to the operation network starts with the pre-access authentication (1). After the pre-access authentication is past, the access requester receives an access code and becomes a network user (2). Then, the access requester uses the access code and can enter or exit the network (3).

The users can request to access the operations by authenticating their qualifications with respect to their technical knowledge, field and role experiences (4). After the qualification authentication is past, the users receive access codes and can access the live operations (5). Then, the users use their access codes and can access or exit the operations.

Conceptual Design Validation:

In order to enhance the conceptual development and enrich the methodology for network-based live operations and the associated access controls, the conceptual designs need to be validated with real applications of the similar degree of complexity. The nuclear operation can be chosen for the validation as the nuclear operation is of human-safety-critical, infrastructure/economical critical, time-of-operation critical, etc. The validation has to have representative details as many conceptual designs fail to consolidate practical details and never be implementable with significant impacts on technology advances.

This thesis research selects the nuclear operation for the proof of the significances of the above-mentioned conceptual designs. This leads to the innovative development of ***SNP***, the *Security-integrated Nuclear Process* design and its key associated designs of ***OBAC*** **-** the *Operation-Based Access Control*, ***NOAA*** **-** the *Nuclear Operation Access Authentication*, ***APP*** **-** the *Authentication Pre-access Protocol*, ***AQP*** **-** the *Authentication Qualification Protocol*, etc. All of these designs are to be presented in this thesis.

2.2 Operation-Based Access Control (OBAC)

This section is focused on the development of ***OBAC***, the *Operation-Based Access Control* for the secure control to the nuclear process operation network.

For validation and consolidation of the conceptual development presented in the previous section 2.1, some of its supporting materials are utilized for the formation of the basic criteria and theories for the creation of the OBAC and the architecture for the OBAC presented in this section.

2.2.1 *Basic Criteria for Creation of OBAC*

In order to develop a secure access control for the new conceptual full-scale network-based nuclear process operations, criteria for the development have to be first established to satisfy the nuclear practice requirements. The following establishes the *Basic Criteria* (*BC*) and *Basic Proposition* (*BP*) for the creation of this thesis' new design of ***OBAC***.

- ***BC-1****: Access controls must be designed on the absolute requirement of error-free direct nuclear operations access*.

  Reasoning:

  - No error in access controls is tolerable, as any error may have adverse impacts on nuclear safety that may cause extremely serious consequences to public and employees' health and safety.
  - Any error occurred is almost non-recoverable, as the access directly goes to the live nuclear operations. Even though the error may be controllable by other means before any massive damages are caused, but the design of the access controls is required to be error-free.
  - Most of the standard available access controls, e.g. RBAC, are designed on the role base for data access and information management access, but not readily for live operations access.
  - Small portion of access controls relate to operations but they are likely embedded inside the equipment system with manufacturer specific embedment but not accessible or extendable.

BP-1: *Effective and reliable nuclear operations access control roots to operation base*.

Conforming:

- Role-based access controls if without enforcement through complex control loops of static separations of duty, dynamic separations of duty, layers of hierarchy, etc., would lead to users granted with over-privileges or lead to loose access control in the live operations; role-based access control if enforced with complex control loops would result in unaffordable time delays for on-line operations/during nuclear events or result in some undiscovered/untestable grey operation areas due to complex control loops. Complex access controls are not used in this thesis' new OBAC access control to be shown in sections 2.2 to 2.6.

- Operation-based access modules given in section 2.2 are to illustrate the simple, reliable and effective operation access controls that are to be built based on the nuclear core operations directly, not through roles as media, where the role becomes one of the qualification requirements that is to be detailed in section 2.2.

- ***BC**-2: Access control logics must be designed as simple and straightforward as possible, on the requirement of easy-of-maintainable, modifiable, upgradeable access control logics.*

Reasoning:

- Access controls for operations are required to be maintained regularly, especially when the operation conditions change or equipment/devices are replaced. Therefore access control logics not only must be maintainable but also must be easy to maintain and as a rule of thumb, the simpler the logic the easier it can be maintained.
- Operational access control logics needs to be upgraded from time to time, as operation obstacles or operation issues may occur unpredictably and need to be resolved rapidly. Access control logics must be upgradable, but not requiring a complete replacement that will be very costly (not due to replacement cost but due to consequently production interruption and loss of revenue).

***BP**-2: Maintainable, modifiable and upgradeable nuclear access control roots to modular, simple, single-loop control logics.*

Conforming:

- Role-based access controls for nuclear operations application if not to be stretched back to the lengthy access list form, seems unavoidable to be implemented with complex control loops of static separations of duty, dynamic separations of duty, hierarchies, etc. in order to sufficiently handle the real live nuclear operations. Access controls implemented with complex control loops may not comply with the nuclear generation facilities' standard of requiring control systems/equipment to be *COMS* (Constructable, Operable, Maintainable, and Safety) due to complex control loops. Complex access control loops are not used in the new OBAC, to be shown in sections 2.2 to 2.6.

  - Modular operation-based access controls (in section 2.2) and modular control specifications (in sections 2.3 to 2.6) provide easy-of-maintainable, modifiable, and upgradeable nuclear access controls that also comply with the nuclear standard of *COMS*.

- ***BC****-3: The access control elements must be precisely defined in details, and the access specifications must be verifiable under all on-line nuclear operation conditions.*

  Reasoning:

  - Access controls must be precisely defined covering all operation areas, because ambitious access controls can cause serious damages to nuclear equipment/systems, interruptions to electricity generation, significant loss of revenue (≈ $1M per day for some nuclear units), or even can endanger nuclear workers' safety, neighbouring residents' health, and environment.
  - Access control specifications must be verifiable to ensure the correctness of the access controls for all operating conditions. Verification is essential for approving changes on the access specifications due to changes of operating conditions or replacements of nuclear equipment/systems. Any unverifiable portion of the access specifications could lead to operation errors that may have serious consequences.

BP*-3: Verifiable access controls roots to precise specifications and simple control logics/algorithms.*

Conforming:

- Role-based access controls with implementation of complex control loops of static separations of duty, dynamic separations of duty, hierarchies, etc. (unavoidable for covering all nuclear operations) would be difficult to be verified, particularly limited by the constraints of the nuclear operations to carry out the exhaustive verifications. This would not affect the new design OBAC as this design does not employ complex control specifications and only use simple specifications to be illustrated in section 2.2 to 2.6.
- The new OBAC is designed in modular forms, breakdowns the complex nuclear processes into 5 simple divisions, groups the complex nuclear operations into 5 simple core operations, gathers the complex conditions of accesses into 3 qualification types, etc. These are to be demonstrated in sections 2.2 to 2.6.

- ***BC**-4: The access controls must be reliable, quality-controllable, comprehensible, reconfigurable, and constructable.*

  Reasoning:

  - Access controls to nuclear operations must be reliable, quality-controllable and clearly understandable to all nuclear users so that the users will not make wrong accesses that possibly lead to disaster operations.
  - Operation access controls must be reconfigurable and constructable under the real complex live nuclear operation environments. Otherwise the access controls may still stay in the conceptual stage or may not be practical at all and may never be implementable.

  ***BP**-4: The access controls of reliable, quality-controllable, reconfigurable and constructable attributes roots to precise and simple access specifications.*

  Conforming:

  - Role-based access controls use the complex constraint algorithms of static separations of duty, dynamic separations of duty, hierarchies, etc. on the role base to regulate the quality control of the accesses. However regardless of the complexity, this is not sufficient and not quite appropriate because with the same role and the same role constraints, the users may not be appropriate to access the same nuclear operations. Typically, a chief engineer or an operation authority can approve/authorize almost all nuclear operations but themselves may not be qualified to carry out an elementary task such as an adjustment of a control valve or a simple change of a pump control configuration if they do not have the current trainings required for the task or their trainings are expired.
  - OBAC is the operation based access control built directly upon the core nuclear operations and facilitates the quality control of the accesses. The OBAC defines three types of qualification requirements that are directly tied with the core operations to provide correct and effective quality controls of the operation network access, as detailed in section 2.3.

2.2.2 *Architecture for OBAC*

A simplified architecture of this new nuclear operations access control is shown in Figure 2.2. This figure shows that the *operation* is the focus of this new access control design, and therefore it is termed as **OBAC**, the *Operation-Based Access Control*.

Figure 2.2 shows that the *operation* access controls for this thesis created SNP operation network are built up from the *operation base* on nuclear devices, the *core operations* access control, the *operation state* access control, and the *operation work-order* access control. There are *constraints* for access to the core operations. For the users to access the nuclear operations, there are *authentication* to validate the qualifications and authorizations of the users' access requests.

The access control of OBAC is to be detailed below.

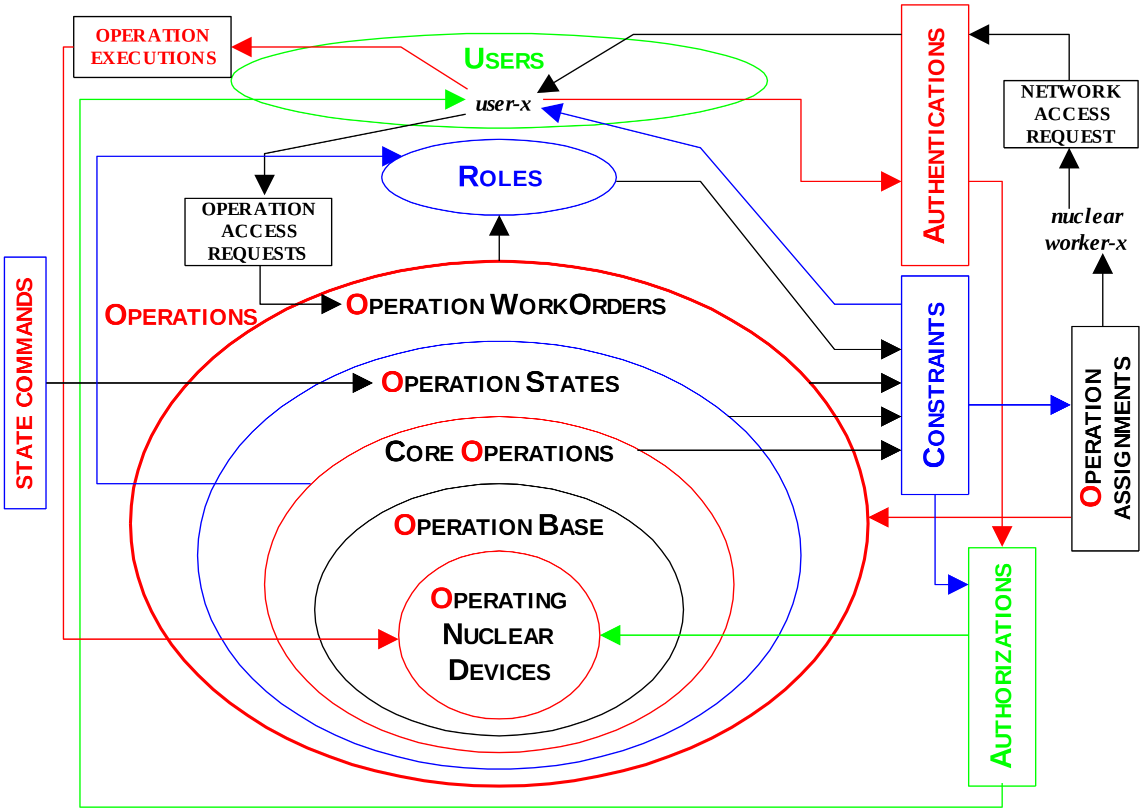


Figure 2.2: **OBAC** architecture

2.3 OBAC Modules

This presents nine (9) modules for the OBAC access controls to the network-based nuclear operations, which include operation base module, core operations module, technical qualifications module, field-experience qualifications module, role-experience qualifications module, operation states module, work-orders module, nuclear users module and overall OBAC flow control module.

Module-1: ***Operation Base*** *module for Access Controls*

Module-1 is defined for the new nuclear network *operation base* that consists of 5 nuclear process divisions for each nuclear unit (one unit has one nuclear reactor), based on this thesis findings from the current live nuclear station facilities and practices. The 5 nuclear process divisions are: Division 1 - the calandria and moderator operations; Division 2 - the primary heat transport and heavy water operations; Division 3 - the boiler and steam operations; Division 4 - the turbine and generator operations, and Division 5 - the condenser and light water operations, as shown in Figure 2.3.

Division 1 has 10 nuclear moderator control systems (e.g. the reactor flux monitoring system, main moderator control system, liquid zone control systems, etc.); Division 2 has 8 control systems; Division 3 has 8 control systems; Division 4 has 8 control systems; and Division 5 has 10 control systems. Each nuclear control system in each nuclear division contains many equipment and each equipment has a number of control devices. Therefore, for an 8-unit nuclear generating station, there are thousands of monitoring, processing, and controlling devices. Network modules are developed for handling the operations of these devices. Module-1, the operation base is defined precisely through its specifications, *BaseSpec.-1* in section 2.2.

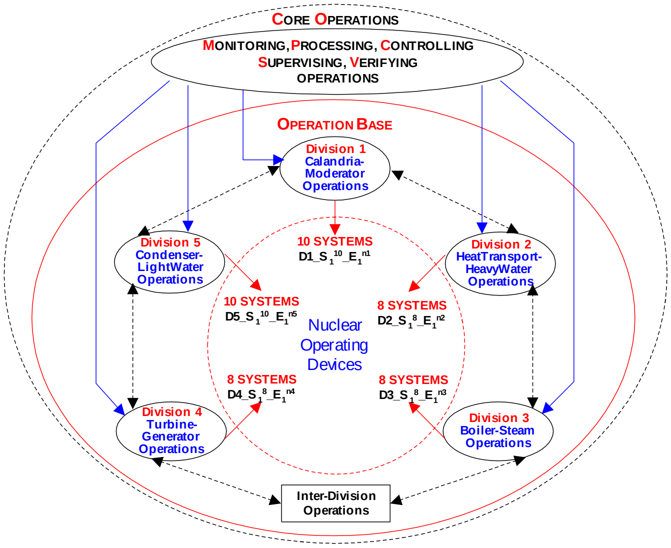


Figure 2.3: Nuclear core operation access controls

Module-2: ***Core Operations** module for Access Controls*

Module-2 is defined for the 5 *core operations* access control in the nuclear process network developed in this thesis based on investigations on the actual operating functions of the nuclear devices. The 5 groups of the core operations are: the nuclear equipment performance monitoring, the nuclear data processing, the nuclear equipment controlling, the nuclear device change verifying, and the nuclear system supervising, as shown in Figure 2.4. Each group has many operations that are to be detailed in chapter 4. These core operations have their unique access controls, covering all essential nuclear-to-electrical power generation controls.

This core operation access control maps the operation states access control (Module-3) to the operation base (Module-1) nuclear devices. The mapping of each of the 5 core operation accesses to any nuclear device in any nuclear division has defined access requirements/constraints in order to ensure the qualified/authorized access to the nuclear operating device that may bear impacts on the nuclear safety and serious consequences if the device is not operated correctly.

Module-2, the core operation is defined precisely through its specifications, *BaseSpec.-2* in section 2.2.

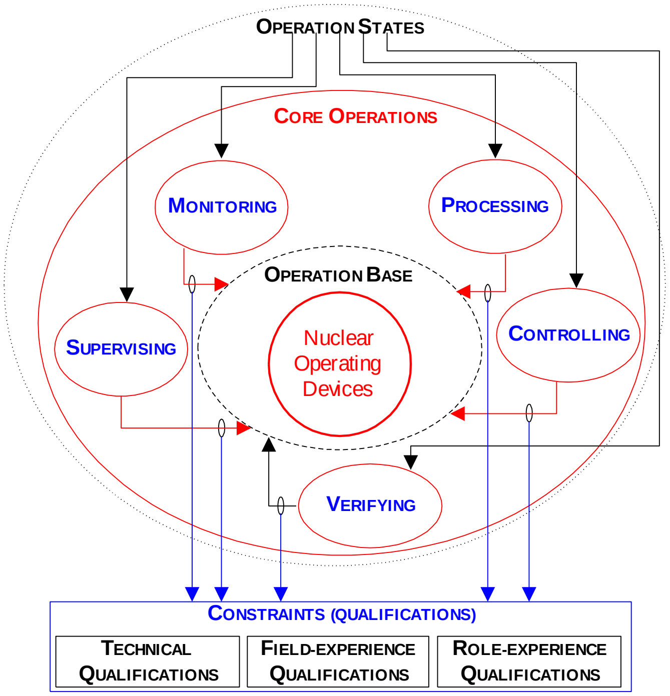


Figure 2.4: Nuclear core operation access controls

Module-3: **Technical Qualifications** *module for Access Controls*

Module-3 is defined for the *technical qualifications* requirement for the core operations access to the operation base nuclear devices for carrying out operations. There are 5 groups of core operations as shown in Figure 2.5, and each group has hundreds of nuclear devices and operations. Each operation has its own technical qualifications requirement that is specified from the nuclear training data base.

The nuclear trainings can be grouped into 4 groups: TG1 – nuclear awareness trainings; TG2 – nuclear practices trainings; TG3 – nuclear system process trainings; and TG4 – nuclear technologies trainings, as shown in Figure 2.5. Each training group has many training courses and passing a course, the nuclear worker is awarded with the certificate of that course. For example, TG1 has a total of 35 courses (10 courses in nuclear worker general awareness trainings, 10 courses in nuclear safety awareness trainings, and 15 courses in nuclear information, cyber security, OPEX awareness trainings); TG2 has 29 courses; TG3 has 25 courses, and TG4 has 31 courses. The information of the training courses is to be given in chapter 4.

Module-3, the technical qualifications requirement is defined precisely through its specifications, *BaseSpec.-3* in section 2.2.

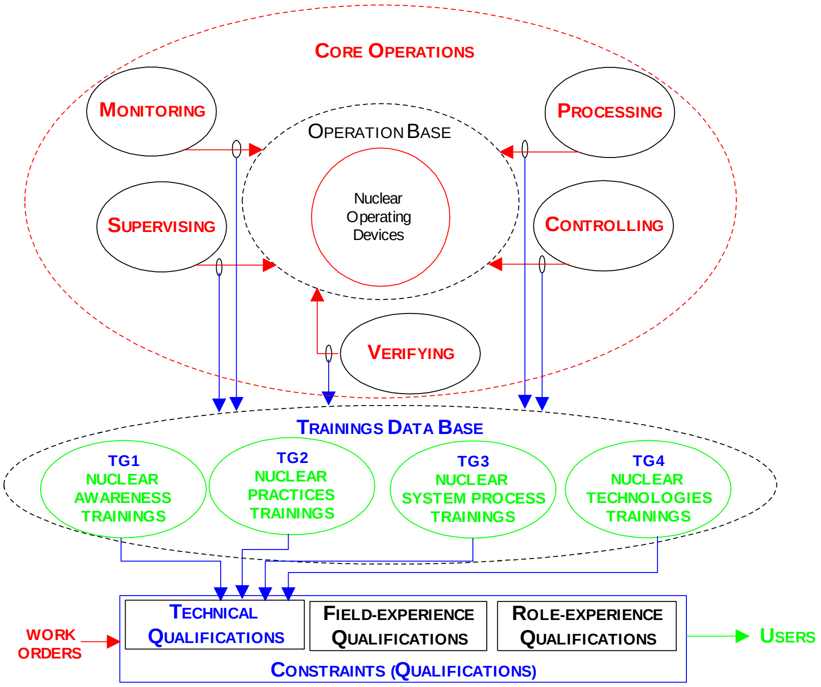

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
TRAININGS DATA BASE
TG1 NUCLEAR AWARENESS TRAININGS
TG2 NUCLEAR PRACTICES TRAININGS
TG3 NUCLEAR SYSTEM PROCESS TRAININGS
TG4 NUCLEAR TECHNOLOGIES TRAININGS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.5: Technical qualifications for core operation access controls

Module-4: ***Field-Experience Qualifications*** *module for Access Controls*

Module-4 is defined for the *field-experience* qualifications requirement for the core operations access to the operation base nuclear devices for carrying out operations. The field-experience qualifications can be assembled into 5 groups: FG1 – on-line divisional-level op-exp., FG2 – on-line system-level op-exp., FG3 – on-line critical equipment op-exp., FG4 – on-line non-critical equipment op-exp., and FG5 – outage maintenance op-exp., as shown in Figure 2.6. The nuclear worker is awarded with a certificate for each of the worker's field operation experiences got approved. For example, FG1 has a total of 7 recognized field operation experiences (on-line reactor regulating operations, on-line reactor shutdown operations, on-line moderator regulating operations, etc.); FG2 has 43, FG3 has 4, FG4 has 4, and FG5 has 7 recognized field operation experiences. The information of the recognized field operation experiences is to be provided in chapter 4. There are 5 groups of core operations as shown in Figure 2.6, each group has hundreds of nuclear devices and operations, and each operation has its own field-experience qualifications requirement that is specified from the field experiences data base.

Module-4, the field-experience qualification requirement is defined precisely through its specifications, *BaseSpec.-4* in section 2.2.

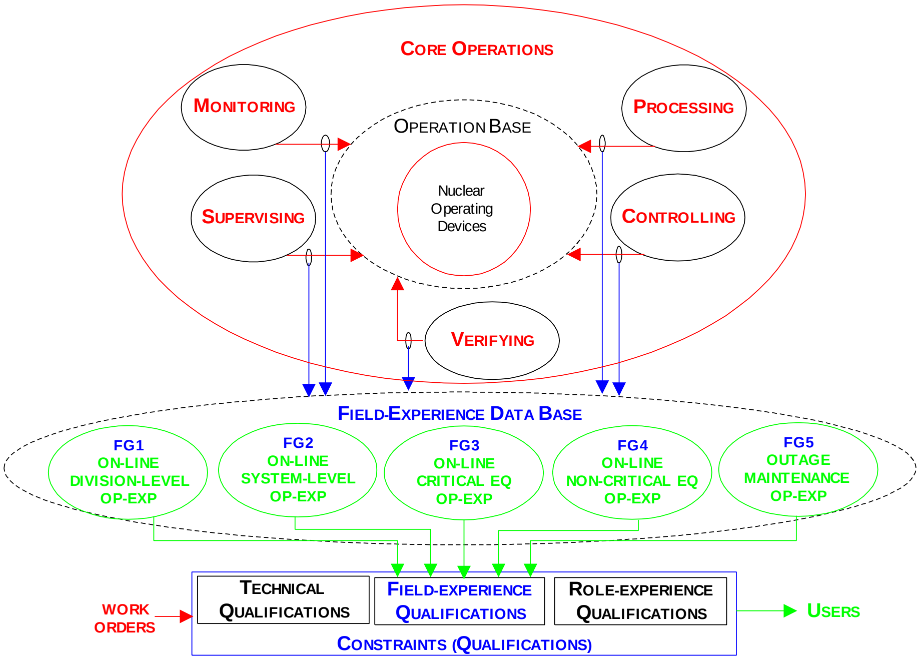

CORE OPERATIONS
MONITORING
OPERATION BASE
PROCESSING
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.6: Field-experience qualifications

Module-5: ***Role-Experience Qualifications*** *module for Access Controls*

Module-5 is defined for the *role-experience* qualifications requirement for the core operations access to the operation base nuclear devices for carrying out operations. There are 3 major groups of nuclear roles: Operation group, Engineering group, and Control Maintenance group, as shown in Figure 2.7.

Within the Operation major group, there are Operation Authorities group, Control Room Supervisors group, ANO (Authorized Nuclear Operators) group, etc. Within the Engineering major group, there are Engineering Authorities group, Design Engineers group, Field Engineers group, Project Engineers group, Training Officers group, etc. Within the Control Maintenance (CM) major group, there are CM Supervisors group, Technologists group, Control Technicians group, Maintenance Technicians group, Installation Technicians groups, etc. Each of the 5 core operation groups has hundreds of nuclear devices and operations, and each operation has its own role-experience qualifications requirement that is specified from the role experiences data base.

Module-5, the role-experience qualification requirement is defined precisely through its specifications, *BaseSpec.-5* in section 2.2.

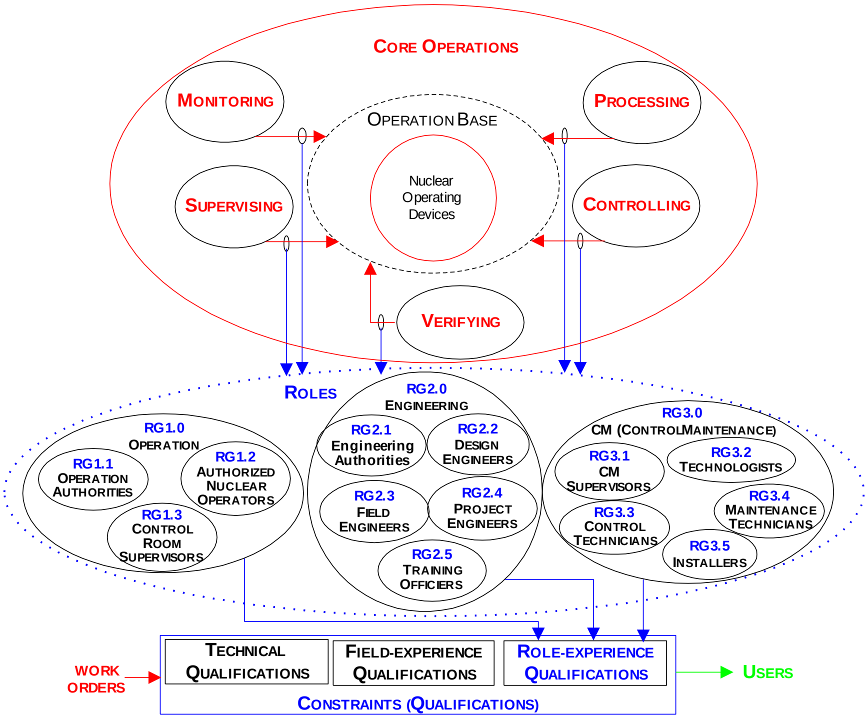

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
ROLES
RG2.0 ENGINEERING
RG1.0 OPERATION
RG1.1 OPERATION AUTHORITIES
RG1.2 AUTHORIZED NUCLEAR OPERATORS
RG1.3 CONTROL ROOM SUPERVISORS
RG2.1 Engineering Authorities
RG2.2 DESIGN ENGINEERS
RG2.3 FIELD ENGINEERS
RG2.4 PROJECT ENGINEERS
RG2.5 TRAINING OFFICERS
RG3.0 CM (CONTROLMAINTENANCE)
RG3.1 CM SUPERVISORS
RG3.2 TECHNOLOGISTS
RG3.3 CONTROL TECHNICIANS
RG3.4 MAINTENANCE TECHNICIANS
RG3.5 INSTALLERS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.7: Nuclear roles for access controls

Module-6: ***Operation States** module for Access Controls*

Module-6 is defined for the 4 *operation states* access control in the nuclear process network, designed based on the current nuclear operating practices. The four nuclear operation states shown in Figure 2.8, are: the routine operations when the nuclear unit is generating electricity in its normal way, the emergency operations when there is a nuclear event or a major equipment failure, the on-line maintenance when a nuclear device is not functioning properly but not affecting the normal operation of the nuclear reactor or the normal generation of electricity, and the outage maintenance when the nuclear reactor is shut down with no electricity generation and the nuclear unit is undergoing maintenance during either a scheduled outage or a forced outage.

The current operation state is the condition of the nuclear unit is being operated (in only one of: routine state, emergency state, on-line maintenance or outage maintenance state). The change of the operation states in the nuclear network access control is commanded by the nuclear unit control center based on the actual operating condition. The users have no access to the state command unit. The work order operation access requests from the users have to pass the check of the operation state access control in order to be able to access the core operations. Certain work orders are not allowed to be carried out for some states of the nuclear unit in operation.

Module-6, the operation states control is defined precisely through its specifications, *BaseSpec.-6* in section 2.2.

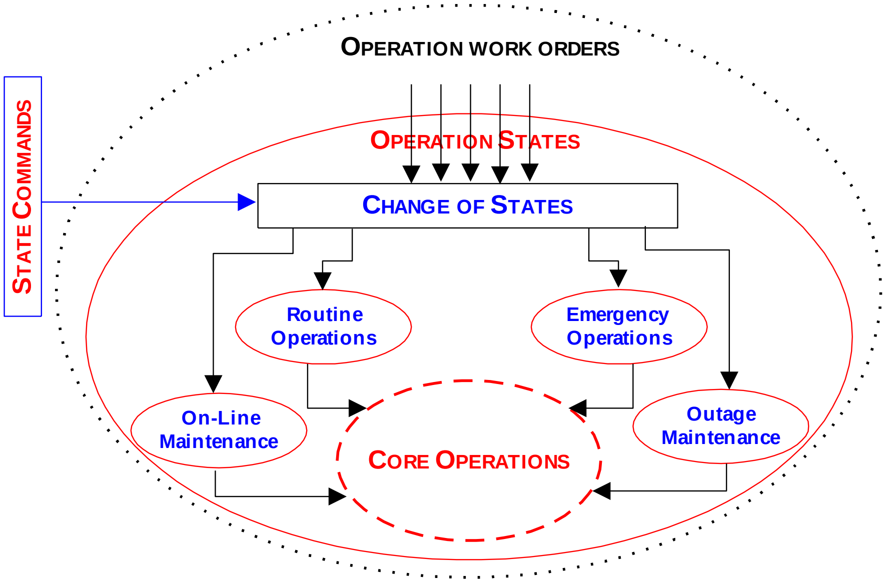


Figure 2.8: Nuclear operation state access controls

Module-7: ***Work Orders module*** *for Access Controls*

Module-7 is defined for the 5 operation *work orders* access control in the nuclear process network, the same as the core nuclear operations grouped based on the current nuclear practices. The 5 nuclear work order groups, as shown in Figure 2.9, are: the nuclear equipment performance monitoring work orders, the nuclear data processing work orders, the nuclear equipment controlling work orders, the nuclear device change verifying, and the nuclear unit supervising work orders.

According to the continued monitoring of the nuclear unit operating conditions and equipment performance, and based on recommendations from the authorized nuclear operators (ANO), control-maintenance first line managers (FLM), system-responsible managers (SRM) and engineering managers, the nuclear unit operating authority (UOA) determines if any new operation actions are required and if required, the authority is to set the directions, completion time lines, allocation of resources, etc. With the joint efforts from the project departments, engineering departments, operation departments, and CM departments, operation assignments are detailed to execute the actions outlined by the UOA. The operation assignments are turned into operation work orders as shown in Figure 2.9.

Module-7, the operation work order access control is defined precisely through its specifications, *BaseSpec.-7* in section 2.2.

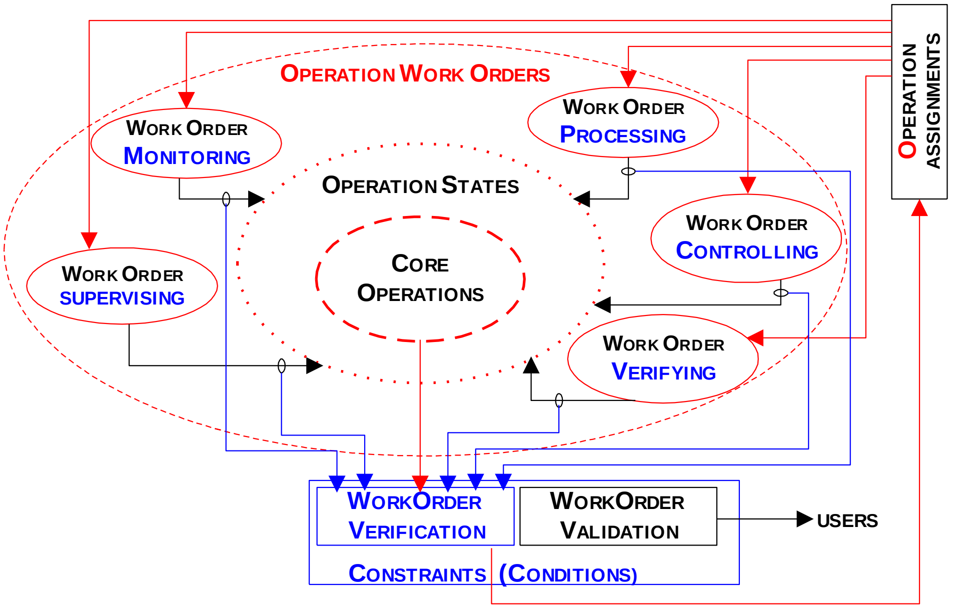


Figure 2.9: Operation work orders assignment

Module-8: – ***Nuclear Users*** *module for Access Controls*

Module-8 is defined for the nuclear *users* access control, as shown in Figure 2.10. The operation assignment authority assigns the operation tasks/work orders to the nuclear worker/user. The user makes an access request to the operation work order system where it has defined validation requirements, to ensure eventually the proper access to the nuclear device with no impact on the nuclear safety. The validation is to compare each work order of any operation type with the corresponding operation registered in one of the 5 groups of nuclear core operations. If the work-order operation requested by a nuclear user matches with the registered operation in the core operation data base, then the work-order operation is validated.

The constraints associated with the work order are fed back to the user. The user then sends the information for authentication in order to satisfy the constraints. After all constraints are satisfied, the work order is authorized. Finally the user starts to execute the work order operation.

Module-8, the nuclear users access control is defined precisely through its specifications, *BaseSpec.-8* in section 2.2.

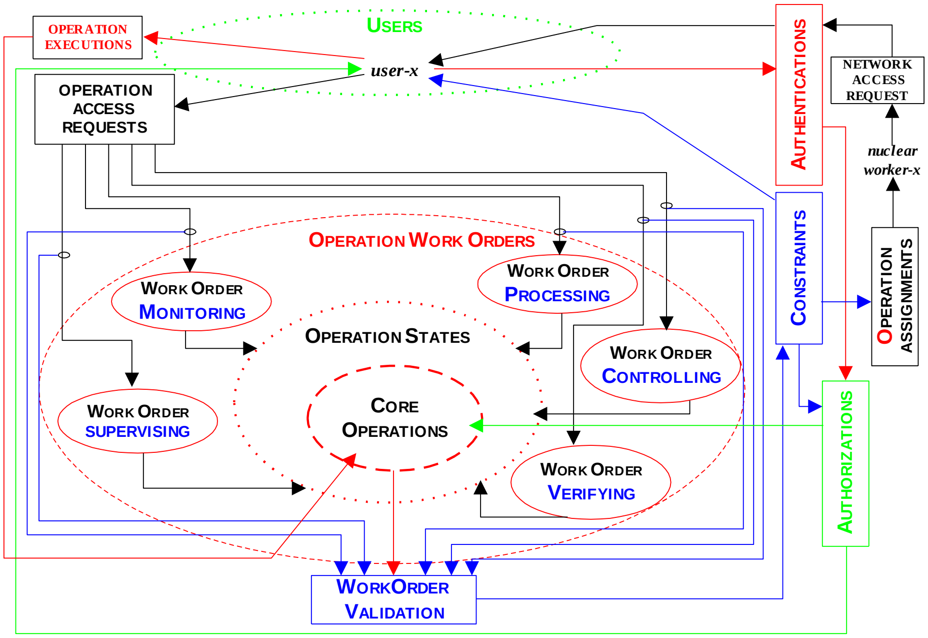


Figure 2.10: User access control

Module-9: ***Overall OBAC Flow Control*** *module for Access Controls*

Module-9 is defined for the overall OBAC access flow control. The flow of the access control in *OBAC* is numbered in Figure 2.11. Starting with the assignment of operation work orders, the operation network may be checked (1) to get information of the current constraints/requirements for the work order to be assigned (2). The operation work order is to assign to the nuclear worker-*x* (3). The nuclear worker-*x* makes a network access request (4) and carries out pre-access authentication (see chapter 3) to validate the worker's access legitimacy (5) and then the worker-*x* enter into the nuclear operation access network and becomes an authorized nuclear network user-*x* (6). The user-*x* makes an operation access request (7) to check the operation work-order access control (8) that generates the work-order validation and feedbacks as constraints (9). The operation work order access is mapped to the operation states that controls the work order access to the nuclear core operations and feedbacks as constraints (10). The work order is then mapped to the core operation access and generates the technical, field-experience and role-experience qualification requirements and feedbacks as constraints (11) and (12). Then all the access constraints/requirements are sent back to the user-*x* (13) to request for satisfying these access requirements. The user-*x* sends his/her qualification certificates for satisfying the access requirements to the authentication server (14). The server verifies the user-*x*' certificates and if they are verified (15), the authenticated certificates are sent to the authorization server where they are checked against the operation access requirements (16). If the check is passed, the authorization server informs the core nuclear operation control (17) and sends an operation-access permit to the user-x (18). The permit allows user-x to make work order operation execution (19) and finally user-x can access to the nuclear operation network to execute their assigned work orders (20).

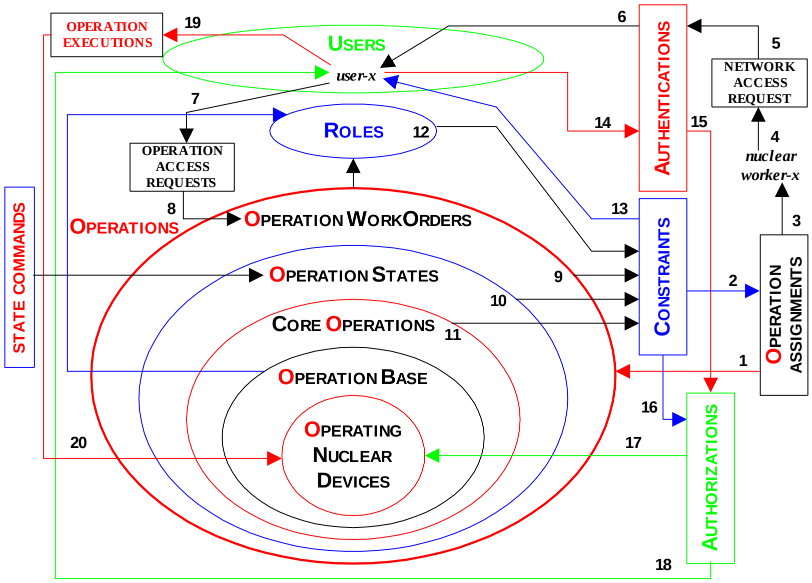


Figure 2.11: OBAC flow of access controls

2.4 OBAC Base Specifications

This section presents the *Base Specifications* in the OBAC Specification Series that consists of base specification, hierarchy specification, assignment specification, and mapping specification.

As the specifications for the RBAC (*Role Base Access Control*) has been rooted and widely accepted, the specifications presented here assume some of the RBAC formats for convenience, but with significant simplifications and extensions in order to cover the needs for the nuclear operation network access controls whereas the RBAC falls short of.

This section presents the base specifications for the nuclear operation base, the core operations, the technical qualifications, the field experience qualifications, the role experience qualifications, the operation states, the work orders, and the nuclear users.

BaseSpec.-1*:** ***Operation Base *specification*

BaseSpec.-1 defines the specifications for the elements in the nuclear *operation base* (Figure 2.3)

The specifications cover the elements for the inter-division, divisional system, equipment and device operations in the nuclear process.

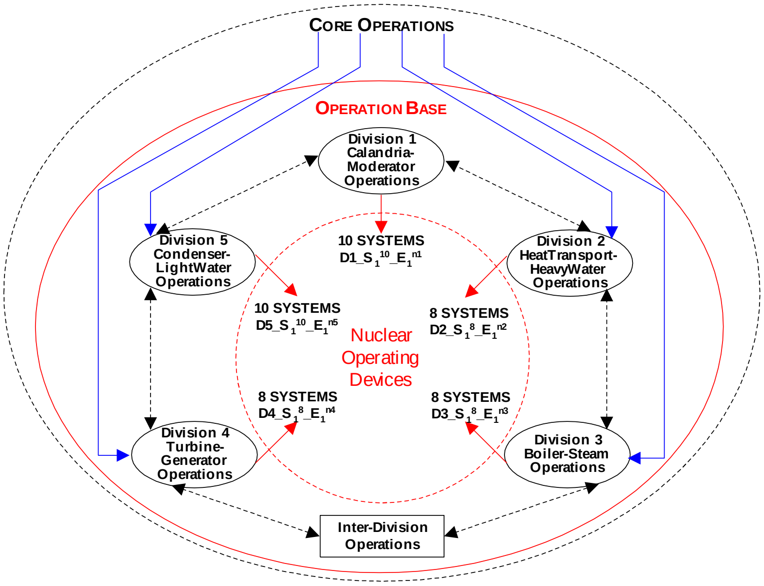

CORE OPERATIONS
OPERATION BASE
Division 1 Calandria-Moderator Operations
Division 5 Condenser-LightWater Operations
Division 2 HeatTransport-HeavyWater Operations
10 SYSTEMS
D1_S$_1$^{10}_E$_1$^{n1}
10 SYSTEMS
D5_S$_1$^{10}_E$_1$^{n5}
8 SYSTEMS
D2_S$_1$^{8}_E$_1$^{n2}
Nuclear Operating Devices
8 SYSTEMS
D4_S$_1$^{8}_E$_1$^{n4}
8 SYSTEMS
D3_S$_1$^{8}_E$_1$^{n3}
Division 4 Turbine-Generator Operations
Division 3 Boiler-Steam Operations
Inter-Division Operations

Figure 2.3: Nuclear core operation access controls

- *Data Sets*: Below defines the data sets for the nuclear network operation base.

$IDIVS\{(div_i, div_j, sys)\}$: INTER_DIVISION where div_i, div_j=divisions
$SYSTS\{(div, sys)\}$: SYSTEM where div = division, sys = system
$EQUPS\{(eqp, com)\}$: EQUIPMENT where eqp = equipment, com = component identity
$DEVIS\{(div, sys, eqp, com)\}$: DEVICE

- *Inter-Division elements*

AddInDiv: This command is to create a new nuclear divisional element in the OBAC operation base. The command is valid only if the new element is not already a member of the data set *IDIVS*. The set is to be updated. The following schema describes this command:

$AddInDiv(div_i, div_j, sys: ALPHANUMERIC)$
$(div_i, div_j, sys) \notin IDIVS$
$IDIVS' = IDIVS \cup \{(div_i, div_j, sys)\}$

DeleteInDiv: This command is to delete an existing nuclear divisional element from the OBAC operation base. The command is valid only if the divisional element to be deleted is a member of *IDIVS*. The following schema describes this command:

$DeleteInDiv(div_i, div_j, sys: ALPHANUMERIC)$
$(div_i, div_j, sys) \in IDIVS$
$IDIVS' = IDIVS \setminus \{(div_i, div_j, sys)\}$

- *System elements*

AddSystem: This command is to create a new nuclear system element in the OBAC operation base. The command is valid only if the new system element is not already a member of the data set *SYSTS*. The set is to be updated. The following schema describes this command:

$AddSystem(div, sys: ALPHANUMERIC)$
$(div, sys) \notin SYSTS$
$SYSTS' = SYSTS \cup \{(div, sys)\}$

DeleteSystem: This command is to delete an existing nuclear system element from the OBAC operation base. The command is valid only if the system element to be deleted is a member of *SYSTS*. The following schema describes this command:

$DeleteSystem(div, sys: ALPHANUMERIC)$
$(div, sys) \in SYSTS$
$SYSTS' = SYSTS \setminus \{(div, sys)\}$

- *Equipment elements*

AddEquip: This command is to create a new nuclear equipment element in the OBAC operation base. The command is valid only if the new equipment element is not already a member of the data set *EQUPS*. The set is to be updated. The following schema describes this command:

$$\begin{array}{l} AddEquip(eqp, com{:}\,ALPHANUMERIC) \\ \quad (eqp, com) \notin EQUPS \\ \quad EQUPS' = EQUPS \cup \{(eqp, com)\} \end{array}$$

DeleteEquip: This command is to delete an existing nuclear equipment element from the OBAC operation base. The command is valid only if the equipment element to be deleted is a member of *EQUPS*. The following schema describes this command:

$$\begin{array}{l} DeleteEquip(eqp, com{:}\,ALPHANUMERIC) \\ \quad (eqp, com) \in EQUPS \\ \quad EQUPS' = EQUPS \setminus \{(eqp, com)\} \end{array}$$

- *Device elements*

AddDevice: This command is to create a new nuclear device element in the OBAC operation base. The command is valid only if the new device element is not already a member of the data set *DIVCS*. The set is to be updated. The following schema describes this command:

$$\begin{array}{l} AddDevice(div, sys, eqp, com{:}\,ALPHANUMERIC) \\ \quad (div, sys) \in SYSTS \\ \quad (eqp, com) \in EQUPS \\ \quad (div, sys, eqp, com) \notin DEVIS \\ \quad DEVIS' = DEVIS \cup \{(div, sys, eqp, com)\} \end{array}$$

DeleteDevice: This command is to delete an existing nuclear device element from the OBAC operation base. The command is valid only if the device element to be deleted is a member of *DIVCS*. The following schema describes this command:

$$\begin{array}{l} DeleteDevice(div, sys, eqp, com{:}\,ALPHANUMERIC) \\ \quad (div, sys, eqp, com) \in DEVIS \\ \quad DEVIS' = DEVIS \setminus \{(div, sys, eqp, com)\} \end{array}$$

BaseSpec.-2: ***Core Operations** specification*

BaseSpec.-2 defines the specifications for the elements in the 5 nuclear *core operations* (Figure 2.4).

The 5 core operations are: nuclear device *monitoring*, nuclear data *processing*, nuclear equipment *controlling*, nuclear device changes *verifying*, and nuclear system performance observing/*supervising* operations.

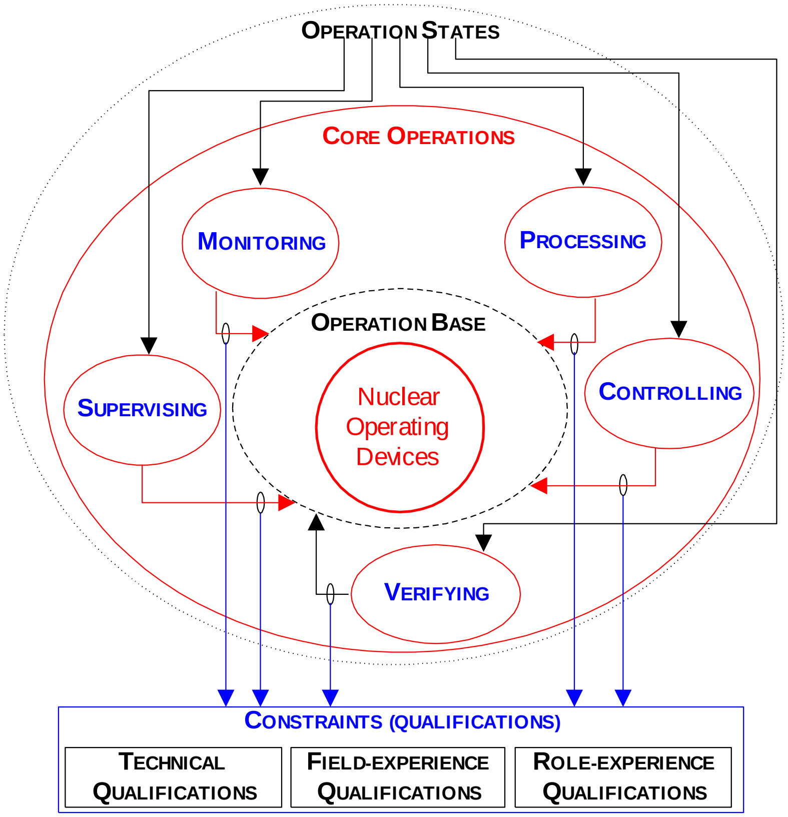


Figure 2.4: Nuclear core operation access controls

- *Data Sets*: Below defines the data sets for the core operations.

$CORES\{div, sys, eqp, com, core\}$: CORE OPERATION
where *core* = monitoring, processing, controlling, verifying, or supervising operations

- *Core operations elements*

AddCore: This command is to create a core function element in the OBAC operation base. The command is valid only if the new core function element is not already a member of the data set *CORES*. It is to be updated. The following schema describes this command:

$AddCore(div, sys, eqp, com, core: ALPHANUMERIC)$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, core) \notin CORES$
$CORES' = CORES \cup \{(div, sys, eqp, com, core)\}$

DeleteCore: This command is to delete an existing core function element from the OBAC operation base. The command is valid only if the core function element to be deleted is a member of the data set *CORES*. It is to be updated. The following schema describes this command:

$DeleteCore(div, sys, eqp, com, core: ALPHANUMERIC)$
$(div, sys, eqp, com, core) \in CORES$
$CORES' = CORES \setminus \{(div, sys, eqp, com, core)\}$

BaseSpec.-3: ***Technical Qualifications** specification*

BaseSpec.-3 defines the specifications for the elements in the *technical qualifications* for the nuclear network core operations (Figure 2.5).

Each of the 5 core operations has its own technical qualification requirements. In general, the nuclear equipment *controlling* operation requires the *highest* technical qualification because the controlling operation is to make changes to an existing nuclear device for example adjusting the settings of the device or even completely replacing the device and improper controlling operation can have serious consequence. Therefore the controlling operation usually carries the largest number of technical qualification elements. Conversely, the supervising/ observing operation often has the least number of technical qualification elements as this operation does not alter the on-line operation and therefore it usually has the minimum impact on the on-going nuclear operation.

There are 4 groups of technical and nuclear qualification trainings as shown in Figure 2.5 below. They are: TG1 – *nuclear awareness trainings* group; TG2 – *nuclear practices trainings* group; TG3 – *nuclear system process trainings* group; and TG4 – *technologies trainings* group. Anyway, the basic ADD and DELETE of a technical-nuclear qualification element for all core operations and all groups are similar.

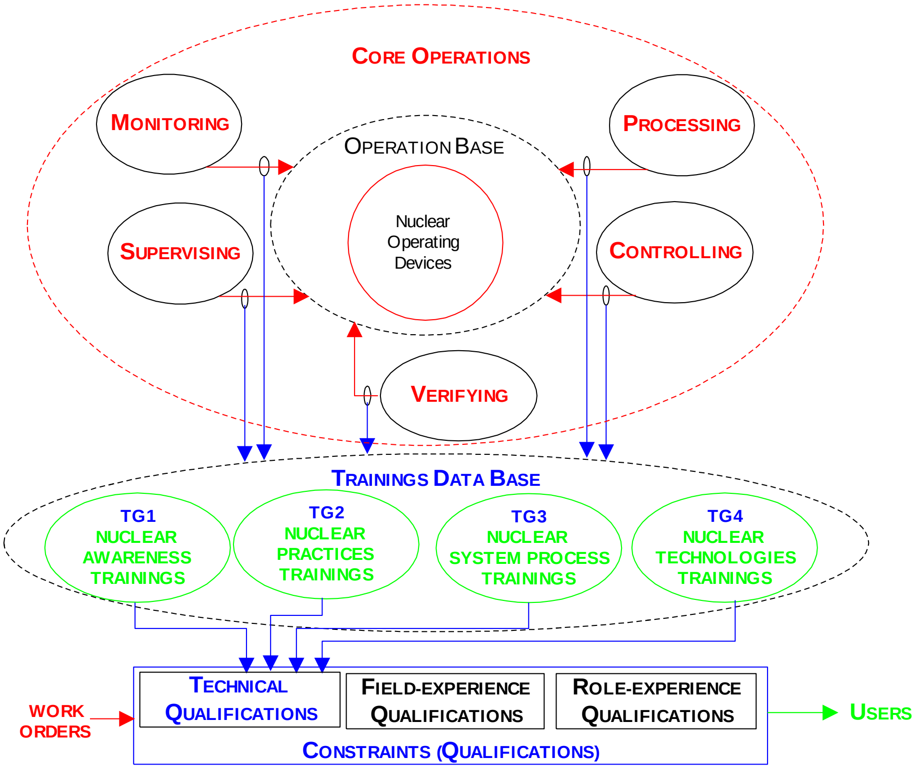

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
TRAININGS DATA BASE
TG1 NUCLEAR AWARENESS TRAININGS
TG2 NUCLEAR PRACTICES TRAININGS
TG3 NUCLEAR SYSTEM PROCESS TRAININGS
TG4 NUCLEAR TECHNOLOGIES TRAININGS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.5: Technical qualifications for core operation access controls

- *Data Sets*: Below defines the data set for the *technical-experience* qualification elements.

$TECHBS\{((div, sys, eqp, com, core), tech_{base})\}$: TECHNICAL BASES
$HTECS\{tech_i, tech_{i-1}, \ldots, tech_1\}$ where $\mathrm{tech_i} \succcurlyeq \mathrm{tech_{i-1}}$: TECH HIERARCHY

- *Technical-Experience Qualification elements*

AddTechB: This command is to add a new technical-qualification base element. The command is valid only if this base element is not already a member of the data set $TECHBS$. It is to be updated. The following schema describes this command:

$AddTechB((div, sys, eqp, com, core), tech_{base}: ALPHANUMERIC)$
$tech_{base} \in HTECS$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, core) \in CORES$
$((div, sys, eqp, com, core), tech_{base}) \notin TECHBS$
$TECHBS' = TECHBS \cup \{((div, sys, eqp, com, core), tech_{base})\}$

DeleteTechB: This command is to delete an existing technical-qualification base element. The command is valid only if the base element to be deleted is a member of the data set $TECHBS$. It is to be updated. The following schema describes this command:

$DeleteTechB((div, sys, eqp, com, core), tech_{base}: ALPHANUMERIC)$
$((div, sys, eqp, com, core), tech_{base}) \in TECHBS$
$TECHBS' = TECHBS \setminus \{((div, sys, eqp, com, core), tech_{base})\}$

BaseSpec.-4: ***Field Experience Qualifications*** *specification*

BaseSpec.-4 defines the specifications for the elements in the *field-experiences qualifications* for the nuclear network core operations (Figure 2.6).

There are 5 groups of field-experiences qualifications: FG1 – *on-line division-level* op-exp (operation-experiences) group; FG2 – *on-line system-level* op-exp group; FG3 – *on-line critical equipment* op-exp group; FG4 – *on-line non-critical equipment* op-exp group; and FG5 – *outage maintenance* op-exp group. Anyway, the basic ADD and DELETE of a field-experience qualification element for all core operations and all qualification groups are similar.

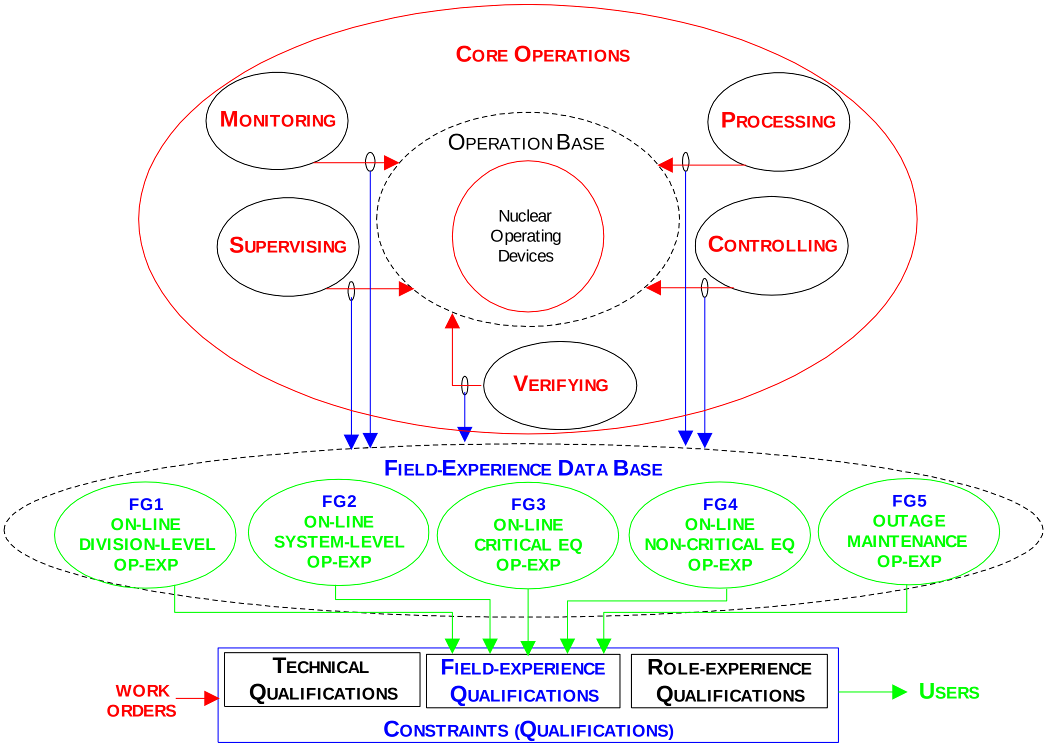

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.6: Field-experience qualifications

- *Data Sets*: Below defines the data set for the *field-experience* qualification elements.

$FIELDBS\{((div, sys, eqp, com, core), field_{base})\}$: FIELD BASES
$HFILS\{field_i, field_{i-1}, \dots, field_1\}$ where $\mathrm{field}_\mathrm{i} \succcurlyeq \mathrm{field}_{\mathrm{i}-1}$: FIELD HIERARCHY

- *Field-Experience Qualification elements*

AddFieldB: This command is to add a new field-qualification base element. The command is valid only if this base element is not already a member of the data set $FIELDBS$. It is to be updated. The following schema describes this command:

$AddFieldB((div, sys, eqp, com, core), field_{base}: ALPHANUMERIC)$
$field_{base} \in HFILS$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, core) \in CORES$
$((div, sys, eqp, com, core), field_{base}) \notin FIELDBS$
$FIELDBS' = FIELDBS \cup \{((div, sys, eqp, com, core), field_{base})\}$

DeleteFieldB: This command is to delete an existing field-qualification base element. The command is valid only if the base element to be deleted is a member of the data set $FIELDBS$. It is to be updated. The following schema describes this command:

$DeleteFieldB((div, sys, eqp, com, core), field_{base}: ALPHANUMERIC)$
$((div, sys, eqp, com, core), field_{base}) \in FIELDBS$
$FIELDBS' = FIELDBS \setminus \{((div, sys, eqp, com, core), field_{base})\}$

BaseSpec.-5: ***Role Experience Qualifications*** *specification*

BaseSpec.-5 defines the specifications for the elements in the *role experience* qualifications for the core operations (Figure 2.7).

There are 3 major groups of nuclear roles: *Operation* group, *Engineering* group, and *CM* (*Control Maintenance*) group. Within the Operation major group, there are *Operation Authorities* group, *Control Room Supervisors* group, *ANO* (*Authorized Nuclear Operators*) group, etc. Within the Engineering major group, there are *Engineering Authorities* group, *Design Engineers* group, *Field Engineers* group, *Project Engineers* group, *Training Officers* group, etc. Within the CM major group, there are *CM Supervisors* group, *Technologists* group, *Control Technicians* group, *Maintenance Technicians* group, *Installation Technicians* groups, etc.

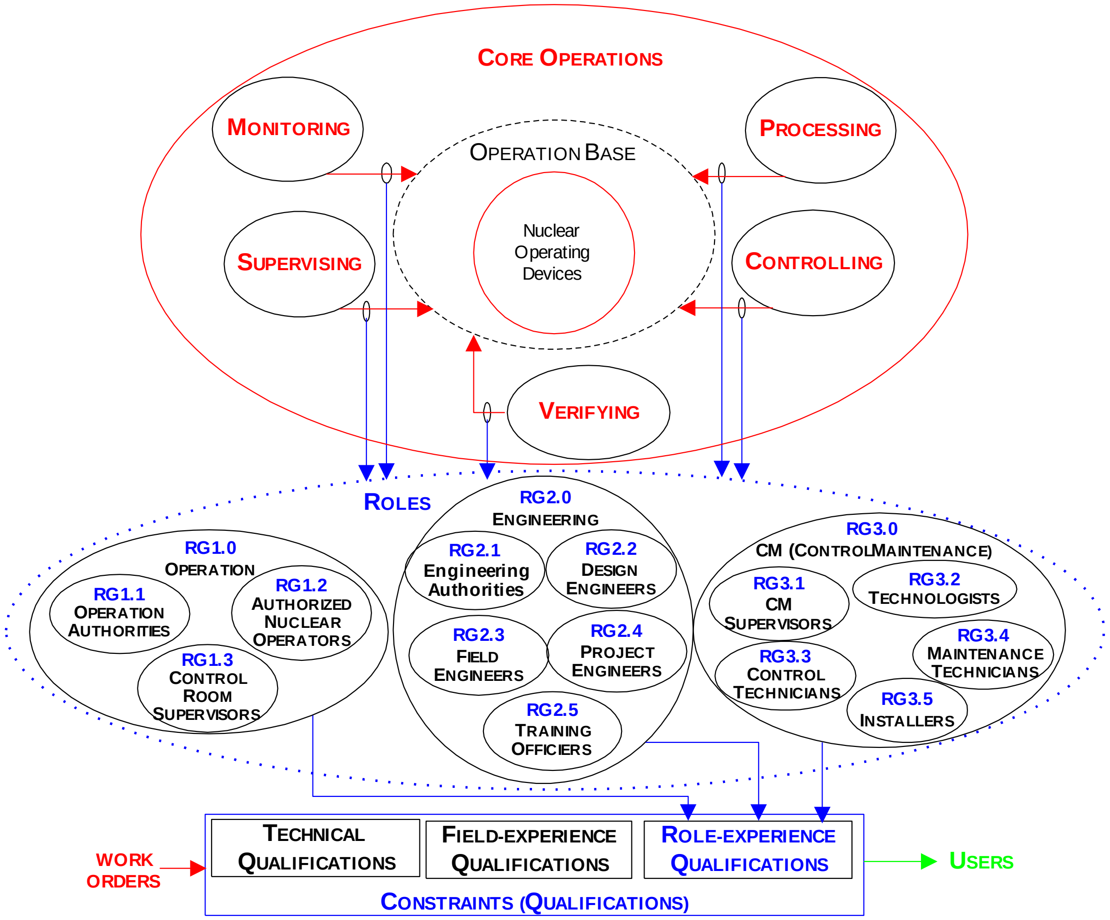

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
ROLES
RG1.0 OPERATION
RG1.1 OPERATION AUTHORITIES
RG1.2 AUTHORIZED NUCLEAR OPERATORS
RG1.3 CONTROL ROOM SUPERVISORS
RG2.0 ENGINEERING
RG2.1 Engineering Authorities
RG2.2 DESIGN ENGINEERS
RG2.3 FIELD ENGINEERS
RG2.4 PROJECT ENGINEERS
RG2.5 TRAINING OFFICIERS
RG3.0 CM (CONTROLMAINTENANCE)
RG3.1 CM SUPERVISORS
RG3.2 TECHNOLOGISTS
RG3.3 CONTROL TECHNICIANS
RG3.4 MAINTENANCE TECHNICIANS
RG3.5 INSTALLERS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 2.7: Nuclear roles for access controls

- *Data Sets*: Below defines the data set for the *role-experience* qualification elements.

$ROLEBS\{((div, sys, eqp, com, core), role_{base})\}$: ROLE BASES
$HROLS\{role_i, role_{i-1}, \dots, role_1\}$ where $\mathrm{role_i} \succcurlyeq \mathrm{role_{i-1}}$: ROLE HIERARCHY

- *Role-Experience Qualification elements*

AddRoleB: This command is to add a new role-qualification base element. The command is valid only if this base element is not already a member of the data set $ROLEBS$. It is to be updated. The following schema describes this command:

$AddRoleB((div, sys, eqp, com, core), role_{base}: ALPHANUMERIC)$
$role_{base} \in HROLS$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, core) \in CORES$
$((div, sys, eqp, com, core), role_{base}) \notin ROLEBS$
$ROLEBS' = ROLEBS \cup \{((div, sys, eqp, com, core), role_{base})\}$

DeleteRoleB: This command is to delete an existing role-qualification base element. The command is valid only if the base element to be deleted is a member of the data set $ROLEBS$. It is to be updated. The following schema describes this command:

$DeleteRoleB((div, sys, eqp, com, core), role_{base}: ALPHANUMERIC)$
$((div, sys, eqp, com, core), role_{base}) \in ROLEBS$
$ROLEBS' = ROLEBS \setminus \{((div, sys, eqp, com, core), role_{base})\}$

BaseSpec.-6: ***Operation States** specification*

BaseSpec.-6 defines the specifications for the elements in the 4 operation states (Figure 2.8).

The 4 operation states are: *Routine* operations, *Emergency* operations, *On-line Maintenance* operations, and *Outage Maintenance* operations.

The *non-operation* work for each of the 4 states are to be specified in this specification.

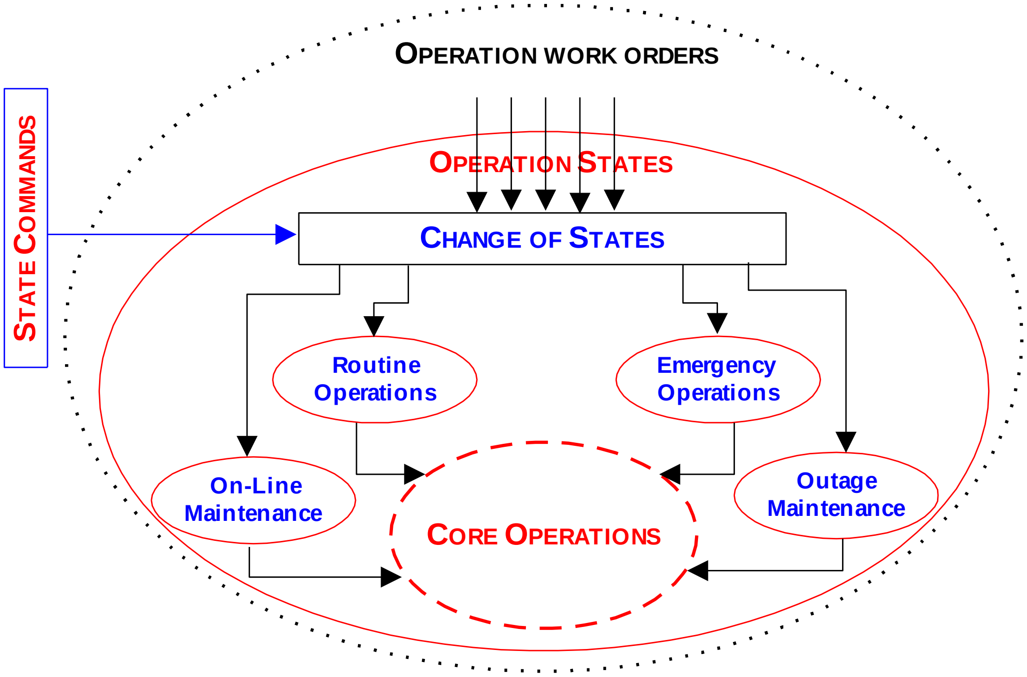


Figure 2.8: Nuclear operation state access controls

- *Data Sets*: Below defines the data set for the state of *non-operations*.

$NONOPS\{div, sys, eqp, com, core, state\}$: NON-OPERATION STATE
where *state* = routine, emergency, on-line maintenance, and outage maintenance

- *Non-operations elements*

AddNonOp: This command is to add a new non-operation element for each of 4 operation states. The command is valid only if the new element is not already a member of the data set $NONOPS$. It is to be updated. The following schema describes this command:

$AddNonOp(div, sys, eqp, com, core, state: ALPHANUMERIC)$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, core) \in CORES$
$(div, sys, eqp, com, core, state) \notin NONOPS$
$NONOPS' = NONOPS \cup \{(div, sys, eqp, com, core, state)\}$

DeleteNonOP: This command is to delete an existing non-operation element. The command is valid only if the non-operation element to be deleted is a member of the data set $NONOPS$. It is to be updated. The following schema describes this command:

$DeletenNonOp(div, sys, eqp, com, core, state: ALPHANUMERIC)$
$(div, sys, eqp, com, core, state) \in NONOPS$
$NONOPS' = NONOPS \setminus \{(div, sys, eqp, com, core, state)\}$

BaseSpec.-7*: *Work Orders* *specification

BaseSpec.-7 defines the specifications for the elements in the 5 groups of work orders for the 5 nuclear network core operations (Figure 2.9).

The 5 groups are: nuclear device *monitoring* work orders, nuclear data *processing* work orders, nuclear equipment *controlling* work orders, nuclear device changes *verifying* work orders and nuclear system performance *supervising* work orders.

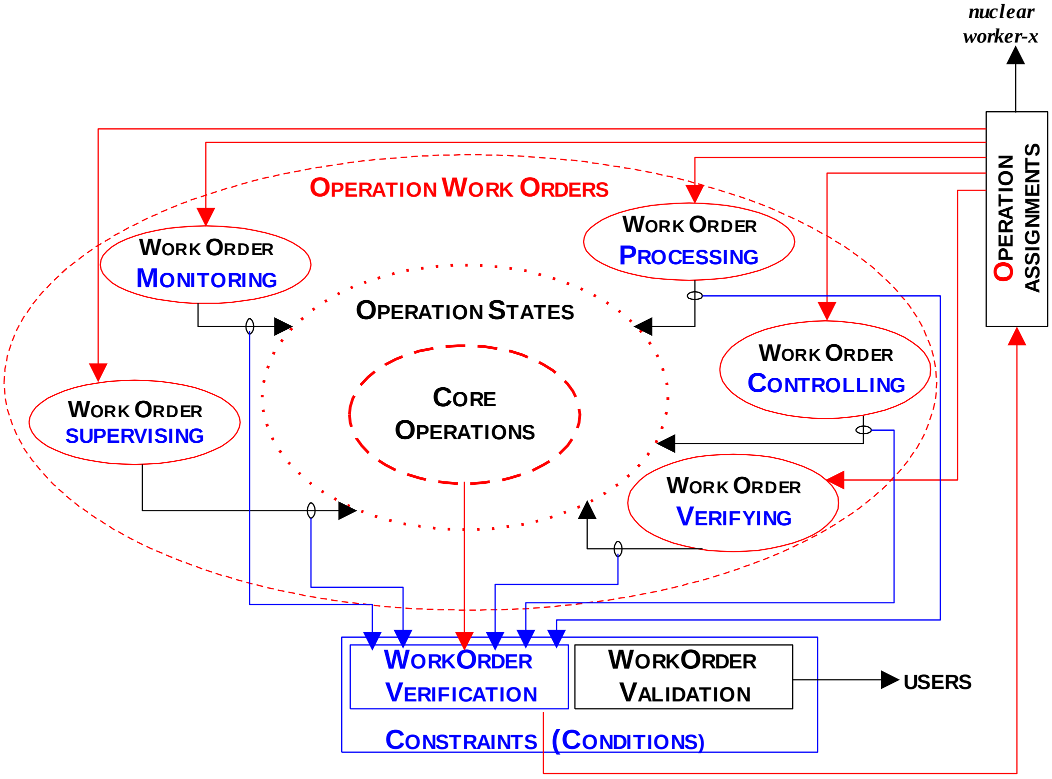


Figure 2.9: Operation work orders assignment

- *Data Sets*: Below defines the data set for the *work orders*.

$WORKS\{(div, sys, eqp, com, work, wstate)\}$: WORK ORDER
where *work*= monitoring, processing, controlling, verifying, or supervising work orders
wstate=routine, emergency, on-line, and outage

- *Work Orders elements*:

AddWork: This command is to create a new work order element in the OBAC operation base. The command is valid only if the new order element is a member of the data set *CORES* (work order verification with respect to the core operation) and is not already a member of the data set *WORKS* (new element). It is to be updated. The following schema describes this command:

$AddWork(div, sys, eqp, com, work, wstate: ALPHANUMERIC)$
$(div, sys) \in SYSTS$
$(eqp, com) \in EQUPS$
$(div, sys, eqp, com) \in DEVIS$
$(div, sys, eqp, com, work) \in CORES$
$(div, sys, eqp, com, work, wstate) \notin WORKS$
$WORKS' = WORKS \cup \{(div, sys, eqp, com, work, wstate)\}$

DeleteWork: This command is to delete an existing work order element from the OBAC operation base. The command is valid only if the work order element to be deleted is a member of the data set *WORKS*. It is to be updated. The following schema describes this command:

$DeleteWork(div, sys, eqp, com, work, wstate: ALPHANUMERIC)$
$(div, sys, eqp, com, work, wstate) \in WORKS$
$WORKS' = WORKS \setminus \{(div, sys, eqp, com, work, wstate)\}$

BaseSpec.-8: ***Users*** *specification*

BaseSpec.-8 defines the specifications for the elements in the nuclear *user*, as shown in Figure 2.12.

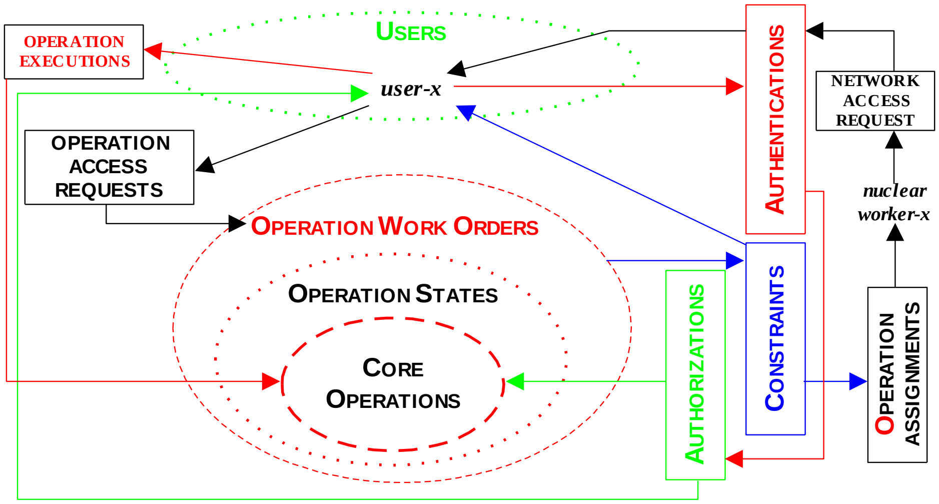


Figure 2.12: User access controls

- *Data Sets*: Below defines the data set for the nuclear *users*.

$$USERS\{user\} : \mathrm{USERS}$$

- *users elements*:

AddUser: This command is to create a new user element in the OBAC operation base. The command is valid only if the new user element is not already a member of the data set *USERS*. It is to be updated. The following schema describes this command:

$$AddUser(user\colon ALPHANUMERIC)$$
$$user \notin USERS$$
$$USERS' = USERS \cup \{user\}$$

DeleteUser: This command is to delete an existing user element from the OBAC operation base. The command is valid only if the user element to be deleted is a member of the data set *USERS*. It is to be updated. The following schema describes this command:

$$DeleteUser(user\colon ALPHANUMERIC)$$
$$user \in USERS$$
$$USERS' = USERS \setminus \{user\}$$

2.5 Hierarchies Specifications for OBAC

This section presents the *Hierarchies Specification* the OBAC Specifications. This is to establish the specifications for the *technical* qualification hierarchies, *field*-experience qualification hierarchies, and *role*-experience qualification hierarchies.

HierSpec.-1: ***Role Experiences Qualification*** *hierarchies specification*

HierSpe.-1 defines the specifications for the role experiences qualification hierarchies for the OBAC core operations, of which the role experience groups are shown in Figure 2.13.

The inheritance relation can be expressed using the symbol $\succcurlyeq$. The property of $\succcurlyeq$ for role application in the access control can be expressed as: $role_1 \succcurlyeq role_2$ only if all permissions of $role_2$ are also permissions of $role_1$. For the OBAC application, $role_1 \succcurlyeq role_2$ means that all experience qualifications of $role_2$ are also qualifications of $role_1$. The role experience qualifications for the core operations are partially expanded with respect to the nuclear design engineering shown in Figure 2.13.

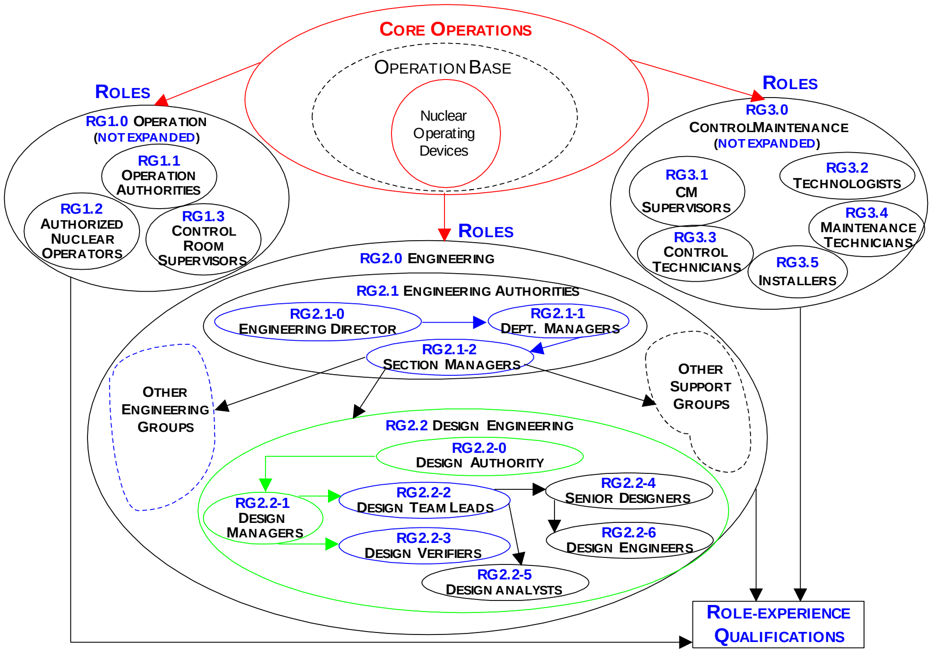


Figure 2.13: Role experience hierarchies

The hierarchies in the nuclear design engineering groups (only consider design here) are as follows:

$$Engineer\ Director \succcurlyeq Department\ Mangers \succcurlyeq Section\ Managers \succcurlyeq Design\ Authority \succcurlyeq$$

$$Design\ Managers \left\{ \begin{array}{l} \succcurlyeq Design\ Team\ Leads \left\{ \begin{array}{l} \succcurlyeq Senior\ Designers \succcurlyeq Design\ Engineers \\ \succcurlyeq Design\ Analysts \end{array} \right\} \\ \succcurlyeq Design\ Verifiers \end{array} \right\}$$

- *Data Sets*: Define the data sets for the *role-experience qualifications* as follows.

$ROLES\{role\}$: ROLES

$HROLS\{role_i, role_{i-1}, \dots, role_1\}$ where $\mathrm{role_i} \succcurlyeq \mathrm{role_{i-1}}$: ROLE HIERARCHY

- *Role qualification hierarchies*:

AddRole: This command is to add a new role element. The command is valid only if the new role element is not already a member of the data set $ROLES$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} AddRole(role) \\ \quad role \notin ROLES \\ \quad ROLES' = ROLES \cup \{role\} \end{array}$$

DeleteRole: This command is to delete an existing role element. The command is valid only if the role element to be deleted is a member of the data set $ROLES$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} DeleteRole(role) \\ \quad role \in ROLES \\ \quad ROLES' = ROLES \setminus \{role\} \end{array}$$

AssignHRole: This command is to create a new role hierarchy. This command is repeated until $ROLES \longmapsto \emptyset$. The following schema describes this command:

$$\begin{array}{l} AssignHRole(ROLES) \\ \begin{pmatrix} ROLES \longmapsto \emptyset \circ \exists role_{asc} \in ROLES \circ \forall role \in ROLES \circ role_{asc} \succcurlyeq role \\ \quad \Longrightarrow HROLS' = HROLS \cup \{role_{asc}\};\ ROLES' = ROLES \setminus \{role_{asc}\} \end{pmatrix}^{*} \end{array}$$

DeAssignHRole: This command is to delete an existing role in the role hierarchy. The command is valid only if the role element to be deleted is a member of the data set $HROLS$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} DeAssignHRole(role) \\ \quad role \in HROLS \\ \quad HROLS' = HROLS \setminus \{role\} \\ \quad ROLES' = ROLES \cup \{role\} \end{array}$$

HierSpec.-2: ***Field Experiences Qualification** hierarchies specification*

HierSpe.-2 defines the specifications for the field experiences qualification hierarchies for the OBAC core operations, of which the field experience groups are shown in Figure 2.14.

For the OBAC application, $f_1 \succcurlyeq f_2$ means that all qualifications recognized for field f_2 are also recognized for field f_1. As defined in Figure 2.14, *FG1* is the *on-line division-level* operation experience qualifications and *FG2* is the *on-line system-level* operation experience qualifications. *FG1* qualifications almost cover *FG2* qualifications. Therefore in general, $FG1 \gtrsim FG2$ and *FG1* is approximately the ascendant of *FG2*, or *FG2* is approximately the descendant of *FG1*. In the other words, all qualifications recognized for *FG1* are almost recognized for *FG2*.

Similarly, $FG3 \gtrsim FG4$, where *FG3*, the *on-line critical equipment* operation experience qualifications is approximately the ascendant of *FG4*, the *on-line non-critical equipment* operation experience qualifications, as *FG3* qualifications almost cover *FG4* qualifications and all qualifications recognized for *FG3* are almost recognized for *FG4*.

In general, the *on-line* operation experience qualifications are approximately the *ascendant* of the *outage* operation qualifications, as most of the on-line operations are *time critical* and have *nuclear safety* implication when compared with the outage operations.
Therefore $\{FG1, FG2, FG3, FG4\} \gtrsim FG5$

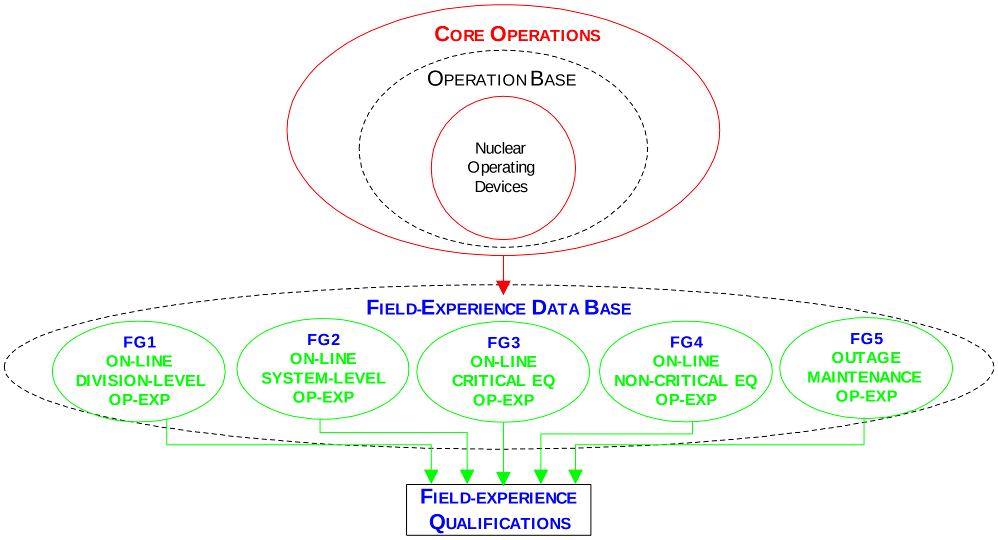

CORE OPERATIONS
OPERATION BASE
Nuclear Operating Devices
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
FIELD-EXPERIENCE QUALIFICATIONS

Figure 2.14: Field experience hierarchies

- *Data Sets*: Define the data sets for the *field-experience qualifications* as follows.

$FIELDS\{field\}$: FIELDS
$HFILS\{field_i, field_{i-1}, \dots, field_1\}$ where $\mathrm{field}_{\mathrm{i}} \succcurlyeq \mathrm{field}_{\mathrm{i}-1}$: FIELD HIERARCHY

- *Field qualification hierarchies*:

AddFil: This command is to add a new field-experience qualification element. The command is valid only if the new field element is not already a member of the data set $FIELDS$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} AddFil(field) \\ \quad field \notin FIELDS \\ \quad FIELDS' = FIELDS \cup \{field\} \end{array}$$

DeleteFil: This command is to delete an existing field element. The command is valid only if the field element to be deleted is a member of the data set $FIELDS$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} DeleteFil(field) \\ \quad field \in FIELDS \\ \quad FIELDS' = FIELDS \setminus \{field\} \end{array}$$

AssignHFil: This command is to create a new field hierarchy. This command is repeated until $FIELDS \longmapsto \emptyset$. The following schema describes this command:

$$\begin{array}{l} AssignHFil(FIELDS) \\ \left(\begin{array}{l} FIELDS \longmapsto \emptyset \circ \exists field_{asc} \in FIELDS \circ \forall field \in FIELDS \circ field_{asc} \succcurlyeq field \\ \qquad \Longrightarrow HFILS' = HFILS \cup \{field_{asc}\};\ FIELDS' = FIELDS \setminus \{field_{asc}\} \end{array}\right)^{*} \end{array}$$

DeAssignHFil: This command is to delete an existing field in the field hierarchy. The command is valid only if the field element to be deleted is a member of the data set $HFILS$. It is to be updated. The following schema describes this command:

$$\begin{array}{l} DeAssignHFil(field) \\ \quad field \in HFILS \\ \quad HFILS' = HFILS \setminus \{field\} \\ \quad FIELDS' = FIELDS \cup \{field\} \end{array}$$

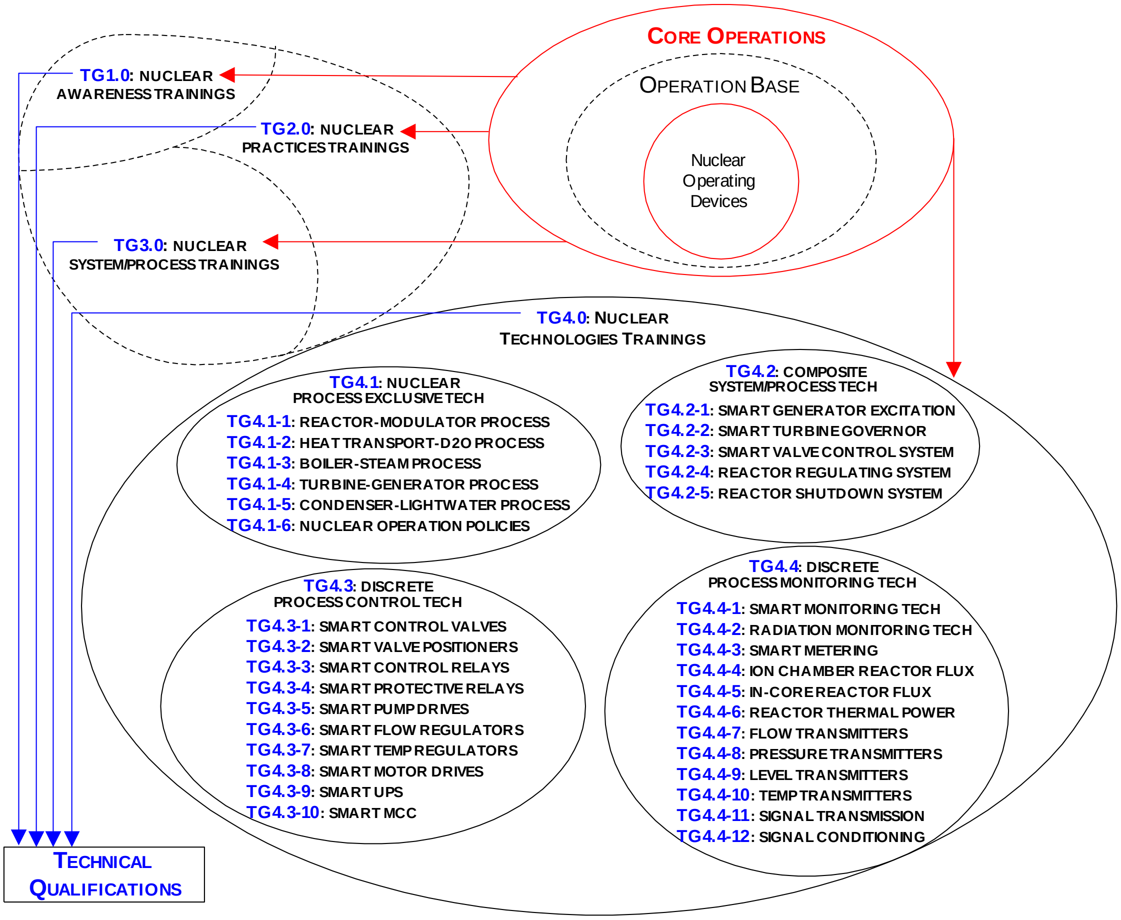
HierSpec.-3: ***Technical Experiences Qualification*** *hierarchies specification*

HierSpe.-3 defines the specifications for the technical experiences qualification hierarchies for the OBAC core operations, of which the technical experience groups are shown in Figure 2.15.

For the OBAC application, $tech_1 \succcurlyeq tech_2$ means that all technical experience qualifications of $tech_2$ are also qualifications of $tech_1$. The technical experience qualifications for the nuclear core operations are partially expanded with respect to the nuclear technologies trainings, as shown in Figure 2.15.

The hierarchies in the nuclear technical experience qualification through trainings (only consider technologies trainings here) are as follows:

$$TG4.1\colon nuclear\ process\ exclusive\ tech \succcurlyeq TG4.2\colon composite\ process\ system\ tech \succcurlyeq$$
$$TG4.3\colon discrete\ process\ control\ tech \succcurlyeq TG4.4\colon Discrete\ process\ monitoring\ tech$$



CORE OPERATIONS
OPERATION BASE
Nuclear Operating Devices
TG1.0: NUCLEAR AWARENESS TRAININGS
TG2.0: NUCLEAR PRACTICES TRAININGS
TG3.0: NUCLEAR SYSTEM/PROCESS TRAININGS
TG4.0: NUCLEAR TECHNOLOGIES TRAININGS
TG4.1: NUCLEAR PROCESS EXCLUSIVE TECH
TG4.1-1: REACTOR-MODULATOR PROCESS
TG4.1-2: HEAT TRANSPORT-D2O PROCESS
TG4.1-3: BOILER-STEAM PROCESS
TG4.1-4: TURBINE-GENERATOR PROCESS
TG4.1-5: CONDENSER-LIGHTWATER PROCESS
TG4.1-6: NUCLEAR OPERATION POLICIES
TG4.2: COMPOSITE SYSTEM/PROCESS TECH
TG4.2-1: SMART GENERATOR EXCITATION
TG4.2-2: SMART TURBINE GOVERNOR
TG4.2-3: SMART VALVE CONTROL SYSTEM
TG4.2-4: REACTOR REGULATING SYSTEM
TG4.2-5: REACTOR SHUTDOWN SYSTEM
TG4.3: DISCRETE PROCESS CONTROL TECH
TG4.3-1: SMART CONTROL VALVES
TG4.3-2: SMART VALVE POSITIONERS
TG4.3-3: SMART CONTROL RELAYS
TG4.3-4: SMART PROTECTIVE RELAYS
TG4.3-5: SMART PUMP DRIVES
TG4.3-6: SMART FLOW REGULATORS
TG4.3-7: SMART TEMP REGULATORS
TG4.3-8: SMART MOTOR DRIVES
TG4.3-9: SMART UPS
TG4.3-10: SMART MCC
TG4.4: DISCRETE PROCESS MONITORING TECH
TG4.4-1: SMART MONITORING TECH
TG4.4-2: RADIATION MONITORING TECH
TG4.4-3: SMART METERING
TG4.4-4: ION CHAMBER REACTOR FLUX
TG4.4-5: IN-CORE REACTOR FLUX
TG4.4-6: REACTOR THERMAL POWER
TG4.4-7: FLOW TRANSMITTERS
TG4.4-8: PRESSURE TRANSMITTERS
TG4.4-9: LEVEL TRANSMITTERS
TG4.4-10: TEMP TRANSMITTERS
TG4.4-11: SIGNAL TRANSMISSION
TG4.4-12: SIGNAL CONDITIONING
TECHNICAL QUALIFICATIONS

Figure 2.15: Technical experience hierarchies

- *Data Sets*: Define the data sets for the *technical-experience qualifications* as follows.

$TECHS\{tech\}$: TECHS
$HTECS\{tech_i, tech_{i-1}, \dots, tech_1\}$ where $\mathrm{tech_i} \succcurlyeq \mathrm{tech_{i-1}}$: TECH HIERARCHY

- *Technical qualification hierarchies*:

AddTec: This command is to add a new technical-experience qualification element. The command is valid only if the new technical element is not already a member of the data set $TECHS$. It is to be updated. The following schema describes this command:

$AddTec(tech)$
$tech \notin TECHS$
$TECHS' = TECHS \cup \{tech\}$

DeleteTec: This command is to delete an existing technical qualification element. The command is valid only if the technical element to be deleted is a member of the data set $TECHS$. It is to be updated. The following schema describes this command:

$DeleteTec(tech)$
$tech \in TECHS$
$TECHS' = TECHS \setminus \{tech\}$

AssignHTec: This command is to create a new technical hierarchy. This command is repeated until $TECHS \longmapsto \emptyset$. The following schema describes this command:

$AssignHTec(TECHS)$

$$\begin{pmatrix} TECHS \longmapsto \emptyset \circ \exists tech_{asc} \in TECHS \circ \forall tech \in TECHS \circ tech_{asc} \succcurlyeq tech \\ \Longrightarrow HTECS' = HTECS \cup \{tech_{asc}\};\ TECHS' = TECHS \setminus \{tech_{asc}\} \end{pmatrix}^{*}$$

DeAssignHTec: This command is to delete an existing technical in the technical hierarchy. The command is valid only if the technical element to be deleted is a member of the data set $HTECS$. It is to be updated. The following schema describes this command:

$DeAssignHTec(tech)$
$tech \in HTECS$
$HTECS' = HTECS \setminus \{tech\}$
$TECHS' = TECHS \cup \{tech\}$

2.6 Assignment Specifications for OBAC

This section presents the specifications of *assignments* in the OBAC Specifications, which include role qualifications assignment, field qualifications assignment, and technical qualifications assignment.

AssigSpec.-1: ***Role Qualifications*** *assignment specification*

AssigSpec.-1 defines the specification for the assignments of the role-experience qualifications.

- *Data Sets*: Define the data sets for the role-experience qualification assignments as follows.

$$\boxed{ARQS\{((div, sys, eqp, com, core), \{role_1 \ldots role_i\})\} : \text{ASSIGNED ROLE QUALIS}}$$

- *Role qualification hierarchies*:

AssignRoleQ: This command is to create a seniority role-experience qualification hierarchy. The command is valid only if the reference role qualification element is not already a member of $ARQS$, and it is to be updated. The command is repeated* until $role \not\succcurlyeq role_{base}$. The following schema describes this command:

$$\begin{array}{l}
AssignRoleQ(ROLEBS) \\
\quad ROLEBS\{((div, sys, eqp, com, core), role_{base})\} \\
\quad role_{base} \in HROLS \\
\quad role_1 = role_{base} \\
\quad ((div, sys, eqp, com, core), \{role_1\}) \notin ARQS \\
\quad ARQS' = ARQS \cup \{((div, sys, eqp, com, core), \{role_1\})\} \\
\quad \left(\begin{array}{c} \forall role_i \in HROLS \circ role_i \succcurlyeq role_1 \\ \Rightarrow ARQS' = ARQS \cup \{((div, sys, eqp, com, core), \{role_i\})\} \end{array} \right)^{*} \\
\quad ARQS = \{((div, sys, eqp, com, core), \{role_1, \ldots role_i\})\}
\end{array}$$

AddAssignRoleQ: This command is to add a new role qualification element. The command is valid only if the new element is not already a member of $ARQS$. It is to be updated. The following schema describes this command:

$$
\begin{array}{l}
AddAssignRoleQ\left(\left((div, sys, eqp, com, core), role_i\right)\right) \\
\quad role_i \in HROLS \\
\quad \left((div, sys, eqp, com, core), \{role_i\}\right) \notin ARQS \\
\quad ARQS' = ARQS \cup \left\{\left((div, sys, eqp, com, core), \{role_i\}\right)\right\}
\end{array}
$$

DeAssignRoleQ: This command is to delete an existing role qualification element. The command is valid only if the new element is a member of $ARQS$. It is to be updated. The following schema describes this command:

$$
\begin{array}{l}
DeAssignRoleQ\left(\left((div, sys, eqp, com, core), role_i\right)\right) \\
\quad role_i \in HROLS \\
\quad \left((div, sys, eqp, com, core), \{role_i\}\right) \notin ARQS \\
\quad ARQS' = ARQS \setminus \left\{\left((div, sys, eqp, com, core), \{role_i\}\right)\right\}
\end{array}
$$

AssigSpec.-2: ***Field Qualifications*** *assignment specification*

AssigSpec.-2 defines the specification for the assignments of the field-experience qualifications.

- *Data Sets*: Define the data sets for the field-experience qualification assignments as follows.

$AFQS\{((div, sys, eqp, com, core), \{field_1 \dots field_i\})\}$: ASSIGNED FIELD QUALIS

- *Field qualification hierarchies*:

AssignFieldQ: This command is to create a seniority field-experience qualification hierarchy. The command is valid only if the reference field qualification element is not already a member of $AFQS$, and it is to be updated. The command is repeated* until $field \nsucccurlyeq field_{base}$. The following schema describes this command:

$$AssignFieldQ(FIELDBS)$$

$$FIELDBS\{((div, sys, eqp, com, core), field_{base})\}$$

$$field_{base} \in HFILS$$

$$field_1 = field_{base}$$

$$((div, sys, eqp, com, core), \{field_1\}) \notin AFQS$$

$$AFQS' = AFQS \cup \{((div, sys, eqp, com, core), \{field_1\})\}$$

$$\begin{pmatrix} \forall field_i \in HFILS \circ field_i \succcurlyeq field_{base} \\ \Rightarrow AFQS' = AFQS \cup \{((div, sys, eqp, com, core), \{field_i\})\} \end{pmatrix}^*$$

$$AFQS = \{((div, sys, eqp, com, core), \{field_1 \dots field_i\})\}$$

AddAssignFieldQ: This command is to add a new field qualification element. The command is valid only if the new element is not already a member of $AFQS$. It is to be updated. The following schema describes this command:

$$AddAssignFieldQ\left(((div, sys, eqp, com, core), field_i)\right)$$

$$field_i \in HFILS$$

$$((div, sys, eqp, com, core), \{field_i\}) \notin AFQS$$

$$AFQS' = AFQS \cup \{((div, sys, eqp, com, core), \{field_i\})\}$$

DeAssignFieldQ: This command is to delete an existing field qualification element. The command is valid only if the new element is a member of $AFQS$. It is to be updated. The following schema describes this command:

$DeAssignFieldQ\left(\left((div, sys, eqp, com, core), field_i\right)\right)$

$field_i \in HFILS$

$\left((div, sys, eqp, com, core), \{field_i\}\right) \notin AFQS$

$AFQS' = AFQS \setminus \left\{\left((div, sys, eqp, com, core), \{field_i\}\right)\right\}$

AssigSpec.-3: ***Technical Qualifications*** *assignment specification*

AssigSpec.-3 defines the specification for the assignments of the technical-experience qualifications.

- *Data Sets*: Define the data sets for the technical-experience qualification assignments as follows.

$$\boxed{ATQS\{((div, sys, eqp, com, core), \{tech_1 \ldots tech_i\})\} : \text{ASSIGNED TECHNICAL QUALIS}}$$

- *Technical qualification hierarchies*:

AssignTechQ: This command is to create a seniority technical-experience qualification hierarchy. The command is valid only if the reference technical qualification element is not already a member of $ATQS$, and it is to be updated. The command is repeated* until $tech \nsucceq tech_{base}$. The following schema describes this command:

$$\begin{array}{l}
AssignTechQ(TECHBS) \\
\quad TECHBS\{((div, sys, eqp, com, core), tech_{base})\} \\
\quad tech_{base} \in HTECS \\
\quad tech_1 = tech_{base} \\
\quad ((div, sys, eqp, com, core), \{tech_1\}) \notin ATQS \\
\quad ATQS' = ATQS \cup \{((div, sys, eqp, com, core), \{tech_1\})\} \\
\quad \left(\begin{array}{c} \forall tech_i \in HTECS \circ tech_1 \succcurlyeq tech_i \\ \Longrightarrow ATQS' = ATQS \cup \{((div, sys, eqp, com, core), \{tech_i\})\} \end{array} \right)^* \\
\quad ATQS = \{((div, sys, eqp, com, core), \{tech_1 \ldots tech_i\})\}
\end{array}$$

AddAssignTechQ: This command is to add a new technical qualification element. The command is valid only if the new element is not already a member of $ATQS$. It is to be updated. The following schema describes this command:

$$\begin{array}{l}
AddAssignTechQ\left(((div, sys, eqp, com, core), tech_i)\right) \\
\quad tech_i \in HTECS \\
\quad ((div, sys, eqp, com, core), \{tech_i\}) \notin ATQS \\
\quad ATQS' = ATQS \cup \{((div, sys, eqp, com, core), \{tech_i\})\}
\end{array}$$

DeAssignTechQ: This command is to delete an existing technical qualification element. The command is valid only if the new element is a member of $ATQS$. It is to be updated. The following schema describes this command:

$$
\begin{array}{l}
DeAssignTechQ\left(\left((div, sys, eqp, com, core), tech_i\right)\right) \\
\quad tech_i \in HTECS \\
\quad \left((div, sys, eqp, com, core), \{tech_i\}\right) \notin ATQS \\
\quad ATQS' = ATQS \setminus \left\{\left((div, sys, eqp, com, core), \{tech_i\}\right)\right\}
\end{array}
$$

2.7 Mapping Specifications for OBAC

This section presents the specifications for the *mappings* in the OBAC Specifications, with respective to Figure 2.11. This includes the user-work mapping, the user-role qualifications mapping, the user-field qualifications mapping, and the user-technical qualifications mapping.

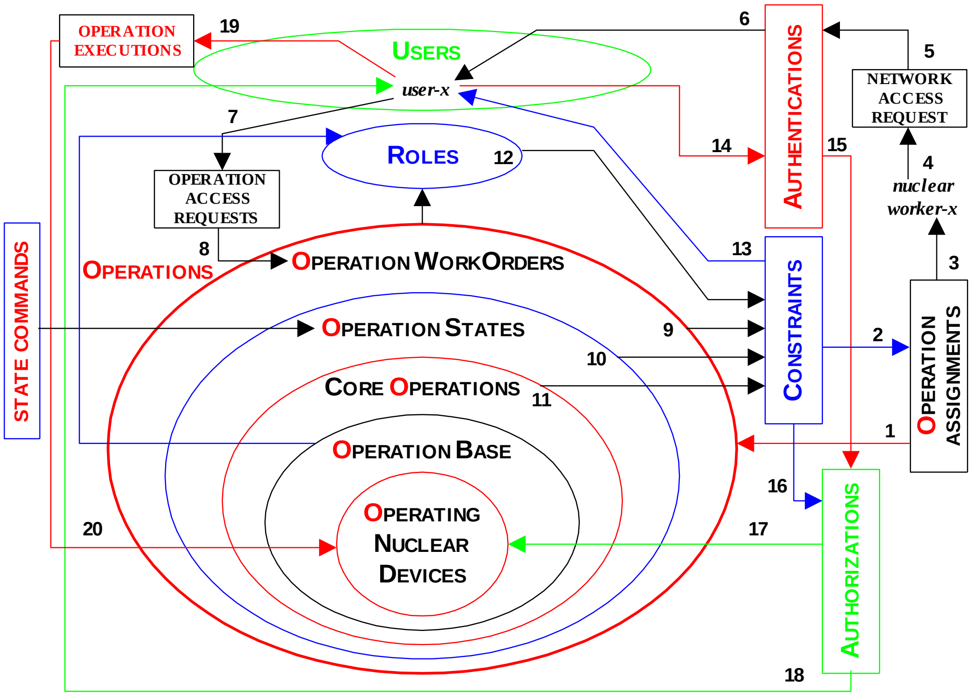


Figure 2.11: OBAC flow of access controls

MapSpec.-1: ***user-work*** *mapping for access controls*

MapSpec.-1 defines the specification for the mapping of work orders to the users who are assigned for carrying out the work orders.

- *Data Sets*: Define the data sets for the user-work mapping.

$UWS\{(user, WORKS, NONOP)\}$: USER-WORK MAPPING

- *User-Work elements*:

MapUW: This command is to map work elements to users, as described in following schema:

$$
\begin{aligned}
&MapUW(user, WORKS)\\
&\quad user \in USERS\\
&\quad WORKS\{(div, sys, eqp, com, work, wstate)\}\\
&\quad NONOPS\{(div, sys, eqp, com, core, state)\}\\
&\quad WORKS \neq NONOPS\\
&\quad UWS' = UWS \cup \{(user, (div, sys, eqp, com, work))\}
\end{aligned}
$$

MapSpec.-2: ***user-role qualifications*** *mapping for access controls*

MapSpec.-2 defines the specification for the mapping of role-experience qualifications to the users who are assigned for carrying out the work orders.

- *Data Sets*: Define the data sets for the user-role qualifications mapping.

$URS\{(UWS, ARQS)\}$: USER-ROLE Qualification MAPPING

- *User-Role elements*:

MapURQ: This command is to map role elements to users, as described in following schema:

$$
\begin{aligned}
&MapURQ(UWS, ARQS)\\
&\quad UWS\{(user, (div, sys, eqp, com, work))\}\\
&\quad ARQS\{((div, sys, eqp, com, core), \{role_1 \ldots . role_i\})\}\\
&\quad \forall(div, sys, eqp, com, core) = (div, sys, eqp, com, work)\\
&\quad \Rightarrow URS' = URS \cup \{(user, ((div, sys, eqp, com, core), \{role_1 \ldots . role_i\}))\}
\end{aligned}
$$

MapSpec.-3: ***user-field qualifications*** *mapping for access controls*

MapSpec.-3 defines the specification for the mapping of the field-experience qualifications to the users who are assigned for carrying out the work orders.

- *Data Sets*: Define the data sets for the user-field qualifications mapping.

$UFS\{(UWS, AFQS)\}$: USER-FIELD Qualification MAPPING

- *User-Field elements*:

MapUFQ: This command is to map field elements to users, as described in following schema:

$$MapUFQ(UWS, AFQS)$$

$$UWS\{(user, (div, sys, eqp, com, work))\}$$

$$AFQS\{((div, sys, eqp, com, core), \{field_1 \ldots. field_i\})\}$$

$$\forall (div, sys, eqp, com, core) = (div, sys, eqp, com, work)$$

$$\Longrightarrow UFS' = UFS \cup \left\{\left(user, \left((div, sys, eqp, com, core), \{field_1 \ldots. field_i\}\right)\right)\right\}$$

MapSpec.-4: ***user-technical qualifications*** *mapping for access controls*

MapSpec.-4 defines the specification for the mapping of the technical-experience qualifications to the users who are assigned for carrying out the work orders.

- *Data Sets*: Define the data sets for the user-technical qualifications mapping.

$UTS\{(UWS, ATQS)\}$: USER-TECHNICAL Qualification MAPPING

- *User-Technical elements*:

MapUTQ: This command is to map technical elements to users, as described in following schema:

$$MapUTQ(UWS, ATQS)$$

$$UWS\{(user, (div, sys, eqp, com, work))\}$$

$$ATQS\{((div, sys, eqp, com, core), \{tech_1 \ldots. tech_i\})\}$$

$$\forall (div, sys, eqp, com, core) = (div, sys, eqp, com, work)$$

$$\Longrightarrow UFS' = UFS \cup \left\{\left(user, \left((div, sys, eqp, com, core), \{tech_1 \ldots. tech_i\}\right)\right)\right\}$$

Chapter 3

SECURITY-INTEGRATED NUCLEAR PROCESS

Part 2: NUCLEAR OPERATION AUTHENTICATIONS

This thesis research has carried out a fundamental nuclear practices change, of the first-of-the-kind total network-based nuclear operations, for the two objectives: economic & efficiency advancements and safety & security enhancements for nuclear modernization. This chapter is focused on some aspects of safety & security enhancements of the creation of the total network-based nuclear operations.

This chapter presents a new authentication design for the nuclear process access controls termed as ***NOAA***, the *Nuclear Operation Access Authentication*.

This thesis is to research for a new security-integrated access control to the new formation of the network-based nuclear process termed as ***SNP***, the *Security-integrated Nuclear Process*. In this new *SNP*, any access to the operations and resources in the nuclear generating unit must pass two checks: the access authentication security check and the user experience and technical qualifications check. The qualifications check has been presented in chapter 2. This chapter is to describe the access authentication security check.

This chapter presents:

Section 3.1:	This section presents the basic criteria for the creation of *NOAA*, the *Nuclear Operation Access Authentication.*
Section 3.2:	This section presents the design of *APP*, the *Authentication Pre-access Protocol*.
Section 3.3:	This section presents the design of *AQP* the *Authentication Qualifications Protocol*.
Section 3.4:	This section presents the specifications of *APP* and *AQP* authentications.
Section 3.5:	This section presents the creation of the operation network pre-access authentication.

3.1 Nuclear Operation Access Authentication (NOAA)

This chapter is focused on the development of ***NOAA***, the *Nuclear Operation Access Authentication* for the secure control to the nuclear process operation network.

This section presents the basic criteria for the creation of the *NOAA*.

3.1.1 Basic Criteria for Creation of NOAA

In order to develop an effective access authentication system for the new conceptual full-scale network-based nuclear process operations, criteria for the development have to be first established to satisfy the network access security by verifying the identity of a user as a prerequisite for granting access to the SNP network as well as a necessary measure for preventing or rejecting unauthorized network access. The following establishes the Basic Criteria (*BC*) for the creation of this thesis' new design of ***NOAA***.

- Mutual authentication criterion

BC-1: Mutual authentication shall be used in the pre-access authentication.

  - A mutual (two-way) authentication shall be used between the users and the SNP authentication server for the SNP network *pre-access* authentication.
  - The users can ensure that they are not communicating with a malicious authentication server by authenticating the server. If this property is absent, a malicious authentication server may be able to mount a person/device-in-the-middle attack to gather data from the user.
  - The SNP authentication server can ensure that it is not communicating with a malicious user by authenticating the user. If this property is absent, a malicious user is able to access the SNP network.

- Unilateral authentication criterion

BC-2: Unilateral authentication shall be used in the user qualifications authentication.

  - A unilateral authentication shall be used between the users and the SNP authentication server for the user qualifications authentication.
  - The user qualifications authentication takes action after the user passed the pre-access authentication and already entered the SNP network, then a quick authentication process is carried out for technical, field-experience, or role-experience qualifications authentication.

- Public-private key-based authentication criterion

BC-3: Public-private key-based authentication shall be used in the pre-access authentication.

  - A public key is a cryptographic key used with a public key cryptographic algorithm. The public key is uniquely associated with its owner and may be made public. The key is used to verify a digital signature. The public key is mathematically linked with a corresponding private key.
  - A private is a cryptographic key used with a public key cryptographic algorithm. The private key is uniquely associated with its owner and is *not* made public. The key is used to generate a digital signature. The private key is mathematically linked with a corresponding public key.

- Random number challenge/digital signature-based authentication criterion

BC-4: Authentication shall use random number challenges and digital signatures.

  - The use of random number challenges and digital signatures eliminates the need for transmitting passwords for network access for authentication.
  - The use of digital signature reduces the 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 authentication makes computationally infeasible for an attacker to masquerade as another user.

- Auxiliary authentication criteria

BC-5: Authentication shall be high efficient.

Efficiency is crucial to achieve the high availability requirement in the real-time nuclear operations, and the authentication should not incur excess procedures and redundancy.

BC-6: Authentication shall be resilient to attacks.

Authentication schemes are required to resist malicious attacks, such as forgery attack, replay attack, and denial-of-service attack.

BC-7: Authentication shall minimize the use of passwords and require them be kept secure.

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 therefore the passwords must be kept secure.

3.1.2 *Nuclear Operation Access Authentication*

The new design of ***NOAA***, the *Nuclear Operation Access Authentication* composed of two parts: one is designed for pre-access authentication, and the other is designed for user's access qualifications authentication.

For the pre-access authentication, a new protocol termed ***APP***, the *Authentication Pre-access Protocol* is developed. The development of this protocol is detailed in sections 3.2, 3.4 and 3.5.

For the user's access qualification authentication, a simple protocol termed ***AQP***, the *Authentication of Qualifications Protocol* is developed. This protocol is to be shown in section 3.3 and 3.4.

The *NOAA* authentication system embedded with the two protocols, *APP* and *AQP*, is an integral part of ***SNP***, the *Security-integrated Nuclear Process*, which controls the security aspect of the new formation of network-based nuclear operations.

3.1.3 *Flow of access controls to SNP operation network*

The *NOAA* authentication system is integrated into the flow of ***OBAC***, the *Operation-Based Access Controls*, as shown in Figure 3.1.

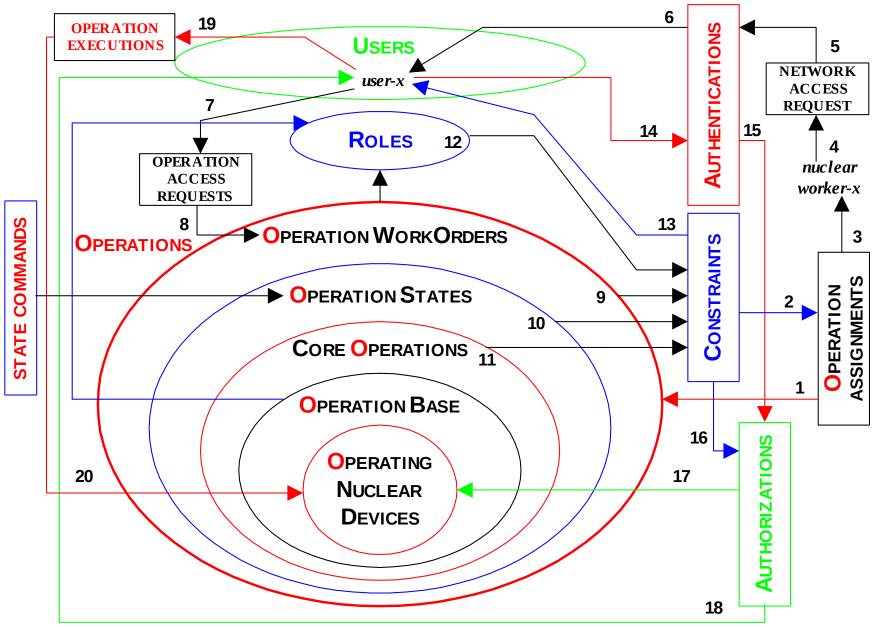


Figure 3.1: Flow of nuclear operation network access controls

- ***Pre-Access Authentication*** *in the access control flow*

The flow of the *OBAC* access controls starts with the assignment of operation work orders, where the work order authority may check the operation network (1) to get information of the current constraints and requirements for the work order to be assigned (2). The operation work order is to assign to the nuclear worker-*x* (3). The nuclear worker-*x* makes a network access request (4) and carries out pre-access authentication to validate the worker's access legitimacy (5). *The pre-access authentication part of the NOAA is applied with the APP protocol for the nuclear worker's access request authentication*.

- ***Qualifications Authentication*** *in the access control flow*

Then, the worker-*x* enter into the nuclear operation access network and becomes an authorized nuclear network user-*x* (6). The user-*x* makes an operation access request (7) to check the operation work-order access control (8) that generates the work-order validation and feedbacks as constraints (9). The operation work order access is mapped to the operation states that controls the work order access to the nuclear core operations and feedbacks as constraints (10). The work order is then mapped to the core operation access and generates the technical, field-experience and role-experience qualification requirements and feedbacks as constraints (11) and (12). Then all the access constraints/requirements are sent back to the user-*x* (13) to request for satisfying these access requirements. The user-*x* sends his/her qualification certificates for satisfying the access requirements to the authentication server (14). *The qualifications authentication part of the NOAA is applied with the AQP protocol.*

- ***NOAA completion*** *in the access control flow*

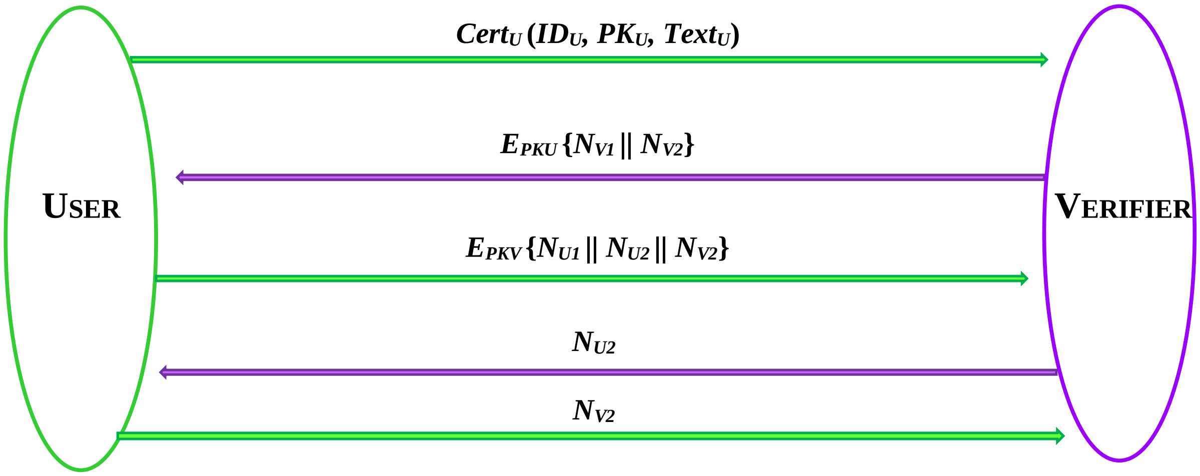
The server verifies the user-*x*' certificates and if they are verified (15), the authenticated certificates are sent to the authorization server where they are checked against the operation access requirements (16). If the check is passed, the authorization server sends an operation-access permit to the user-*x* (17) and to the nuclear device control to allow user-*x*' operation network access.

3.2 *APP* for Nuclear Operation Pre-Access Authentication

This thesis develops ***APP***, the *Authentication Pre-access Protocol* for authentication of nuclear workers who request to login the nuclear operation network for carrying out their assigned work orders. The development of the *APP* is detailed in section 3.5. The authentication steps in the *APP* procedure are given in Table 3.1 as well as displayed in Figure 3.2

Table 3.1: APP - the pre-access authentication

Steps	Transmission	Messages
1	User to Verifier Message$_{U\text{-}1}$:	$\boldsymbol{Cert_U\,(ID_U,\ PK_U,\ Text_U)}$
2	Verifier to User Message$_{V\text{-}1}$:	$\boldsymbol{E_{PKU}\,\{N_{V1} \,\|\, N_{V2}\}}$
3	User to Verifier Message$_{U\text{-}2}$:	$\boldsymbol{E_{PKV}\,\{N_{U1} \,\|\, N_{U2} \,\|\, N_{V2}\}}$
4	Verifier to User Message$_{V\text{-}2}$:	$\boldsymbol{N_{U2}}$
5	User to Verifier Message$_{U\text{-}3}$:	$\boldsymbol{N_{V2}}$



$Cert_U\,(ID_U,\ PK_U,\ Text_U)$
$E_{PKU}\,\{N_{V1} \| N_{V2}\}$
USER
VERIFIER
$E_{PKV}\,\{N_{U1} \| N_{U2} \| N_{V2}\}$
N_{U2}
N_{V2}

Figure 3.2: Pre-access authentication *APP* in *NOAA*

The *APP* pre-access authentication proceeds, as follows:

Step-1: *user-x U* sends his/her certificate $Cert_U$ that contains certificate identity ID_U, expire date, etc., public key PK_U, and optional text $Text_U$ to the verifier *V*:

Message $_{U\text{-}1}$: $\boldsymbol{Cert_U\,(ID_U,\ PK_U,\ Text_U)}$

Step-2: *V* verifies the digital signature of $Cert_U$ using the Certificate Authority's public key;

V generates two nonces N_{V1} and N_{V2}, if $Cert_U$ is verified;

V encrypts the two nonces using U's public key PK_U, and sends the encrypted values to *U*:

Message $_{V\text{-}1}$: $\boldsymbol{E_{PKU}\{N_{V1} \,||\, N_{V2}\}}$

Step-3: *U* decrypts Message $_{V\text{-}1}$ to obtain N_{V1} and N_{V2} using *U*'s private key;

U generates two nonces N_{U1} and N_{U2};

U encrypts the nonces using V's public key PK_V, and sends the encrypted values to *V*:

Message $_{U\text{-}2}$: $\boldsymbol{E_{PKV}\{N_{U1} \,||\, N_{U2} \,||\, N_{V2}\}}$

Step-4: *V* decrypts Message $_{U\text{-}2}$ to obtain N_{U1}, N_{U2} and N_{V2} using V's private key;

V sends N_{U2} to *U* for declaring "*U* is authenticated by *V*", if N_{V2} is the correct one that was sent by *V* in *Step-2*.

Message $_{V\text{-}2}$: $\boldsymbol{N_{U2}}$

Step-5: *U* sends N_{V2} to *V* for declaring "*V* is authenticated by *U*"

Message $_{U\text{-}3}$: $\boldsymbol{N_{V2}}$

Finally, *U* and *V* can use $\boldsymbol{\{N_{U1} \,||\, N_{V1}\}}$ to form a shared key for continue communication.

3.3 *AQP* for Nuclear Operation Access Qualifications Authentication

The ***AQP*** core operation qualifications authentication is carried out after the user's work order is validated and the work-order constraints of the role, field, and technical qualifications are fed back to the user. The user sends his/her qualification certificates to the SNP authentication server for authentication, in order to satisfy the work order constraints. The *AQP* authentications of the user's work-order's role, field, and technical qualifications are present in the following:

3.3.1 AQP Authentication of Role Qualifications

The role qualifications for the core operations are shown in Figure 3.3. There are 3 major groups of nuclear roles: operation group, engineering group and control maintenance group. Within each major group, there are medium groups and within each medium group, there are small groups (see chapter 4).

In response to *user-x*'s work order access request, the role qualifications are mapped to the work order assigned to *user-x*. Then these role qualification requirements corresponding to the *user-x*'s work order are fed as constraints back to *user-x*.

Then, *user-x* sent his/her role qualification certificates to the SNP authentication server for authentication.

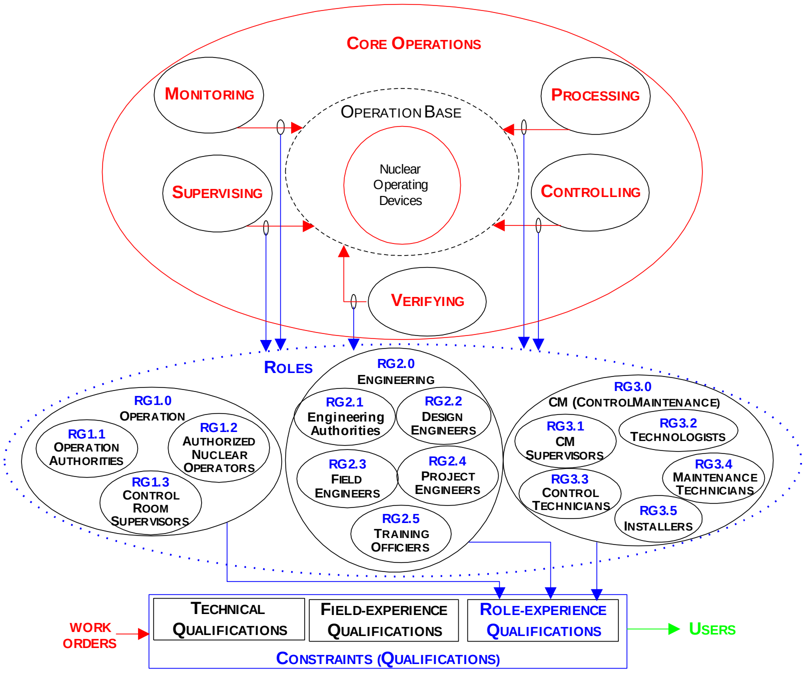

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
ROLES
RG1.0 OPERATION
RG1.1 OPERATION AUTHORITIES
RG1.2 AUTHORIZED NUCLEAR OPERATORS
RG1.3 CONTROL ROOM SUPERVISORS
RG2.0 ENGINEERING
RG2.1 Engineering Authorities
RG2.2 DESIGN ENGINEERS
RG2.3 FIELD ENGINEERS
RG2.4 PROJECT ENGINEERS
RG2.5 TRAINING OFFICIERS
RG3.0 CM (CONTROLMAINTENANCE)
RG3.1 CM SUPERVISORS
RG3.2 TECHNOLOGISTS
RG3.3 CONTROL TECHNICIANS
RG3.4 MAINTENANCE TECHNICIANS
RG3.5 INSTALLERS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 3.3: Nuclear roles for access controls

The *AQP* for *user-x*’s role qualification authentication proceeds as follows:

Step-1: *user-x*, *U* encrypts his/her *role-qualification certificate* $\boldsymbol{Cert}\ {}_{\boldsymbol{R}}\boldsymbol{n}_{-x}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to the verifier *V*, for authentication:

Message $_{\text{R-U}}$: $\boldsymbol{E}_{(N_{U1}N_{V1})}\{\boldsymbol{Cert}\ {}_{\boldsymbol{R}}\boldsymbol{n}_{-x}\}$

Step-2: After the authentication is past, *V* encrypts a code ${}_{\boldsymbol{R}}\boldsymbol{n}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to the operation authorization server *A*, for authorization:

Message $_{\text{R-V}}$: $\boldsymbol{E}_{(N_{U1}N_{V1})}\{{}_{\boldsymbol{R}}\boldsymbol{n}\}$

Step-3: After authorization, *A* encrypts a time-stamped role pass code ${}_{\boldsymbol{R}}\boldsymbol{n}_{-t}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to *U*:

Message $_{\text{R-A}}$: $\boldsymbol{E}_{(N_{U1}N_{V1})}\{{}_{\boldsymbol{R}}\boldsymbol{n}_{-t}\}$

Figure 3.4 shows the flow of *user-x*’s role-qualification authentication.

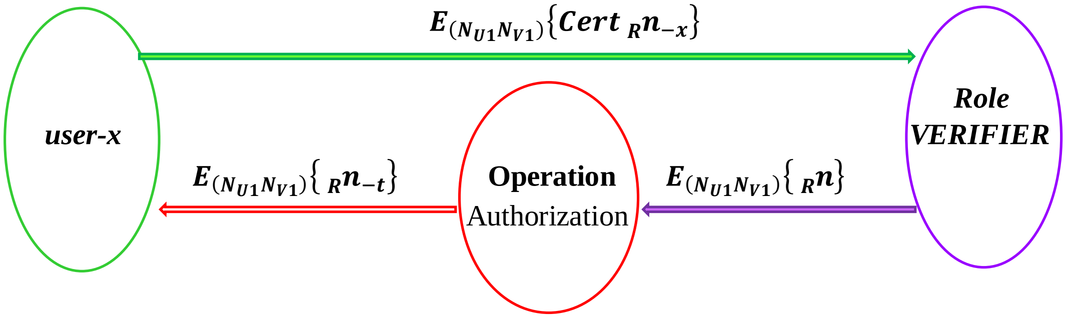

$\boldsymbol{E}_{(N_{U1}N_{V1})}\{\boldsymbol{Cert}\ {}_{\boldsymbol{R}}\boldsymbol{n}_{-x}\}$
user-x
Role VERIFIER
$\boldsymbol{E}_{(N_{U1}N_{V1})}\{{}_{\boldsymbol{R}}\boldsymbol{n}_{-t}\}$
Operation Authorization
$\boldsymbol{E}_{(N_{U1}N_{V1})}\{{}_{\boldsymbol{R}}\boldsymbol{n}\}$

Figure 3.4: Role-qualification authentication

3.3.2 AQP Authentication of Field Qualifications

The field qualifications for the core operations are shown in Figure 3.5. The field-experience qualifications can be assembled into 5 groups: FG1 on-line divisional-level op-exp., FG2 on-line system-level op-exp., FG3 on-line critical equipment op-exp., FG4 on-line non-critical equipment op-exp., and FG5 outage maintenance op-exp.

In response to *user-x*'s work order access request, the field qualifications are mapped to the work order assigned to *user-x*. Then these field qualification requirements corresponding to the *user-x*'s work order are fed as constraints back to *user-x*.

Then, *user-x* sent his/her field qualification certificates to the SNP authentication server for authentication.

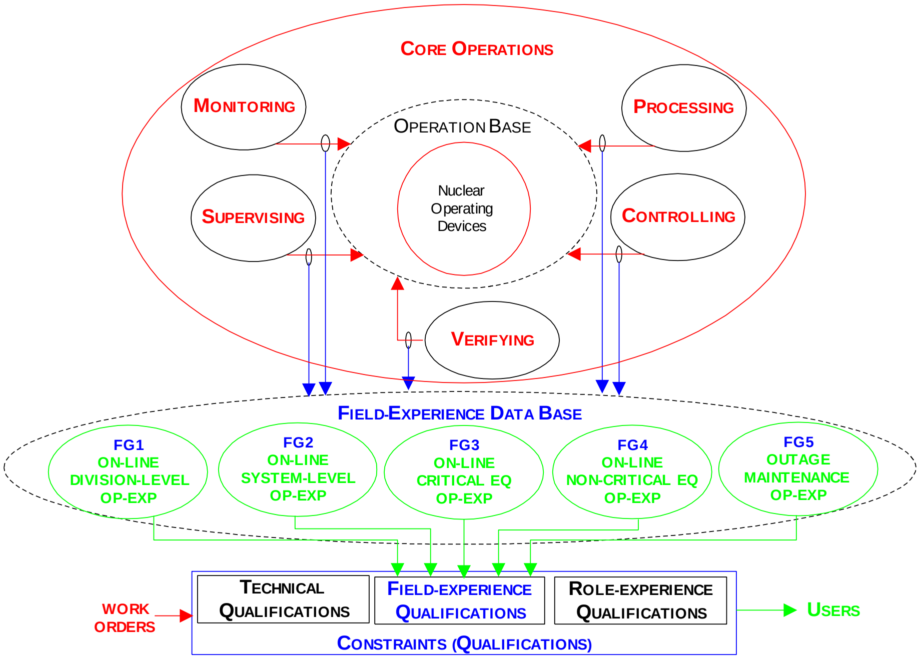

CORE OPERATIONS
MONITORING
OPERATION BASE
PROCESSING
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
USERS
CONSTRAINTS (QUALIFICATIONS)

Figure 3.5: Nuclear field qualification for access controls

The *AQP* for *user-x*'s field qualification authentication proceeds as follows:

Step-1: *user-x*, *U* encrypts his/her *field-qualification certificate* $\boldsymbol{Cert}\ _{\boldsymbol{F}}\boldsymbol{n}_{-\boldsymbol{x}}$ using the two nonces $(\boldsymbol{N_{U1}}, \boldsymbol{N_{V1}})$, and then sends the encrypted values to the verifier *V*, for authentication:

Message $_{\text{F-U}}$: $\boldsymbol{E}_{(\boldsymbol{N_{U1}N_{V1}})}\{\boldsymbol{Cert}\ _{\boldsymbol{F}}\boldsymbol{n}_{-\boldsymbol{x}}\}$

Step-2: After the authentication is past, *V* encrypts a code $\boldsymbol{{}_{F}n}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to the operation authorization server *A*, for authorization:

Message $_{\text{F-V}}$: $\boldsymbol{E_{(N_{U1}N_{V1})}\{{}_{F}n\}}$

Step-3: After authorization, *A* encrypts a time-stamped field pass code $\boldsymbol{{}_{F}n_{-t}}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to *U*:

Message $_{\text{F-A}}$: $\boldsymbol{E_{(N_{U1}N_{V1})}\{{}_{F}n_{-t}\}}$

Figure 3.6 shows the flow of *user-x*'s field-qualification authentication.

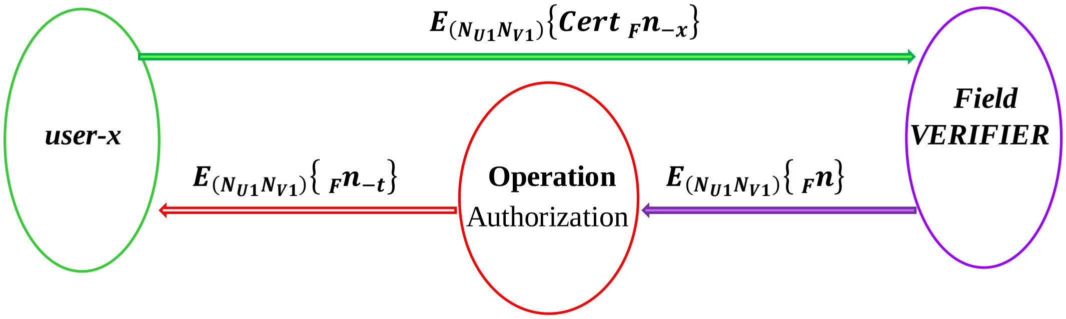

$\boldsymbol{E_{(N_{U1}N_{V1})}\{Cert\ {}_{F}n_{-x}\}}$
user-x
Field VERIFIER
$\boldsymbol{E_{(N_{U1}N_{V1})}\{{}_{F}n_{-t}\}}$
Operation Authorization
$\boldsymbol{E_{(N_{U1}N_{V1})}\{{}_{F}n\}}$

Figure 3.6: Field-qualification authentication

3.3.3 AQP Authentication of Technical Qualifications

The technical qualifications for the core operations are shown in Figure 3.7. The nuclear technical trainings can be grouped into 4 groups: TG1 – nuclear awareness trainings; TG2 – nuclear practices trainings; TG3 – nuclear system process trainings; and TG4 – nuclear technologies trainings.

In response to *user-x*’s work order access request, the technical qualifications are mapped to the work order assigned to *user-x*. Then these technical qualification requirements corresponding to the *user-x*’s work order are fed as constraints back to *user-x*.

Then, *user-x* sent his/her technical qualification certificates to the SNP authentication server for authentication.

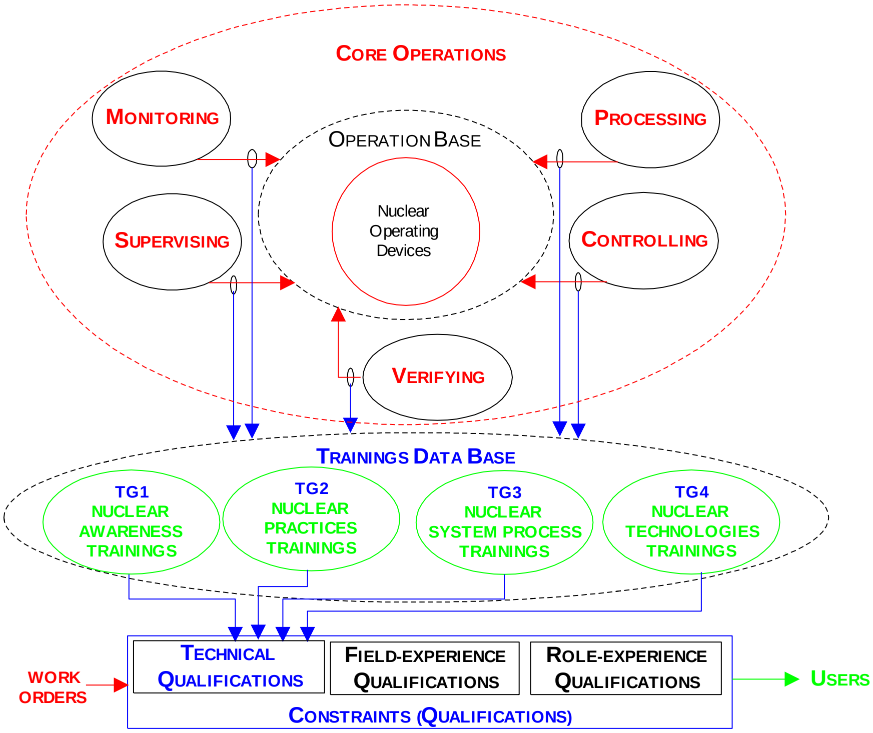

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
TRAININGS DATA BASE
TG1 NUCLEAR AWARENESS TRAININGS
TG2 NUCLEAR PRACTICES TRAININGS
TG3 NUCLEAR SYSTEM PROCESS TRAININGS
TG4 NUCLEAR TECHNOLOGIES TRAININGS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS

Figure 3.7: Nuclear technical qualification for access controls

The *AQP* for *user-x*’s technical qualification authentication proceeds as follows:

Step-1: *user-x*, *U* encrypts his/her *technical-qualification certificate* $\boldsymbol{Cert}\ _{T}\boldsymbol{n}_{-x}$ using the two nonces (N_{U1}, N_{V1}), and then sends the encrypted values to the verifier *V*, for authentication:

$$\text{Message}_{\text{T-U}}: \quad \boldsymbol{E}_{(N_{U1}N_{V1})}\{\boldsymbol{Cert}\ _{T}\boldsymbol{n}_{-x}\}$$

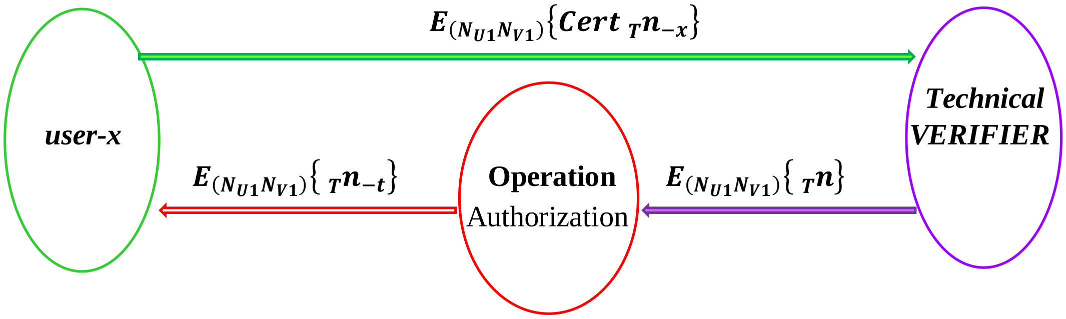
Step-2: After the authentication is past, *V* encrypts a code $_{T}\boldsymbol{n}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to the operation authorization server *A*, for authorization:

Message$_{\text{T-V}}$: $\boldsymbol{E}_{(\boldsymbol{N}_{U1}\boldsymbol{N}_{V1})}\{\,_{T}\boldsymbol{n}\}$

Step-3: After authorization, *A* encrypts a time-stamped technical pass code $_{T}\boldsymbol{n}_{-t}$ using the two nonces ($\boldsymbol{N_{U1}}$, $\boldsymbol{N_{V1}}$), and then sends the encrypted values to *U*:

Message$_{\text{T-A}}$: $\boldsymbol{E}_{(\boldsymbol{N}_{U1}\boldsymbol{N}_{V1})}\{\,_{T}\boldsymbol{n}_{-t}\}$

Figure 3.8 shows the flow of *user-x*'s technical-qualification authentication.



$\boldsymbol{E}_{(\boldsymbol{N}_{U1}\boldsymbol{N}_{V1})}\{\boldsymbol{Cert}\ _{T}\boldsymbol{n}_{-x}\}$
user-x
Technical VERIFIER
$\boldsymbol{E}_{(\boldsymbol{N}_{U1}\boldsymbol{N}_{V1})}\{\,_{T}\boldsymbol{n}_{-t}\}$
Operation Authorization
$\boldsymbol{E}_{(\boldsymbol{N}_{U1}\boldsymbol{N}_{V1})}\{\,_{T}\boldsymbol{n}\}$

Figure 3.8: Technical-qualification authentication

3.4 Specifications for Authentications

This section presents the specifications for the access authentication that consists of *APP pre-access* authentication specification and *AQP qualification* authentication specification. Abstract Syntax Notation One (ASN.1) and FIPS-196 notations are adopt for the specifications.

3.4.1 APP pre-access authentication specification

The following presents the specifications for the *APP* pre-access authentication.

- $\boldsymbol{Cert_U(ID_U, PK_U, Text_U)}$

```
CertU  ::= SEQUENCE  {
          certU                          CertificateP
}
```

- $\boldsymbol{Cert_V(ID_V, PK_V, Text_V)}$

```
CertV  ::= SEQUENCE  {
          certV                          CertificateP
}
```

```
CertificateP  ::= SIGNED   {SEQUENCE  {
          version                             Version
          serialNumber                        CertSerialNumber
          signature                           Signature
          issuer                              Issuer
          validity                            Validity
          publicKey                           PublicKey
          issuerInfo                          TEXT, OPTION
}
```

```
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
```

3.4.2 AQP qualification authentication specification

The following presents the specifications for the *AQP* qualifications authentication.

- Role qualification certificate: **Cert-$_{R}$n$_{-x}$**

```
CertR  ::= SEQUENCE  {
          cert-Rn                      CertificateR
}
```

```
CertificateR  ::= SIGNED   {SEQUENCE  {
          version                               Version
          serialNumber                          CertSerialNumber
          issuer                                Issuer
          validity                              Validity
          role                                  Role
}
```

- Field qualification certificate: **Cert-$_{F}$n$_{-x}$**

```
CertF  ::= SEQUENCE  {
          cert-Fn                      CertificateF
}
```

```
CertificateF  ::= SIGNED   {SEQUENCE  {
          version                               Version
          serialNumber                          CertSerialNumber
          issuer                                Issuer
          validity                              Validity
          field                                 Field
}
```

- Technical qualification certificate: **Cert-$_{T}$n$_{-x}$**

```
CertT  ::= SEQUENCE  {
          cert-Tn                      CertificateT
}
```

```
CertificateT  ::= SIGNED   {SEQUENCE  {
          version                               Version
          serialNumber                          CertSerialNumber
          issuer                                Issuer
          validity                              Validity
          tech                                  Tech
}
```

```
Version  ::= INTEGER
```

```
CertSerialNumber  ::= INTEGER
```

```
Issuer  ::= ALPHANUMERIC
```

```
Validity  ::= SEQUENCE  {
          notBefore                   Time
          notAfter                    Time
}
```

```
Role  ::=  SEQUENCE  {
          roleId                      INTEGER
          roleText                    BIT STRING
}
```

```
Field  ::=  SEQUENCE  {
          fieldId                     INTEGER
          fieldText                   BIT STRING
}
```

```
Tech  ::=  SEQUENCE  {
          techId                      INTEGER
          techText                    BIT STRING
}
```

3.5 Current States of Process Network Access Authentication

This section presents this thesis research findings on the assessment of the current state of process network access authentication. This assessment is to lay out the background for the design ***NOAA*** that is exclusively developed for the access security control to CANDU nuclear power electricity generating processes and is eventually contributed for realization of nuclear unit operations modernization in this thesis research.

3.5.1 *Authentication – Basics and Network Applications*

Authentication is a procedure of verifying the identity of a user as a prerequisite for granting access to a communication network as well as a necessary measure for preventing or rejecting unauthorized network access. Many authentication protocols have been proposed for general network applications, for wired networks [27-28] or wireless networks [29-31]. There are a few authentication protocols designed for power systems, such as for smart grid meter authentications [32-33]. An overview of authentication basics and applications is given below:

Authentication Protocols for Wired Networks: As a typical protocol developed for wired network, Kerberos [27] is a network authentication protocol that works on the basis of *tickets* to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aim primarily at a client-server model and it provides mutual authentication that both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

Authentication with Hardware for Wired Networks: The RSA SecurID [28] employs hardware tokens to authenticate user. The hardware token stores secrets in a tamper-resistant module carried by the user. The simplest dedicated-hardware version has only a display and no buttons. Each instance of the device holds a secret “seed” known to the back-end. A cryptographically strong transform generates a new 6-digit code from this secret every 60 seconds. The current code is shown on the device’s display. On enrollment, the user connects to the administrative back-end through a web interface, where the user selects a PIN and where the pairing between username and token is confirmed. From then on, for authenticating, instead of username and password, the user shall type username and “passcode” that is a concatenation of a static 4-digit PIN and a dynamic 6-digit code.

Authentication Protocols for Wireless Networks: As a typical protocol developed for wireless network, a Protocol for carrying Authentication for Network Access (PANA) [29] enables authentication between clients and access networks in Wireless Local Area Networks. PANA runs between a client and a server to perform authentication and authorization for the network access service. PANA does not define any new authentication mechanism but performs authentication protocol of IEEE Std. 802.11. In cellular networks, assuming that a client roams from a home network to a foreign network, the client needs to be authenticated by the foreign network. The foreign network must communicate with the client's home network via multi-hop communications to authenticate the client [30]. The subscriber identification module card of a client and the authentication center of the client's home network are pre-installed with a shared secret key K. When the client roams to a foreign network, the foreign network must communicate with the client's home network in order to obtain the shared key K that will then be used to authenticate the client. In the handover authentication protocol of IEEE Std. 802.11i, after the authentication server successfully authenticates a mobile client, it will send a key called pairwise master key to the access point associated with the client. The client will perform the same calculation as the authentication server to obtain the same pairwise master key. The access point and client will use the pairwise master key to derive a pairwise transient key for encrypting future packets exchanged between them [31]. The authentication server then sends the pairwise master key to the neighbors of the current access point, one by one. The pairwise master key serves as proof of the client's successful login authentication performed by the authentication server. By letting the authentication server pre-distribute the pairwise master key to the neighbors of the current access point, the client will not need to be authenticated by the authentication server when it moves to another access point.

Authentication Protocols for Smart Grids: Some authentication protocols for smart grids have been proposed, for example a light-weight and secure message authentication mechanism [32]. This proposed mechanism is based on Diffie-Hellman key establishment protocol and hash-based message authentication code, which allows various smart meters at different points of the smart grids to make mutual authentication and achieve message authentication with low latency and few signal message exchanges. Another authentication scheme is proposed to employ the Merkle hash tree technique to secure smart gird communication [33]. Specifically the proposed protocol considers the smart meters with computation-constrained resources and puts the minimum computation overhead on them.

Authentication Protocols using Public-Key Cryptography: The authentication protocol to be designed in this thesis for users of a nuclear site to access critical process with nuclear safety requirements needs high level of security as well as high efficiency for real-time nuclear operations. The protocol is therefore based on public key cryptography.

Transport Layer Security: The International Electrotechnical Commission (IEC) standard IEC61850 [22] is developed for power substation automation, and this IEC standard recommends Transport Layer Security [25], a public-key based authentication protocol, to achieve secure communications. However, transport layer security has two weaknesses: 1) it is not efficient, and 2) the key updates are vulnerable.

Authentication Protocols for Power Systems: The authentication protocol for the power system applications shall meet the following requirements [23]:

High Efficiency: Efficiency is crucial to achieve the high availability requirement in real-time power system applications. The indication of high efficiency is two-fold: 1) the authentication schemes should not incur too much redundancy for security; and 2) computation involved in authentication must be fast enough to meet timing requirements of messages in the power systems.

Resilient to Attacks: Authentication schemes are required to resist malicious attacks, such as forgery attack, replay attack, and denial-of-service attack.

Mutual Authentication: Mutual authentication is a two-way authentication process between a user and the authentication server. The users ensure that they are not communicating with a malicious authentication server by authenticating the server. If this property is absent, a malicious authentication server may be able to mount a person/device-in-the-middle attack to gather private messages from the user. The authentication server also needs to authenticate the client to ensure that the server is communicating with a valid user. The authentication server ensures that the server is not communicating with a malicious client by authenticating the client. If this property is absent, a malicious user is able to access the network without authentication.

The authentication protocol for the nuclear power application must ensure with full security attributes for data integrity during authentication process and with no effects on subsequent nuclear operation safety. A new public key-based authentication protocol will be proposed below in this chapter. In chapter 4, the security analysis is to be carried to show that the proposed protocol is resilient to attacks, and the performance analysis is to be conducted to demonstrate that the proposed protocol has higher efficiency than the standard transport layer security.

3.5.2 *State-of-the-Art Authentication Protocol for IT Networks*

This thesis research identifies that the Federal Information Processing Standards (FIPS) publication, *FIPS-196*: *Entity Authentication Using Public Key Cryptography* [23] is a good source for the study of the computer communication network authentication. This standard, however, is designed for general IT network applications and cannot be directly employed for nuclear process access authentication. Nevertheless, this standard provides state-of-the-art protocol and is a good reference for the research and development of a new authentication protocol best suitable for the secure access to the nuclear process and real-time operations, as one objective in this thesis research.

The standard FIPS-196 specifies two challenge-response protocols by which the user and the verifier may authenticate their identities to one another. The authentication uses public key cryptography, digital signatures, and random number challengers. The pubic key-based authentication has advantages over other authentication schemes as no secret information is shared by the user or the verifier during the authentication information exchange. A user to be authenticated must use a private key to digitally sign a random number challenge issued by the verifier. This random number is a time variant parameter and is unique to the authentication information exchange. If the verifier can successfully verify the signed response using the user's public key, then the user is successfully authenticated.

The FIPS-196 specifies two protocols for authentication that use a public key cryptographic algorithm for generating and verifying digital signatures. One can prove its identity to another by using a private key to generate a digital signature on a random challenge. The use of cryptography provides for strong authentication and does not require authenticating individuals to share secret information. The generation and verification of digital signatures are based on *FIBS 186-4*: *Digital Signature Standard* [24], an approved public key digital signature algorithm, and the authentication protocol is based on *ISO/IEC 9798-3*: *Entity authentication Part 3: Mechanisms using digital signature techniques* [25].

The authentication protocols are independent of the nature of the authenticating user or verifier such as the same protocol to be used for user-to-device and device-to-device authentication. The authentication of a user to a verifier depends on two successful actions: 1) the verification of the user's binding with its public-private key pair, and 2) the verification of the user's digital signature on a random number challenge. A binding of a user's unique identifier with its key pair is essential to proving the authenticity of the user's identity. The public key certificate is not required by this standard. Whether or not public key certificate is used, each public-private key pair shall be bound to a particular user.

During an authentication exchange, the verifier generates a random number challenge associated with the user's identifier. Then the user generates a signature on that challenge and the signature is freshly generated for this authentication exchange. For verification of the signature, the verifier uses the user's identifier to find a public key that is bound to that identifier, and if that public key can be used to successfully verify the user's signature on the challenge then the verifier has verified that the user is the one bound to the key pair. This chain of associations, bindings, and signatures leads to successful authentication.

The authentication protocol utilizes pseudorandom number for the authentication token's time variant parameters, authentication does not need to use synchronized clocks to verify the freshness and timeliness of authentication token. Random number challenges are generally easier to use in widely distributed environments where authenticating individuals do not necessarily know one another prior to authentication.

- *Access Security Concerns & Resolutions*

  The protocol can address threats including masquerade, password compromise, replay attacks, etc. by the following means:

  Use of challenges and digital signatures for authentication eliminates the need for transmitting passwords and therefore to reduce the passwords being compromised. Passwords however may still be used for users to access their private keys, and thus passwords must be kept secure.

  Use of public key cryptography eliminates the need for the authenticating individuals to share their secret values, and therefore it is extremely important to always keep the private keys secure and under the owners' sole control.

  Use of random number challenges prevents an intruder from copying an authentication token signed by another user and replaying it successfully at a later time. However, a new random number challenge should be generated for each authentication exchange. The security of replay prevention hinges on the generation of random number challenges that have a low probability of being duplicated.

  Use of a random number of its own in an authentication token allows the user to preclude the signing of only data that is pre-defined by the verifier. If a user uses its private key for more than just signing authentication tokens, then a verifier could maliciously create a challenge consisting of information which is meaningful in another context. This can be prevented when the user signs both the challenge and unpredictable, meaningless data - a random number.

  Other threats include denial of service, session capture, transmission modification, and compromised private key. No aspect of the authentication tokens or protocols preclude another entity from rerouting or modifying authentication transmissions. Maintaining the secrecy of the private key is of extreme importance and failure to do so may result in an attacker masquerading as the legitimate user by using the user's private key for authentication.

- *Authentication Protocol Considerations*

The following items are to be considered for initiating the authentication protocols:

Digital signatures: A user shall have a facility for generating a digital signature, and the verifier shall have a facility for verifying a digital signature, in accordance with FIPS-186.

Public-Private Key Pair: Each authenticating individual shall possess a public-private key pair that is compliant with the digital signature algorithm, and it is critical to the security of the authentication that the private key is accessible to only one individual.

Random numbers: In the authentication exchanges, the verifier uses a random number as a challenge to the user, and the user uses a random number to preclude signing only data determined by the verifier. A verifier must maintain state as knowledge of the original random number challenge is essential when the verifier attempts to verify the user's response. To maintain state during an authentication exchange, a verifier must keep a record of a freshly generated random number challenge and an association between that challenge and the user. Linking the user to the correct random number challenge is very important when the verifier is involved in several simultaneous authentication sessions.

Identifiers: The users and the verifiers shall determine their unique and distinguishing identifiers prior to initiating the authentication protocol. A naming convention shall be established such that a verifier can differentiate between all users, and each user shall have a unique identifier for each verifier. If authentication certificates are used, the naming convention used in identifying the individuals to one another during the authentication exchange does not have to be the same as the certificate naming convention. However, each individual must have some means of correlating a name in a certificate with the identifier used during authentication. An authentication token identifier is included with each token transmission, and the identifier indicates the type of the tokens and the authentication exchanges.

Public key certificates: The public key certificate shall be generated prior to the authentication exchange and shall be readily accessible to an individual that is to authenticate another individual's identity. A certificate is usually generated by a trusted third party and then distributed or stored where the authenticating individuals have access to it. The certificate can be retrieved from a directory server prior to the authentication exchange. During the authentication exchange, the token is sent with the certificate. To verify the binding between the user and the user's public key, a verifier shall have access to a valid and verifiable certificate issued by a trusted third party whose public key is known to the verifier. Failure of any verification in the certificate shall result in a failure to verify the signature on the user's certificate.

If certificates are not used, the user's public key and any global variables necessary for signature verification shall be exchanged prior to initiating the authentication exchange. A trusted third party may be used by a verifier to obtain a user's public key. Each individual for performing authentication verifications may choose to maintain a public key database.

Optional fields: The authentication token may include an optional text field containing data that does not have to be signed. The information included in the unsigned portion of a token is not guaranteed for data integrity. It is recommended that a signature be generated over all information included in a token. The number of different types of data in each optional field is not limited.

Text fields: The use of the text fields should be carefully implemented as the use may create vulnerabilities in the authentication exchange. The text fields may contain a) *Identifiers*: A user may choose to include an identifier in the text field of a token. If certificates are not used to distribute a user's public key, then the user is required to include information identifying it in the authentication token. b) *Time value* – A time variant parameter may be included in a token's text field, in addition to the random challenge used to determine the user's authenticity. However, this additional value shall not replace the random number as the verifier's challenge to the user. For example, a time value may be included in a token for access control auditing, if tokens are logged by a verifier upon successful completion of an authentication exchange. c) *Key exchange data* – The text fields may include information used to distribute a cryptographic key. For example, an encrypted session key or information used in establishing a session key may be included in the text field. The key shall not be used until each user in the exchange has been successfully authenticated.

3.5.3 *Nuclear Operation Access Authentication (NOAA)*

This thesis research develops a new design for nuclear process access authentication system, termed *NOAA*, the *Nuclear Operation Access Authentication.* The design development has considered the authentication application requirements, concerns, resolutions, etc. discussed in section 3.1.

The design of nuclear process access authentication must be, for real-time nuclear operations that are critical due to nuclear safety, high efficient and resilient to attacks. A design objective is to minimize the latency of the authentication protocol, specifically to minimize the burden of message exchanges between the user and the verifier and key operations by the user and the verifier while achieving high resilient to all kinds of possible attacks.

- ***New Authentication Pre-access Protocol***

A new protocol termed the *Authentication Pre-access Protocol* (***APP***) is developed for the *NOAA* system. The ***APP*** proceeds as follows:

Step-1: *nuclear worker-x U* sends its certificate to the verifier *V* for authentication;

Step-2: *V* generates two nonces, encrypts them using *U*'s public key, and sends them to *U*;

Step-3: *U* generates two nonces, encrypts them with one of *V*'s two nonces using *V*'s public key, and sends them to *V*;

Step-4: *V* sends one *U*'s nonce for declaring "*U* is authenticated by *V*";

Step-5: *U* sends one V's nonce for declaring "V is authenticated by U"

Finally, *U* and *V* can use N_{U1} and N_{V1} to form a shared key for continue communication.

- ***NOAA Security Analysis***

The new design of *NOAA* authentication is resilient to cyber-attacks, in particular the forgery attacks and replay attacks. The prevention of these attacks by the *NOAA* is analyzed below.

Forgery Attacks

The forgery attack is an attack in which an attacker deliberately manipulate data. This type of attacks can be prevented by using digital signatures and message encryption. The public key certificate in *Step-1* of *NOAA* authentication uses digital signature to prevent forgery attacks. The digital signature ensures that user's certificate is protected against modifications and that counterfeit messages are infeasible to be fabricated. Any unauthorized changes to the content of the certificate will result in an incorrect signature value because the attacker does not know Certificate Authority's private key to forge the user's original certificate.

Step-2 and *Step-3* of *NOAA* authentication use encryption to prevent forgery attacks. The encrypted messages are protected against modifications. Any changes to the content of the messages will result in the messages that are unable be decrypted successfully by the recipient.

Replay Attacks

An attacker records messages of an ongoing authentication session and then replays these messages in the future in an attempt to be successfully authenticated and possibly gain access to the network as the legitimate user. An attacker may replay the user's messages to gain access to the network or replay the verifier's messages to impersonate the verifier. The *NOAA* prevents the replay attacks by using nonces. A nonce is a random number that is only used for one time [34]. A new message must use newly generated nonces and must not repeat using those that have been sent previously. If a message with nonces was lost or damaged, the message is retransmitted, but the retransmitted message must use newly generated nonces. The following presents an analysis of two possible replay attacks:

Replay User Messages: Even if an attacker has effectively overheard messages of *Step-1*, *Step-3*, and *Step-5* sent by the user, the attacker cannot successfully do the replays as the user, because of the following scenario.

After having received the message of *Step-1* and satisfied with the user's certificate, the verifier replies the user with an encrypted message, $E_{PKU}\{N_{V1} \| N_{V2}\}$ in *Step-2*, including the verifier's two newly generated nonces and the encryption uses the user's public key. The attacker cannot decrypt the message $E_{PKU}\{N_{V1} \| N_{V2}\}$ because the attacker does not have the private key of the user, and therefore the attacker does not know the two nonces N_{V1} and N_{V2}.

If the attacker replays (as the user) the message of *Step-3* with some number (other than N_{V1}) to the verifier, the verifier will immediately detect that it is a replayed message because the replayed message does not contain the nonce N_{V1} that the verifier expects (N_{V1} was sent by the verifier to the legitimate user in *Step-2*, which the attacker does not know as mentioned above).

Similarly, if the attacker replays (as the user) the message of *Step-5* to the verifier, the verifier can detect the replayed message because the verifier does not receive the expected nonce N_{V2}.

Replay Verifier Messages: Even if an attacker has effectively overheard messages of *Step-2* and *Step-4* sent by the verifier, the attacker cannot successfully do the replays as the verifier, because of the following scenario.

After having received the message of *Step-2* and satisfied with the verifier's certificate, the user replies the verifier with an encrypted message, $E_{PKV}\{N_{U1} \| N_{U2} \| N_{V2}\}$ in *Step-3*, including the user's two newly generated nonces and the encryption uses the verifier's public key. The attacker cannot decrypt the message $E_{PKV}\{N_{U1} \| N_{U2} \| N_{V2}\}$ because the attacker does not have the private key of the verifier, and therefore the attacker does not know the two nonces N_{U1} and N_{U2}.

If the attacker replays (as the verifier) the message of *Step-4* with some number (other than N_{U2}) to the user, the user will immediately detect that it is a replayed message because the replayed message does not contain the nonce N_{U2} that the user expects (N_{U2} was sent by the user to the legitimate verifier in *Step-3*, which the attacker does not know as mentioned above).

Chapter 4

SECURITY-INTEGRATED NUCLEAR PROCESS

Part 3: NUCLEAR PRACTICES TRANSFORMATION AND SNP DATA BASE

This thesis research has carried out the development of a fundamental transformation of current nuclear practices, of the first-of-the-kind creation of total network-based nuclear operations.

This chapter first presents the *SNP* transformation of the current nuclear practices on equipment performance monitoring, nuclear data processing, and equipment control and maintenance. Second, this chapter presents a case study for illustration of the *SNP* transformation of nuclear practices. Third, this chapter presents the creation of the nuclear network data base for the support of the *SNP* transformation.

The following lists the sections in this chapter:

Section 4.1:	This section first presents an overview of the nuclear safety concerns and current nuclear practices. Second, this section presents the *SNP* transformation of the current nuclear equipment monitoring and data processing practices. Third, this section presents the *SNP* transformation of the current nuclear equipment maintenance practices.
Section 4.2:	This section presents a case study for illustration of the *SNP* transformation of nuclear practices, in the area of carrying out the equipment performance monitoring, data processing, and control maintenance work orders.
Section 4.3:	This section presents the creation of the nuclear process real-time operation network base, as the first step for realization of the goals of *SNP* transformation on nuclear practices. This nuclear operation network base consists of the equipment monitoring operation data base, the processing operation data base, the controlling operation data base, and the supervising data base.
Section 4.4:	This section presents the certificates base for role, field, and technical qualifications.

4.1 SNP Transformation of Current Nuclear Practices

This section first presents an overview of the nuclear safety concerns and current nuclear practices. Second, this section presents the *SNP* transformation of the current nuclear equipment monitoring and data processing practices. Third, this section presents the *SNP* transformation of the current nuclear equipment maintenance practices.

4.1.1 Overview of Current Nuclear Practices

Intelligent process control equipment of various kinds from simple devices to complex systems, such as from standalone smart valve positioners to state-of-the-art 800MW generator automatic control systems are available for modernization of nuclear process operations, and many of them are already physically installed in the nuclear generating stations. These smart process control equipment have networking capability with intelligent features for central data processing, devices/equipment/systems operations optimizing and coordinating, predictive maintenance scheduling, etc. However, most of the network-based intelligent features in these equipment are deliberately disabled or their network-based capabilities are severely limited intentionally due to security concerns in the nuclear operating environment. Nuclear security concerns if ignored will have extremely serious consequences to public and employees' health and safety. This thesis research is to seek security-concerns resolutions for safe use of networks for nuclear operations.

In the current state due to pending nuclear safety concerns, *first*, millions dollars of potential savings every year from utilizing modern intelligent equipment's networking and computing capabilities and associated benefits cannot be realized; *second*, the replacement of obsolete equipment with newer equipment having intelligent (smart) networking features is not necessary a preference in the expensive nuclear refurbishment unless no equivalence to the obsolete ones can be found, and the equivalent equipment are in general of older technology; *third*, the continued use of equipment of old technology leads to sluggish performance, bulky and energy inefficiency, non/limited on-line diagnosis, intensive maintenance, etc. This results in labour intensive and costly in operating and maintaining equipment of older technologies. This thesis research is to contribute to the secure use of equipment of today's technology with networking capability for on-line diagnosis, operations coordinating, predictive maintenance scheduling, etc.

The current practices for nuclear equipment operations and maintenance are fairly inefficient, labour-intensive and costly, from today's smart system and technology point of view. To date, there are still numerous analog devices and discrete digital devices that were built with older technologies operating in the nuclear plants. In today's nuclear practices, an obsolete device is preferable to be replaced by an equivalent one usually of older technology. Even if the modern smart equipment have to be adopted due to unavailability of equivalent replacements, the modern intelligent features with networking capability were mostly either disabled or substantially limited due to security concerns. In particular, the intelligent features including central data processing, devices/equipment/systems operations optimizing and coordinating, predictive maintenance scheduling, etc. cannot be utilized for improving the efficiency of the nuclear operation and maintenance.

The following sections present the findings of this thesis research on the current practices for nuclear process operations, identifies the areas of weakness in the current practices of nuclear equipment performance monitoring and data processing, and sets the goals for the *SNP* transformation on nuclear practices for addressing the current nuclear operation weakness.

4.1.2 SNP Transformation of Current Nuclear Monitoring Operation

This section first presents this thesis research findings about the current practices on nuclear monitoring, and second presents the *SNP* transformation of current nuclear monitoring practices.

A great part of the nuclear operations is the monitoring of the performance of hundreds of nuclear devices in one nuclear unit. As of today there are still numerous analog or discrete digital devices of old technology operating in the nuclear plant and these devices generally require intensive labour care. Even if equipment made of newer technologies have been installed but their available networking capability is not used, these equipment are treated of no difference from the old devices.

4.1.2-1 ***Current Practices in Nuclear Devices Monitoring***

In the current nuclear generating station, most of the nuclear devices/equipment are being monitored in the older traditional fashion such as:

- The nuclear devices are divided in groups of similar technical functions, of close locations, or of the same nuclear systems. Then a certain number of nuclear operators/technical staff forming a team are responsible for a certain number of groups of nuclear devices.
- The formation of a team of nuclear operators responsible for a particular group of nuclear devices primarily depends on the discretions of the supervising management staff according to their understanding of the candidates' credential, trainings, and experiences, versus the requirements for the monitoring of the group of devices.

- The team of nuclear operators have been intensively trained with the detailed *operation* knowledge, but not necessary with the in-depth technical knowledge, of the devices that they are responsible for monitoring.
- Each team of nuclear operators work in shifts, with backup staff of the same required levels of trainings, for the 24-hour nuclear power electricity generation.
- Each team performs daily routine checks either in the control room or equipment rooms for critical signals monitoring or by conducting physical walkdowns to the device installations.
- Each team carries out daily routine recordings and data logs according to the established operation procedure. Each recording may involve three technical personnel: preparer, verifier, and approver.
- As most of the nuclear devices are discrete in implementations, the data collections from these devices become labour-intensive burdens. It is not uncommon that paper chart recorders are still in use for trend recordings of certain nuclear operation performances.
- If any data being recorded exceed their specified/expected ranges, the team will report them to their superiors for decisions, following the established procedures.
- In case of nuclear event happening, the team will follow the established procedures and will make as many recordings as the nuclear conditions permit, particularly not impacting the safety of the team members.

4.1.2-2 ***SNP transformation of practices on nuclear devices monitoring***

- *SNP transformation of nuclear monitoring*

Once the *SNP* network is established, the *SNP* nuclear equipment monitoring will be efficient, accurate, safe and economical (the economical aspect is to be demonstrated in chapter 5), by the following steps:

Step 1 – Set up a work order (see Figure 4.1).

According to *BaseSpec.-7* in section 2.4, the work order is of the following form:

$$WORKS\{(div, sys, eqp, com, work, wstate)\}$$

Enter device identity: *div*=division #, *sys*=system #, *eqp*=equipment #, *com*=component #

Enter core operation: *work* = M (monitoring), P (processing), C (controlling), S (supervising)

Enter operation state: *wstate* = RO (routine), EO (emergency), OL (on-line), OM (outage)

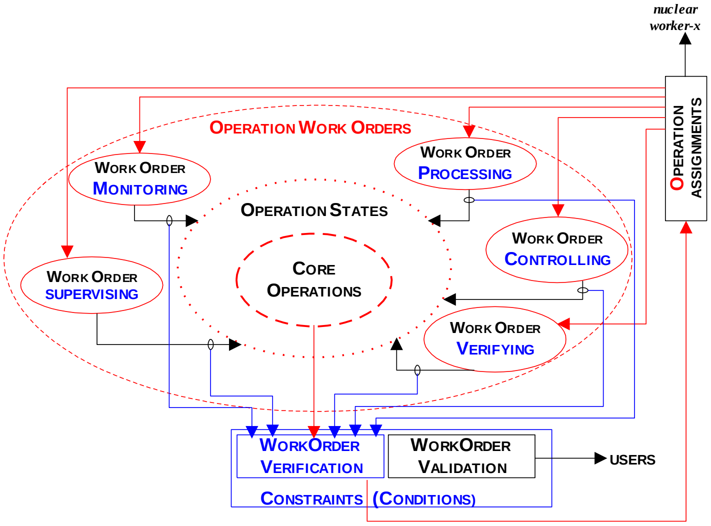


Figure 4.1: *SNP* work orders

Step 2 – obtain access requirements associated to the work order.

- Role-qualification access requirement (see Figure 4.2) – according to *AssgSpec.-1* in section 2.6, the requirement is of the following forms:

  $$ARQS\{((div, sys, eqp, com, core), \{role_1 \ldots role_i\})\}$$

  The role-qualification set $\{role_1 \ldots role_i\}$ is automatically mapped to the user.

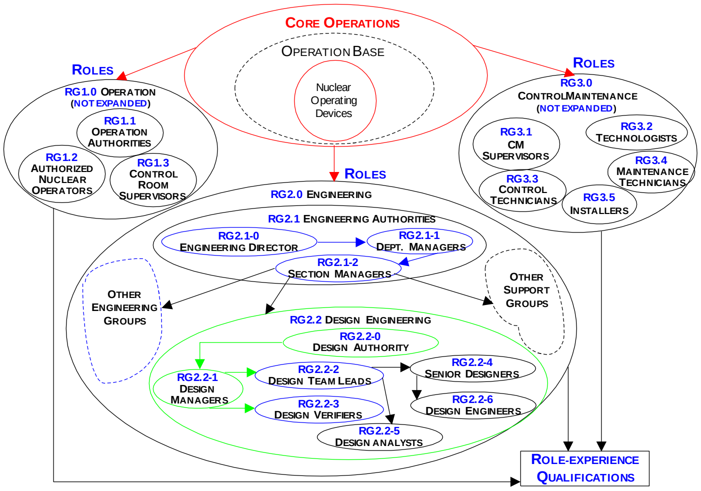


Figure 4.2: Role qualifications

- Field-qualification access requirement (see Figure 4.3) – according to *AssgSpec.-2* in section 2.6, the requirement is of the following forms:

  $$AFQS\{((div, sys, eqp, com, core), \{field_1 \ldots field_i\})\}$$

  The field-qualification set $\{field_1 \ldots field_i\}$ is automatically mapped to the user.

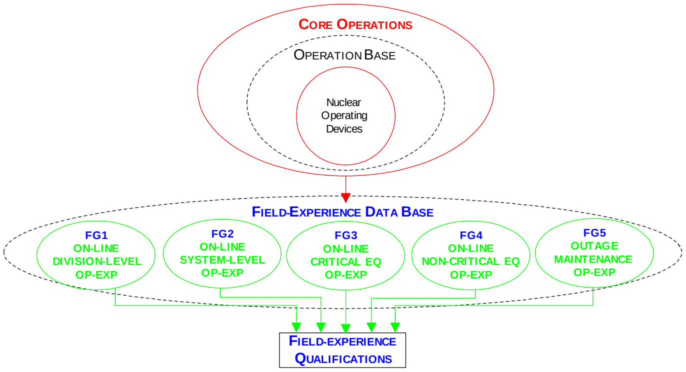

CORE OPERATIONS
OPERATION BASE
Nuclear Operating Devices
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
FIELD-EXPERIENCE QUALIFICATIONS

Figure 4.3: Field qualifications

- Technical-qualification access requirement (see Figure 4.4) – according to *AssgSpec.-3* in section 2.6, the requirement is of the following forms:

$$ATQS\{((div, sys, eqp, com, core), \{tech_1 \ldots tech_i\})\}$$

The technical-qualification set $\{tech_1 \ldots tech_i\}$ is automatically mapped to the user.

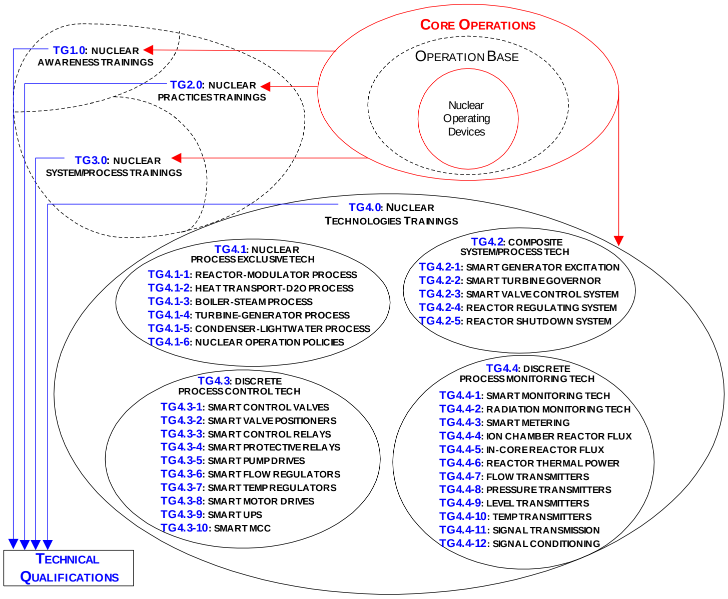

CORE OPERATIONS
OPERATION BASE
Nuclear Operating Devices
TG1.0: NUCLEAR AWARENESS TRAININGS
TG2.0: NUCLEAR PRACTICES TRAININGS
TG3.0: NUCLEAR SYSTEM/PROCESS TRAININGS
TG4.0: NUCLEAR TECHNOLOGIES TRAININGS
TG4.1: NUCLEAR PROCESS EXCLUSIVE TECH
TG4.1-1: REACTOR-MODULATOR PROCESS
TG4.1-2: HEAT TRANSPORT-D2O PROCESS
TG4.1-3: BOILER-STEAM PROCESS
TG4.1-4: TURBINE-GENERATOR PROCESS
TG4.1-5: CONDENSER-LIGHTWATER PROCESS
TG4.1-6: NUCLEAR OPERATION POLICIES
TG4.2: COMPOSITE SYSTEM/PROCESS TECH
TG4.2-1: SMART GENERATOR EXCITATION
TG4.2-2: SMART TURBINE GOVERNOR
TG4.2-3: SMART VALVE CONTROL SYSTEM
TG4.2-4: REACTOR REGULATING SYSTEM
TG4.2-5: REACTOR SHUTDOWN SYSTEM
TG4.3: DISCRETE PROCESS CONTROL TECH
TG4.3-1: SMART CONTROL VALVES
TG4.3-2: SMART VALVE POSITIONERS
TG4.3-3: SMART CONTROL RELAYS
TG4.3-4: SMART PROTECTIVE RELAYS
TG4.3-5: SMART PUMP DRIVES
TG4.3-6: SMART FLOW REGULATORS
TG4.3-7: SMART TEMP REGULATORS
TG4.3-8: SMART MOTOR DRIVES
TG4.3-9: SMART UPS
TG4.3-10: SMART MCC
TG4.4: DISCRETE PROCESS MONITORING TECH
TG4.4-1: SMART MONITORING TECH
TG4.4-2: RADIATION MONITORING TECH
TG4.4-3: SMART METERING
TG4.4-4: ION CHAMBER REACTOR FLUX
TG4.4-5: IN-CORE REACTOR FLUX
TG4.4-6: REACTOR THERMAL POWER
TG4.4-7: FLOW TRANSMITTERS
TG4.4-8: PRESSURE TRANSMITTERS
TG4.4-9: LEVEL TRANSMITTERS
TG4.4-10: TEMP TRANSMITTERS
TG4.4-11: SIGNAL TRANSMISSION
TG4.4-12: SIGNAL CONDITIONING
TECHNICAL QUALIFICATIONS

Figure 4.4: Technical qualifications

Step 3 – submit certificates of the required access qualifications for authentication.

According to section 3.3, users submit their work order-required certificates of role, field, and technical qualifications for authentication, as shown in Figure 4.5.

Step 4 – obtain authorization for access, after passing authentication.

Finally, the nuclear users can execute their work orders.

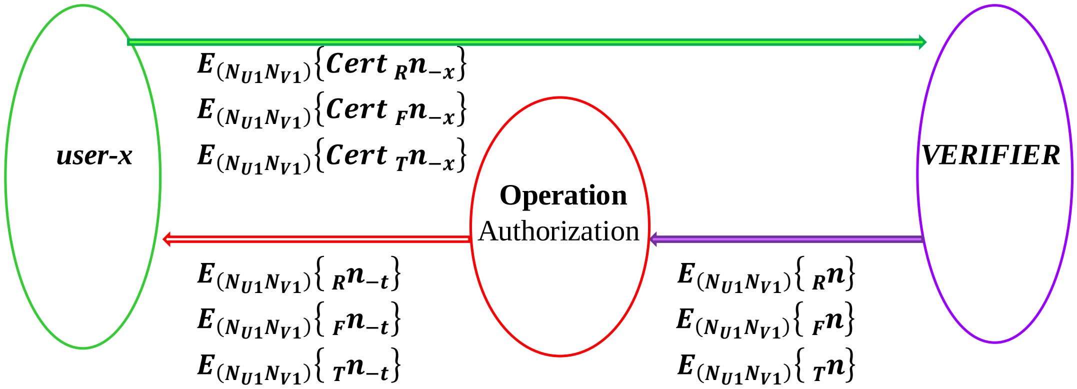

user-x
$E_{(N_{U1}N_{V1})}\{Cert\ _{R}n_{-x}\}$
$E_{(N_{U1}N_{V1})}\{Cert\ _{F}n_{-x}\}$
$E_{(N_{U1}N_{V1})}\{Cert\ _{T}n_{-x}\}$
Operation
Authorization
VERIFIER
$E_{(N_{U1}N_{V1})}\{\ _{R}n_{-t}\}$
$E_{(N_{U1}N_{V1})}\{\ _{F}n_{-t}\}$
$E_{(N_{U1}N_{V1})}\{\ _{T}n_{-t}\}$
$E_{(N_{U1}N_{V1})}\{\ _{R}n\}$
$E_{(N_{U1}N_{V1})}\{\ _{F}n\}$
$E_{(N_{U1}N_{V1})}\{\ _{T}n\}$

Figure 4.5: Role-qualification authentication

- *Goals of SNP on nuclear monitoring*

The *SNP* design is to facilitate nuclear devices monitoring, and its aims are:

- Increase the correctness and efficiency of formation of a team of operators responsible for certain groups of nuclear devices monitoring. This can reduce the reliance on the supervisors' discretions on the candidates' information (credential, training, experiences, etc.) that were "available" to them or they have to conduct an exhaustive search for the sufficient required information.
- Expand the availability of qualified operators for backups of a large number of groups of devices' monitoring by forming a *SNP* network base of which the required qualifications of a candidate can be verified automatically, instead of depending on the supervisors' decisions. This is equivalent to reduction of the backup reserve requirements, leading to significant cost saving and/or work environment improvement such as flexible vacation allocation.
- Improve the efficiency of the nuclear devices monitoring and reduce the amount of monitoring work that includes reduction of physical walkdowns and daily routine recording effort, with the devices' data readily available from the formation of the *SNP* network base.
- Increase the awareness of the nuclear devices or systems' abnormal performance or out-of-range data and responsiveness to such conditions, through the *SNP* network base.
- Increase, during a nuclear event, the capability and the amount of data collection for post-event analysis. This can speed up the event resolution.

4.1.3 SNP transformation of current nuclear devices data processing

This section presents the *SNP* transformation of current nuclear devices data processing.

4.1.3-1 ***Current Practices in Nuclear Devices Processing***

The current practices for processing of nuclear operation data are fairly inefficient, labour-intensive and costly, due to numerous analog or discrete digital devices of old technology still operating in the nuclear plant or newer equipment with their networking capability limited because of safety concerns. The current nuclear device data processing faces the similar weakness and work environment as encountered in the nuclear device monitoring mentioned above, and the processing is also handled in the old traditional fashion.

4.1.3-2 ***SNP transformation of practices on nuclear devices data processing***

The *SNP* transformation for the nuclear devices data processing operations (similar to that for the monitoring operations) is summarized below.

Step 1 – Set up a work order.

Use this digital form of $WORKS\{(div, sys, eqp, com, P, wstate)\}$ and fill which devices to be processed.

Step 2 – obtain access requirements associated to the work order.

- Role-qualification set $\{role_1 \dots role_i\}$ from $ARQS\{((div, sys, eqp, com, core), \{role_1 \dots role_i\})\}$ is automatically mapped to the user.
- Field-qualification set $\{field_1 \dots field_i\}$ from $AFQS\{((div, sys, eqp, com, core), \{field_1 \dots field_i\})\}$ is automatically mapped to the user.
- Technical-qualification set $\{tech_1 \dots tech_i\}$from $ATQS\{((div, sys, eqp, com, core), \{tech_1 \dots tech_i\})\}$ is automatically mapped to the user.

Step 3 – submit certificates of the required access qualifications for authentication.

Step 4 – obtain authorization for access, after passing authentication.

The *SNP* design is to facilitate nuclear operation data processing. The *SNP* design is to create the base for the full use of today's smart process control equipment networking capability and intelligent features for central data processing, devices/equipment/systems operations optimizing and coordinating, predictive maintenance scheduling, etc.

4.1.4 SNP Transformation of Current Nuclear Equipment Maintenance Practices

This section presents the findings of this thesis research on the current practices for nuclear equipment maintenance, identifies the areas of weakness in the nuclear equipment maintenance, and sets the goals for the *SNP* transformation on nuclear practices to address the weakness.

4.1.4-1 Initiation of Nuclear Equipment Maintenance

The nuclear equipment maintenance includes setting adjustments, calibrations, replacements, etc. Most of the equipment maintenances are carried out during the nuclear unit outage; some may be carried out during the unit forced outage due to some events; some may be carried out during on-line live operation.

- *Current practices*

Of the current nuclear practices, the following conditions are for the nuclear equipment maintenance to be carried out:

- The equipment maintenance is usually carried out during the nuclear unit outage, of which the equipment will be re-calibrated or replaced if the calibration fails. During the outage, almost all equipment will undergo the maintenance of various kinds or degrees regardless of the operating status of particular equipment.
- The on-line equipment maintenance may be initiated due to the equipment performance deficiency of minor nature being alarmed or recorded during the on-line live operation, and the physical field assessment indicates that minor adjustments on the equipment settings are feasible/implementable and also are allowable by the established operation procedures for that equipment within the specified conditions.
- The on-line equipment maintenance cannot be initiated if the physical field assessment shows that the performance deficiency during the live operation substantially exceeds the permitted ranges, of which the on-line adjustment is not allowed or is not supported by the established procedure.
- The equipment maintenance may be delayed until the scheduled outage if the equipment deficiency is tolerable for the on-going operation conditions under which the equipment is being operated, upon a satisfactory physical field assessment. Then, the equipment will be put on alert and will be under intensive monitoring for further maintenance decisions.

- The equipment maintenance can be delayed until the scheduled outage even if a particular equipment fails but its failure will not cause an immediate nuclear safety concern or will not cause a nuclear system failure as its backup equipment takes over the control or operation.
- The on-line equipment maintenance decisions may depend upon the criticality of the function of the equipment in the nuclear process. For critical equipment, there is usually a two-out-three implementation of physical devices and control logics in the nuclear process, such that if two out of three independent equipment of the same kind fail, then the function of these equipment is declared to be unavailable or fail. Under this failure condition, the physical field assessment is carried out to determine the equipment maintenance decision.
- The equipment maintenance cannot be delayed if the physical field assessment demonstrates that the equipment deficiency or malfunction are going to cause a catastrophic failure of certain nuclear systems or even may potentially cause a nuclear safety event, then an on-line equipment maintenance or even a forced outage has to be initiated for fixing the deficiency of that equipment.
- The equipment maintenance is required to be carried out if there is a nuclear event that impacts on this particular equipment.

The nuclear outage is extremely expensive and it may cost up to $1million each day, for one nuclear unit, due to mainly loss of revenue and some overtime payments.

- *SNP design*

The *SNP* design is to increase the efficiency of equipment maintenance, to reduce the number of outages particularly those unscheduled forced outages, and to minimize the duration of each outage. The *SNP* network base is created in this thesis research to facilitate equipment operations and maintenance by utilizing the modern smart control process' intelligent features that includes the central data processing, equipment on-line monitoring and self-calibrating, operation optimizing and coordinating, predictive maintenance diagnosing and scheduling, etc. features.

4.1.4-2 Paper Work for Equipment Maintenance Three-Step Procedure

This section presents the finding of this thesis research on the current practices for nuclear equipment maintenance. The current practices are fairly inefficient, labour-intensive and costly, without fully utilizing the intelligent feature of today's smart control process systems and technologies. Of today's nuclear practices, the paper work requirement for initiation of equipment maintenance is tremendous, involving a typical three-step procedure for preparation, verification, and approval, as illustrated below.

- *Preparation - Paper Work*

When the performance of an equipment deteriorates out of its designed tolerance, an alarm will be initiated. The alarm of critical or emergency nature will draw an immediate attention of the control & maintenance (CM) staff who is responsible of this equipment. If the alarm is of minor nature, the CM staff will notice it during the routine work process. After the CM staff receive the equipment alarm, the staff start the physical field assessment. The field assessment could be fairly complex if the equipment is nuclear-safety-related equipment, or its installation is the radiation active zone, or its maintenance affects substantially other equipment, or even the inspection of its deficiency may impact on the health operations of other equipment.

If the physical field assessment carried out by the CM staff indicates that the equipment deficiency can be fixed with minor adjustments and such minor adjustments on the equipment settings are feasible/implementable and also are allowable by the established operation procedures for that equipment within the specified conditions, then the CM staff will prepare paper work for initiation of an on-line live equipment maintenance.

If the physical field assessment shows that the equipment performance deficiency during the live operation substantially exceeds the permitted ranges, of which the on-line adjustment is not allowed or is not supported by the established procedure, then the CM staff will prepare paper work for reporting the findings to their superiors for maintenance decisions.

If the field assessment shows that the equipment deficiency is tolerable for the on-going operation conditions under which the equipment is being operated and the equipment maintenance can be delayed until the scheduled outage, then the CM staff will put the equipment on alert for intensive monitoring of any further performance deterioration and prepare paper work for reporting the conditions to their superiors for further actions.

If the field assessment demonstrates that the equipment maintenance cannot be delayed because the equipment deficiency or malfunction are going to cause a catastrophic failure of certain nuclear systems or even may potentially cause a nuclear safety event, then the CM staff may recommend an on-line equipment maintenance or may report to their superiors for immediate actions if the deficiency condition is very serious that a forced outage may be warranted. The CM staff will prepare paper work if they recommend an on-line equipment maintenance.

The paper work and preparation time required for initiating an on-line equipment maintenance depends on the conditions of the equipment deficiency and its impacts on other equipment. It can be a simple scenario that the CM staff will:

- collect equipment performance information,
- conduct observations on the equipment deficiency,
- carry out field assessment of the deficiency conditions and impacts on other equipment,
- prepare an on-line equipment maintenance plan,
- prepare a back-out plan when the performance of deficient equipment or affected nuclear systems starts to deteriorate,
- submit the whole on-line equipment maintenance plan to an independent verifier for verification.

However, if the conditions of the equipment deficiency and its impacts on other equipment are beyond the scope of the CM staff's responsibility or their capability, the preparation of the on-line equipment maintenance may involve engineering department's input. Then in additional to the above preparation work list, the CM staff will

- provide the equipment performance information to the engineering department,
- seek advices from the engineering staff, and incorporate the advices into their on-line equipment maintenance plan.

- *Verification - Paper Work*

The equipment maintenance plan is required to be verified and accepted by an independent verifier. The verifier usually has extensive experiences on the subject equipment and is responsible for the technical contents of the maintenance plan. The verifier will:

- review the equipment maintenance plan,
- review equipment performance information relative to the plan,
- verify the plan that it can address the equipment deficiency conditions
- verify the plan that it has no foreseeable adverse impact on other equipment or other nuclear systems by reviewing relative documents, records, etc.

- *Approval - Paper Work*

The maintenance plan after passing the verification is sent to an approver for the final approval before plan execution. The approver is usually a person in the senior management. The responsibility of the approver is to ensure the plan satisfying nuclear regulations. The approver will:

- check the qualifications of the preparer, relative to the nature of the maintenance plan,
- check the qualifications of the verifier, with respect to the subject matter,
- check the maintenance plan to ensure it do not violate any nuclear regulations

- *SNP design*

The *SNP* design is to facilitate nuclear equipment maintenance and expedite the preparation, verification, and approval of the on-line maintenance plan. The *SNP* design aims to facilitate:

- *Preparation* – The *SNP* design will facilitate the intelligent features of smart equipment to make the equipment performance information readily available for the preparer to use for review of equipment performance track records and for assessment of the equipment deficiency. This eliminates the physical collection of equipment performance and physical field assessment of the equipment deficiency conditions. The *SNP* design will significantly speed up the preparation of the equipment maintenance plan. The time saving is especially important for the on-line live equipment maintenance as first, the equipment can resume rapidly its normal health operation and second, the longer the equipment deficiency is not corrected then the higher probability the deficiency may cause adverse impacts on other equipment or systems.
- *Verification* – The *SNP* design will expedite the verification work progress as the verifier can review the equipment deficiency data independently and simultaneously at the time the maintenance plan being prepared. This can significantly speed up the verification of on-line maintenance.
- *Approval* – The *SNP* design also will expedite the approval work as the approver can review the preparer's qualification and the verifier's expertize while the maintenance plan is being prepared, as their qualifications are made readily available with the *SNP* design. The approver can examine the maintenance plan with respect to the nuclear regulations while the plan is being verified.

4.1.4-3 Equipment Maintenance Execution

The current practices for the execution of nuclear equipment maintenance plans are fairly inefficient, labour-intensive and costly, from today's smart system and technology point of view.

- *Nuclear Practices for Equipment Maintenance Execution*

To date in the nuclear plant, the implementation of an equipment maintenance requires: 1) an equipment maintenance plan, 2) a work order, 3) maintenance work plan execution, and 4) operation authority's acceptance. The equipment maintenance plan has been mentioned above.

The formation of a work order is similar to, but much simpler than, that of a maintenance plan, and it still requires a preparer, a verifier, and an approver.

The execution of a maintenance work plan requires two teams (at least of two persons): one team for carrying out the maintenance work that includes installation, commissioning for new replacements, and testing; the other team for carrying out independent checking, monitoring, recording, etc.

The maintenance work order implementation is to be verified independently by the nuclear operators, and the completion of the work order requires the acceptance of the nuclear operation authority.

- *SNP design*

The *SNP* design aims to:

- facilitate the equipment maintenance execution,
- expedite the preparation, verification, and approval of work order,
- speed up the equipment replacements or adjustments, including commissioning, testing, etc.
- accelerate the acceptance by the operation authority.
- increase the efficiency of equipment maintenance,
- reduce the number of outages particularly those unscheduled forced outages,
- minimize the duration of each outage.

The cost of *SNP* implementation is a one-time cost and is only a small fraction of one day forced outage. The *SNP* design may avoid some forced outages and each forced outage may take a few days to complete. The *SNP* design may reduce substantially the duration of each scheduled outage that may take a month to complete. Therefore the cost of *SNP* is insignificant compared to the potential savings that it brings to the nuclear plant. This is to be illustrated in chapter 5.

4.1.4-4 SNP Transformation of Nuclear Equipment Maintenance Practices

The following presents the SNP transformation of nuclear practices.

The nuclear practices start with the assignment of operation work orders (see Figure 4.6):

- Work order authority checks the operation network (1) to get information of the current constraints/requirements for the work order to be assigned (2), and then assign the operation work order to the nuclear worker-x (3).
- Nuclear worker-x makes a network access request (4) and carries out pre-access authentication to validate the worker's access legitimacy (5) and then the worker-x enter into the nuclear operation access network and becomes an authorized nuclear network user-x (6).
- Nuclear user-x makes an operation access request (7) to check the operation work-order access control (8) that generates the work-order validation and feedbacks as constraints (9).
- The operation work order access is mapped to the operation states that controls the work order access to the nuclear core operations and feedbacks as constraints (10). The work order is then mapped to the core operation access and generates the technical, field-experience and role-experience qualification requirements and feedbacks as constraints (11) and (12).
- All the access constraints/requirements are sent back to the user-x (13) to request for satisfying these access requirements. The user-x sends qualification certificates for satisfying the access requirements to the authentication server (14).
- The server verifies the user-x' certificates and if they are verified (15), the authenticated certificates are sent to the authorization server where they are checked against the operation access requirements (16).
- If the check is passed, the authorization server informs the core nuclear operation control (17) and sends an operation-access permit to the user-*x* (18).
- The permit allows user-*x* to make work order operation execution (19) and finally user-*x* can access to the nuclear operation network to execute their assigned work orders (20).

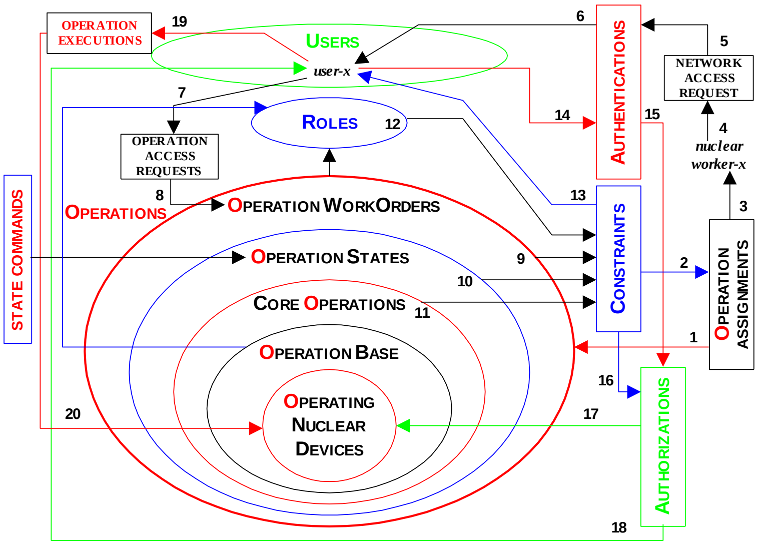


Figure 4.6: OBAC flow of access controls

Most of the above operations are network-assisted that transforms current labour-intensive practices.

4.2 Case Study for SNP Nuclear Practices Transformation

This section presents a case study for illustration of the *SNP* transformation of nuclear practices, in the area of carrying out the equipment performance monitoring, data processing, and control maintenance work orders. The illustration uses the work orders to be executed on a nuclear safety-related device, named the ion-chamber reactor flux detectors, in the nuclear reactor regulating system which is one of the most important system in the nuclear process.

This section presents the mappings of the work orders to the nuclear core operations, and the mappings of the work order requirements of technical qualifications and field and role experiences to the nuclear worker assigned to carry out the work orders.

4.2.1 CANDU Reactor Flux Detector

The work orders on the detection of the nuclear reactor flux/power are chosen for illustration of the *SNP* transformation of nuclear practices. In a typical CANDU nuclear unit, the flux of the reactor is measured by 3 ion-chamber nuclear reactor flux detectors. These detectors are located out of the calandria and they are used to measure the leakage neutron flux that is the flux leaking out from the nuclear reactor core and then, these detectors generate a signal that is proportional only to average nuclear reactor power as detected in that region of the nuclear reactor core. The ion-chamber nuclear reactor flux detector signals are not suitable for use as the control signal for the nuclear reactor regulation at high nuclear reactor power operation because the signal does not represent the flux in regions of the core of remote locations from the detector installation. The ion-chamber nuclear reactor flux detectors can accurately read very low values of neutron flux and provide a rational signal as low as 10-5% of full nuclear reactor power. These detectors can provide a signal representing the reactor power from 0 to 100% of full reactor power. However, these detectors offer poor resolution and therefore are not suitable for the control the reactor power control.

This illustration is to show the *SNP* access controls for the new conceptual formation of network-based work orders execution of the monitoring, data processing, and control maintenance operations on the ion-chamber nuclear reactor flux/power detectors.

4.2.2 SNP core operations on ion-chamber nuclear reactor flux detections

SNP Network Base:

This thesis research creates a *SNP Operation Network Base*, as given in section 4.3. This network base contains the data bases for all nuclear core operations that include the information of monitoring, processing and controlling of the ion-chamber nuclear reactor flux detectors as required for this illustration.

The core operations for the 3 ion-chamber nuclear reactor flux detector are listed in sections 4.3.2-1, 4.3.3-1 and 4.3.4-1 as shown below:

4.3.2-1 a) Calandria equipment – monitoring

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	M	3 ion-chamber reactor Flux detectors monitoring

4.3.3-1 a) Calandria equipment - processing

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	P	3 ion-chamber reactor Flux detectors processing

4.3.4-1 a) Calandria equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	C	3 ion-chamber reactor Flux detectors controlling

The above shows that the ion-chamber detectors are in *div=1* (division #1), *sys=1* (system #1), *eqp=1* (equipment #1), and *com=3* (3 detectors), and the core operations include *core*=M (Monitoring), *core*=P (Processing), and *core*=C (Controlling).

SNP Specifications Base:

The *OBAC Base Specifications* are given in section 2.4, of which *BaseSpec.-2* specifies the nuclear core operations. According to *BaseSpec.-2*, the *Monitoring*, *Processing*, and *Controlling* operations of the ion-chamber detector, say detector #2, are expressed, respectively, as:

$$CORES(1,1,1,2,M);\ CORES(1,1,1,2,P);\ CORES(1,1,1,2,C)$$

4.2.3 SNP access qualifications for ion-chamber nuclear reactor flux detections

- *SNP Access Qualification Base*

The core operations are linked to the *SNP Access Qualification Base*, as given in section 4.4.

The access to the equipment controlling operations, in general, has the highest qualification requirements compared with other operations because the controlling operation usually requires the highest skills for carrying the control work and may have the most serious consequence if it is not handled properly and therefore requires the uppermost experiences particularly for handling unexpected situations raised during the controlling operations. On the other hand, the access to the equipment monitoring operations has less qualification requirements, and the requirements for the access to the equipment data processing operations fall in between those for the monitoring operations and those for the controlling operations. In addition, the operations of the ion-chamber nuclear reactor flux/power detector is an integral part of the nuclear reactor regulating system that is a nuclear safety system. According to the regulation, the nuclear safety system requires the highest standard of operations regardless of the type of operations. Therefore $CORES(1,1,1,2,C)$ is linked to very high qualifications.

- *OBAC Qualification Base Specifications*

In section 2.4, *BaseSpec.-5* gives the format for the role qualification specifications:

$ROLEBS\{((div, sys, eqp, com, core), role_{base})\}$ where $role_{base}$ is the base role qualification

Any role qualification of equal or higher than $role_{base}$ can carry out that operation. The base role qualifications, with respect to engineering, for access to the monitoring, processing, and controlling operations on the ion-chamber nuclear reactor flux/power detectors are listed below, for illustration only (the precise determination of $role_{base}$ requires further investigations on the nuclear sites):

Controlling: $ROLEBS\left\{\left((1,1,1,2,C), RG2.3_{Cert_{R2.3.2}}, R2.2_{Cert_{R2.2.5}}\right)\right\}$

where $role_{base}$ = $RG2.3_{Cert_{R2.3.2}}$ (senior station engineers) or $R2.2_{Cert_{R2.2.5}}$ (senior design engineers)

Processing: $ROLEBS\left\{\left((1,1,1,2,P), RG2.3_{Cert_{R2.3.3}}, R2.2_{Cert_{R2.2.6}}\right)\right\}$

where $role_{base}$ = $RG2.3_{Cert_{R2.3.3}}$ (reactor-room engineers) or $R2.2_{Cert_{R2.2.6}}$ (design engineers)

Monitoring: $ROLEBS\left\{\left((1,1,1,2,M), R2.4_{Cert_{R2.4.2}}, RG2.3_{Cert_{R2.3.5}}, R2.2_{Cert_{R2.2.6}}\right)\right\}$

where $role_{base}$ = $R2.4_{Cert_{R2.4.2}}$ (senior project engineers) or $RG2.3_{Cert_{R2.3.5}}$ (equipment-room engineers) or $R2.2_{Cert_{R2.2.6}}$ (design engineers)

4.2.4 SNP access work orders for ion-chamber nuclear reactor flux detections

- *Work Order Specifications*

In section 2.4, *BaseSpec.-7* gives the format for the work order specifications:

$WORKS\{(div, sys, eqp, com, work, wstate)\}$

where *work* = M (monitoring), P (processing), C (controlling), V (verifying)
wstate = RO (routine operation), EO (emergency operation), OL (on-line maintenance), OM (outage maintenance)

This illustration is to carry out work orders on the ion-chamber nuclear reactor flux/power detectors. The work orders on detector #2 installed in division #1, system #1 and equipment #1 are expressed as:

Monitoring: $WORKS\{(1,1,1,2, M, wstate)\}$ where $wstate$ = RO or EO
Processing: $WORKS\{(1,1,1,2, P, wstate)\}$ where $wstate$ = RO or EO or OL
Controlling: $WORKS\{(1,1,1,2, C, wstate)\}$ where $wstate$ = OL or OM

- *Non-Operation Specifications*

In section 2.4, *BaseSpec.-6* provides the non-operation specification:

$NONOPS\{div, sys, eqp, com, core, state\}$

The operation authority can use this specification to stop the execution of any work order, for example:

$NONOPS\{1,1,1,2, C, NO\}$ ⇒ No, ion-chamber detector controlling operation is not allowed.
$NONOPS\{1,1,1,2, C, YES\}$ ⇒ Yes, ion-chamber detector controlling operation is allowed.

4.3 SNP Operation Network Base

This section presents the creation of the nuclear process real-time operation network base, as the first step for realization of the goals of *SNP* transformation on nuclear practices. This nuclear operation network base consists of the equipment monitoring operation data base, the processing operation data base, the controlling operation data base, and the supervising data base.

4.3.1 SNP Process Base and Authentication Base

In order to fully utilize the intelligent features of smart equipment for the real-time nuclear operations, a secure computer network must be established. The basic requirement for a secure network is the control of its access that is the focus of this thesis research. The network for the safe nuclear process operations must be configured first, starting from the network access point of view.

- ***Define SNP Process Base***

This thesis design defines the access to the nuclear process into four *SNP* levels. Each level is defined according to a typical physical CANDU nuclear process operations in the real on-line Ontario nuclear power plants producing hundreds of MW electricity. The four levels form the nuclear real-time operation network base.

Division-level nuclear process: $SNP\_\boldsymbol{D_n}$
System-level nuclear process: $SNP\_D_n\_\boldsymbol{S_n}$
Equipment-level nuclear process: $SNP\_D_n\_S_n\_\boldsymbol{E_n}$
Function-level nuclear process: $SNP\_D_n\_S_n\_E_n\_\boldsymbol{F_n}$

The functional level nuclear process defines the core operations outlined in chapter 2.

The following outlines the data sets for the nuclear divisions and their systems, as shown in Figure 4.7:

DIVIS **=** **{***calandria-moderator division*$_1$*; primary heat transport-heavy water division*$_2$*; boiler-steam division*$_3$*; turbine-generator division*$_4$*; condenser-light water division*$_5$**}**

SYSTS = **{***systs*$_1$*; systs*$_2$*; systs*$_3$*; systs*$_4$*; systs*$_5$**}**

systs*$_1$** = **{10 calandria-moderator key systems {reactor flux monitoring system, main moderator control system, liquid zone control system, reactivity adjuster control system, moderator liquid poison control system, reactor shutdown mechanical control system, moderator purification control system, cover gas control system, moderator heavy water sampling control system, moderator heavy water collection control system}***}**

systs*$_2$** = **{8 primary heat transport-heavy water key systems {primary heat transport main control system, feed bleed relief control system, purification control system, gland seal control system, deuterium addition control system, heavy-water collection control system, emergency coolant control system, heavy water supply control system}***}**

systs$_3$ = **{***8 boiler-steam key systems {boiler main steam supply control system, steam pressure control system, feedwater control system, chemical feed control system, extraction steam control system, deaerator start-up & poison prevent control system, feedwater heater drains control system, emergency cooling control system}***}**

systs$_4$ = **{***8 turbine-generator key systems {turbine steam control system, electrohydraulic governor control, live steam reheat control system, gland steam control system, low pressure cylinder exhaust cooling control system, extraction steam drains control system, generator lubricating control system, hydrogen cooling control system}***}**

systs$_5$ = **{***10 condenser-light water key systems {condenser main control system, makeup-reject control system, circulating water debris filtering control system, air extraction control system, service water control system, service water low pressure control system, service water high pressure control system, gland injection control system, water sampling control system, emergency water supply control system}***}**

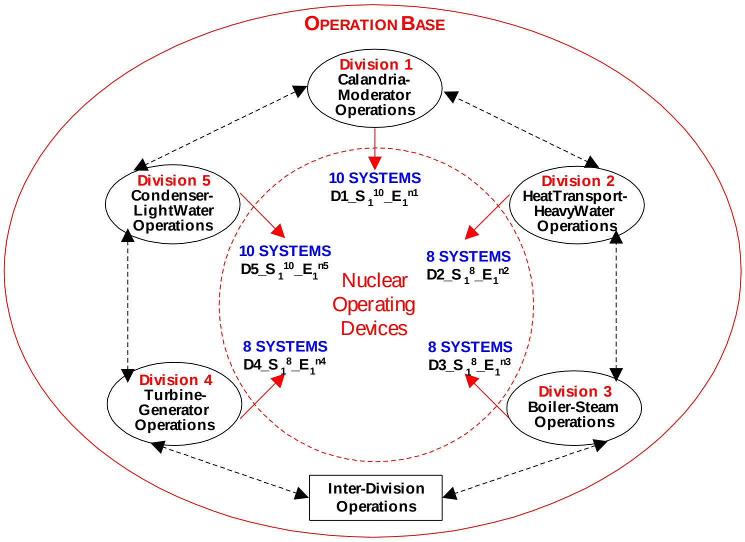


Figure 4.7: Nuclear divisions and divisional systems

- ***Define SNP Access Authentication Certification Base***

The following defines the *SNP* access authentication certification base that consists of digital certificates for users, roles, field, and technical qualifications:

Cert-$_{G\text{-}x}$: Prior to be authorized as a *user*, a person must pass Canadian government security checks, plus specific security checks required by the nuclear station being requested for access. The person (with a unique number *x*) is authorized by the organization as a general *user-x* and is issued with a unique digital certificate *Cert-*$_{G\text{-}x}$.

Cert-$_{Rn\text{-}x}$: Before a user can assume a certain nuclear ***Role-n***, the specialized user must possess the credentials and trainings required by that role and the authorizations from the user's superiors, and the *user-x* is issued with a unique digital certificate *Cert-*$_{Rn\text{-}x}$.

Cert-$_{Fn\text{-}x}$: Before a role can assume a certain nuclear ***Field-n*** experiences the user must possess that role and the most-recent trainings required by that operation, and the *user-x* is issued with a unique digital certificate *Cert-*$_{Fn\text{-}x}$.

Cert-$_{T}$***n***$_{-x}$: For each of the trainings that the user is credited with a pass nuclear ***Technical-n*** experiences, the user is issued with a digital certificate *Cert-*$_{Tn-x}$.

4.3.2 *Creation of Monitoring Data Base*

This section presents the creation of the data base for the nuclear equipment performance monitoring core operations, as shown in Figure 4.8 (for a quick illustration, only two divisions and only key equipment are listed below).

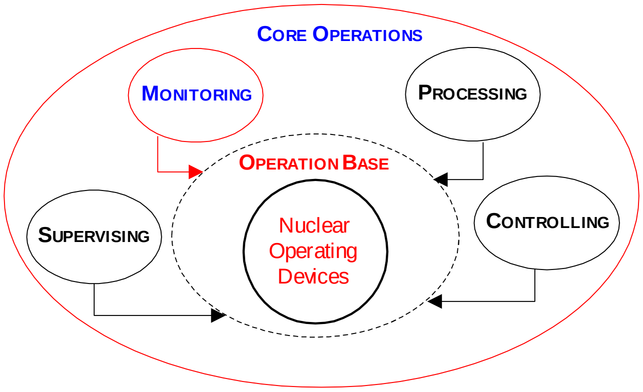


Figure 4.8: Monitoring core operations

4.3.2-1 Calandria-Moderator Monitoring

a) *Calandria equipment – monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	M	3 ion-chamber reactor Flux detectors monitoring access
1	1	2	28	M	28 in-core reactor Flux detectors monitoring access
1	1	3	7	M	7 reactor thermal power detectors monitoring access
1	1	6	3	M	3 startup instruments monitoring access

b) *Main moderator equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	2	1	5	M	5 moderator pumps on/off detectors monitoring access
1	2	1	6	M	5 moderator pumps tripping detectors monitoring access
1	2	1	30	M	30 moderator motor temperature detectors monitoring access
1	2	1	5	M	5 moderator pump motor oil level detectors monitoring access
1	2	1	5	M	5 moderator pump motor heater detectors monitoring access
1	2	1	6	M	5 moderator pump suction pressure detectors monitoring access
1	2	2	2	M	2 heat exchanger discharge flow detectors monitoring access
1	2	2	2	M	2 heat exchanger discharge pressure detectors monitoring access
1	2	3	1	M	1 moderator level (wide range) detector monitoring access
1	2	3	3	M	3 moderator level (narrow range) detectors monitoring access

c) *Liquid zone equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	3	1	3	M	3 liquid-zone light water pumps monitoring access
1	3	2	1	M	liquid zone heat exchanger temp detector monitoring access

1	3	3	2	M	2 helium compressors monitoring access
1	3	4	1	M	hydrogen and oxygen recombination device monitoring access

d) *Reactivity adjuster equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	4	1	1	M	adjuster motor drive monitoring access
1	4	2	21	M	21 adjuster position sensors monitoring access
1	4	3	1	M	adjuster shaft sealing sensor monitoring access

e) *Liquid poison equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	5	1	2	M	2 poison solution pumps monitoring access
1	5	2	2	M	2 tank poison quantity sensors monitoring access
1	5	3	2	M	2 tank level sensors monitoring access
1	5	4	2	M	2 tank poison solutions flow sensors monitoring access

f) *Reactor shutdown equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	6	1	1	M	high in-core neutron flux tripping detector monitoring access
1	6	1	1	M	high ion-chamber neutron flux tripping detector monitoring access
1	6	1	1	M	low gross coolant flow tripping detector monitoring access
1	6	1	1	M	heat transport pressure tripping detector monitoring access
1	6	1	1	M	heat transport outlet temperature tripping detector monitoring
1	6	1	1	M	low boiler level tripping detector monitoring access
1	6	1	1	M	boiler feedline low pressure tripping detector monitoring access
1	6	2	1	M	shutoff rod dropping device monitoring access
1	6	2	1	M	shutoff rod redrawing device monitoring access
1	6	2	1	M	shutoff rod promptness sensor monitoring access
1	6	2	1	M	shutoff rod hardware interlocking device monitoring access

g) *Moderator purification equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	7	1	1	M	ion exchanger flow control valve monitoring access
1	7	2	1	M	ion exchanger bypass control valve monitoring access
1	7	3	1	M	purification discharge flow sensor monitoring access
1	7	4	1	M	filter differential pressure sensors monitoring access
1	7	4	5	M	5 ion exchange columns pressure sensors monitoring access
1	7	4	1	M	discharge strainer differential pressure sensor monitoring access

h) *Moderator cover gas equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	8	1	2	M	2 moderator cover gas safety valves monitoring access
1	8	1	4	M	4 calandria rupture discs monitoring access
1	8	1	3	M	3 helium-oxygen pressure reducing valves monitoring access
1	8	1	1	M	instrument air safety valve monitoring access
1	8	1	1	M	instrument air safety valve monitoring access
1	8	2	2	M	2 containment isolation valves monitoring access
1	8	4	2	M	2 recombination unit preheaters monitoring access
1	8	5	1	M	moderator cover gas flow sensor monitoring access
1	8	5	1	M	moderator cover gas temperature sensor monitoring access

1	8	5	1	M	moderator cover gas pressure sensor monitoring access
1	8	6	1	M	cover gas supply isolation valve monitoring access
1	8	7	1	M	cover gas deuterium concentration sensor monitoring access

i) *Moderator heavy water sampling equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	9	1	1	M	moderator inlet heavy water sampling sensor monitoring access
1	9	1	1	M	purification outlet heavy water sampling sensor monitoring access
1	9	1	1	M	liquid poison heavy water sampling sensor monitoring access
1	9	1	1	M	heavy water collection discharge sampling sensor monitoring
1	9	1	1	M	heavy water recovery outlet sampling sensor monitoring access
1	9	2	1	M	heavy water purification sampling pump monitoring access
1	9	3	3	M	3 heavy water sampling isolation valves monitoring access

j) *Moderator heavy water collecting equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	10	1	1	M	heavy water collection pump monitoring access
1	10	2	1	M	heavy water collection discharge valve monitoring access
1	10	3	1	M	heavy water collection level sensor monitoring access

4.3.2-2 Primary Heat Transport Monitoring

a) *Heat transport circulating equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	1	1	16	M	16 main heat transport circulating pumps monitoring access
2	1	2	16	M	16 main circulating discharge valves monitoring access
2	1	3	24	M	24 steam generator isolation valves monitoring access
2	1	4	4	M	4 reactor outlet header circuit valves monitoring access

b) *Feed and bleed and relief equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	2	1	2	M	2 heat transport feed pumps monitoring access
2	2	2	2	M	2 bleed condenser heaters control sensors monitoring access
2	2	3	1	M	bleed condenser outlet valve monitoring access
2	2	4	1	M	bleed condenser off-gas management valve monitoring access
2	2	4	2	M	2 bleed condenser off-gas solenoid valves monitoring access
2	2	5	1	M	bleed condenser bypass valve monitoring access
2	2	5	1	M	bleed condenser inlet valve monitoring access
2	2	6	1	M	reactor outlet header pressure sensor monitoring access
2	2	6	2	M	2 reactor outlet header feed valves monitoring access
2	2	6	2	M	2 reactor outlet header bleed valves monitoring access
2	2	6	4	M	4 reactor outlet header cross connect valves monitoring access
2	2	7	1	M	bleed condenser pressure sensor monitoring access
2	2	7	1	M	reflux condenser control valve monitoring access
2	2	7	1	M	spray cooling control valve monitoring access
2	2	8	2	M	2 bleed cooler outlet temperature sensors monitoring access
2	2	8	2	M	2 bleed cooler outlet service water valves monitoring access
2	2	8	2	M	2 loss-of-coolant-accident solenoid valves monitoring access
2	2	9	2	M	2 bleed condenser level sensors monitoring access
2	2	9	2	M	2 bleed cooler outlet temperature sensors monitoring access
2	2	10	1	M	fuelling machine heavy water pressure sensor monitoring access
2	2	10	1	M	fuelling machine pressure control valve monitoring access
2	2	11	1	M	heat transport circuit overpressure sensor monitoring access

2	2	11	1	M	heat transport relief valves monitoring access

c) *Heat transport purification equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	3	1	1	M	purification bank inlet pressure sensor monitoring access
2	3	1	2	M	2 purification bank inlet isolating valve monitoring access
2	3	2	1	M	pressure across purification system sensor monitoring access
2	3	2	1	M	purification bypass valve monitoring access
2	3	3	1	M	purification flow temperature sensor monitoring access
2	3	3	1	M	ion exchange resin temperature sensor monitoring access
2	3	4	1	M	purification flow pressure override sensor monitoring access
2	3	4	1	M	purification pressure relief valve monitoring access
2	3	5	1	M	ion exchange lithium ion sensor monitoring access

d) *Heat transport gland sealing equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	4	1	1	M	gland supply flow sensors monitoring access
2	4	1	16	M	16 gland supply circulating pumps monitoring access
2	4	1	4	M	4 gland supply shutdown cooling pumps monitoring access
2	4	1	4	M	4 gland supply isolating valves monitoring access
2	4	2	1	M	gland return flow sensors monitoring access
2	4	2	1	M	gland return circulating pumps monitoring access
2	4	3	1	M	gland supply shutdown cooling pump monitoring access
2	4	4	1	M	gland recirculation cooler isolating valves monitoring access

e) *Heat transport hydrogen addition equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	5	1	1	M	hydrogen addition pressure sensors monitoring access
2	5	1	1	M	hydrogen addition isolating valves monitoring access
2	5	1	1	M	hydrogen addition pressure regulating valves monitoring access
2	5	2	1	M	hydrogen addition heavy water flow sensor monitoring access
2	5	2	1	M	hydrogen addition heavy water flow valve monitoring access
2	5	2	1	M	hydrogen addition heavy water isolating valve monitoring access
2	5	3	1	M	gas flow sensor monitoring access
2	5	3	1	M	pressure switch monitoring access

f) *Heat transport heavy water collection equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	6	1	1	M	heavy water collection tank level sensor monitoring access
2	6	1	4	M	4 heat transport heavy water collection pumps monitoring access
2	6	2	1	M	heavy water collection discharge valve monitoring access
2	6	3	1	M	leak-proof collection pumps monitoring access

g) *Heat transport emergency coolant injection equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	7	1	1	M	high-pressure injection flow sensor monitoring access
2	7	1	1	M	emergency coolant high-pressure pumps monitoring access
2	7	1	1	M	**(**emergency coolant injection valves monitoring access
2	7	1	1	M	emergency coolant injection test valves monitoring access
2	7	1	1	M	emergency coolant injection isolating valves monitoring access
2	7	1	1	M	emergency coolant tank level sensor monitoring access

2	7	1	1	M	emergency coolant injection flow sensor monitoring access
2	7	2	1	M	re-injection pumps monitoring access
2	7	2	1	M	re-injection recovery sump level sensor monitoring access
2	7	2	1	M	re-injection isolating valves monitoring access
2	7	3	1	M	recirculation flow sensor monitoring access
2	7	3	4	M	4 recirculation control valves monitoring access
2	7	3	2	M	2 recirculation isolating valves monitoring access
2	7	4	1	M	long-term recovery pumps monitoring access
2	7	4	1	M	long-term recovery isolating valves monitoring access
2	7	5	1	M	overpressure pressure sensors monitoring access
2	7	5	1	M	overpressure relief valves monitoring access

h) *Heat transport heavy water supply equipment - monitoring*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	8	1	2	M	2 heavy water supply pumps monitoring access
2	8	2	1	M	leak-proof heavy water pump monitoring access
2	8	2	1	M	backup tank level sensor monitoring access
2	8	3	3	M	3 thermal trip pump motor monitoring access

4.3.3 Creation of Processing Data Base

This section presents the creation of the data base for the nuclear equipment data *processing* core operations, as shown in Figure 4.9 (for a quick illustration, only two divisions and only key equipment are listed below).

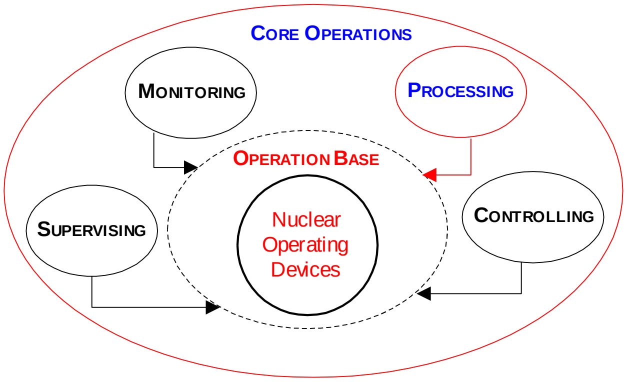


Figure 4.9: Processing core operations

4.3.3-1 Calandria-Moderator Processing

a) *Calandria equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	P	3 reactor power from ion-chamber flux processing access
1	1	4	7	P	7 thermal power-incore reactor power post-processor access
1	1	5	1	P	reactor power logarithm control post-processor processing access
1	1	5	1	P	reactor power linear control post-processor processing access
1	1	6	3	P	3 startup instrument signal processing access

b) *Main moderator equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	2	1	30	P	30 moderator motor temperature signals processing access
1	2	1	5	P	5 moderator pump suction pressure signals processing access
1	2	2	2	P	2 moderator heat exchanger flow signals processing access
1	2	2	2	P	2 moderator heat exchanger pressure signals processing access
1	2	3	1	P	1 moderator level (wide range) signals processing access
1	2	3	3	P	3 moderator levels (narrow range) signals processing access

c) *Liquid zone equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	3	2	1	P	liquid zone heat exchanger temperature signals processing access
1	3	3	2	P	2 helium compressors pressure signals processing access
1	3	4	1	P	hydrogen and oxygen recombination signals processing access

d) *Reactivity adjuster equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	4	2	21	P	21 adjuster positioning signals processing access
1	4	3	1	P	adjuster shaft sealing signal processing access

e) *Liquid poison equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	5	2	2	P	2 tank poison quantity sensor signals processing access
1	5	3	2	P	2 tank level sensor signals processing access

f) *Reactor shutdown equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	6	1	1	P	high in-core neutron flux tripping signal processing access
1	6	1	1	P	high ion-chamber neutron flux tripping signal processing access
1	6	1	1	P	low gross coolant flow tripping signal processing access
1	6	1	1	P	heat transport pressure tripping processing access
1	6	1	1	P	heat transport outlet temperature tripping processing access
1	6	1	1	P	low boiler level tripping processing access
1	6	1	1	P	boiler feedline low pressure tripping processing access
1	6	4	1	P	shutoff rod promptness processing access

g) *Moderator purification equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	7	3	1	P	purification discharge flow signals processing access
1	7	4	1	P	filter differential pressure signals processing access
1	7	4	5	P	5 ion exchange columns pressure signals processing access

h) *Moderator cover gas equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	8	5	1	P	moderator cover gas flow signal processing access
1	8	5	1	P	moderator cover gas temperature signal processing access
1	8	5	1	P	moderator cover gas pressure signal processing access
1	8	7	1	P	cover gas deuterium concentration signal processing access

i) *Moderator heavy water sampling equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	9	1	1	P	moderator inlet heavy water sampling signal processing access
1	9	1	1	P	purification outlet heavy water sampling signal processing access
1	9	1	1	P	liquid poison heavy water sampling signal processing access
1	9	1	1	P	heavy water collection discharge sampling signal processing access
1	9	1	1	P	heavy water recovery outlet sampling signal processing access

j) *Moderator heavy water collecting equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	10	3	1	P	heavy water collection level signal processing access

4.3.3-2 Primary Heat Transport Processing

a) *Heat transport circulating equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	1	1	16	P	16 main heat transport circulating signals processing access

b) *Feed and bleed and relief equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	2	2	2	P	2 bleed condenser heaters control signals processing access
2	2	4	1	P	bleed condenser off-gas management signal processing access
2	2	6	1	P	reactor outlet header pressure signal processing access
2	2	7	1	P	bleed condenser pressure signal processing access
2	2	8	2	P	2 bleed cooler outlet temperature signals processing access
2	2	9	2	P	2 bleed condenser level signals processing access
2	2	9	2	P	2 bleed cooler outlet temperature signals processing access
2	2	10	1	P	fuelling machine heavy water pressure signal processing access
2	2	11	1	P	heat transport main circuit overpressure signal processing access

c) *Heat transport purification equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	3	1	1	P	purification bank inlet pressure signal processing access
2	3	2	1	P	pressure across purification system signal processing access
2	3	3	1	P	purification flow temperature signal processing access
2	3	3	1	P	ion exchange resin temperature signal processing access
2	3	4	1	P	purification flow pressure override signal processing access
2	3	5	1	P	ion exchange lithium ion signal processing access

d) *Heat transport gland sealing equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	4	1	1	P	gland supply flow signals processing access
2	4	2	1	P	gland return flow signals processing access

e) *Heat transport hydrogen addition equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	5	1	1	P	hydrogen addition pressure signal processing access
2	5	2	1	P	hydrogen addition heavy water flow signal processing access
2	5	3	1	P	gas flow signal processing access

f) *Heat transport heavy water collection equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	6	1	1	P	heavy water collection tank level signal processing access

g) *Heat transport emergency coolant injection equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	7	1	1	P	high-pressure injection flow signal processing access
2	7	1	1	P	emergency coolant tank level signal processing access
2	7	1	1	P	emergency coolant injection flow signal processing access
2	7	2	1	P	re-injection recovery sump level signal processing access
2	7	3	1	P	recirculation flow signal processing access
2	7	5	1	P	overpressure pressure signal processing access

h) *Heat transport heavy water supply equipment - processing*

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	8	2	1	P	backup tank level signal processing access

4.3.4 Creation of Controlling Data Base

This section presents the creation of the data base for the nuclear equipment *controlling* core operations, as shown in Figure 4.10 (for a quick illustration, only two divisions and only key equipment are listed).

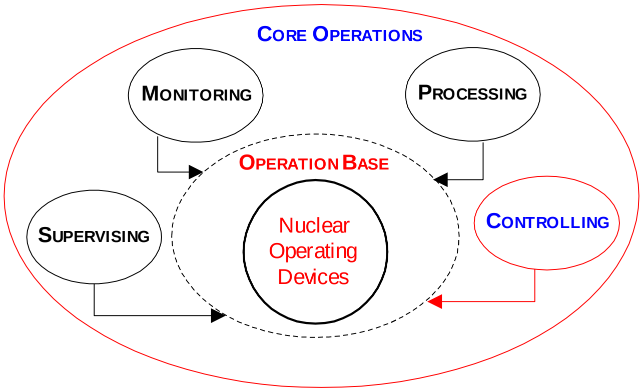


Figure 4.10: Controlling core operations

4.3.4-1 Calandria-Moderator Controlling

a) *Calandria equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	3	C	3 ion-chamber reactor Flux detectors control
1	1	2	28	C	28 in-core reactor Flux detectors control
1	1	3	7	C	7 reactor thermal power detectors control
1	1	6	3	C	3 startup instruments control

b) *Main moderator equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	2	1	5	C	5 moderator pumps on/off detectors control
1	2	1	5	C	5 moderator pumps tripping detectors control
1	2	1	30	C	30 moderator motor temperature detectors control
1	2	1	5	C	5 moderator pump motor oil level detectors control
1	2	1	5	C	5 moderator pump motor heater detectors control
1	2	1	5	C	5 moderator pump suction pressure detectors control
1	2	2	2	C	2 heat exchanger discharge flow detectors control
1	2	2	2	C	2 heat exchanger discharge pressure detectors control
1	2	3	1	C	1 moderator level wide range detector control
1	2	3	3	C	3 moderator level narrow-range detectors control

c) *Liquid zone equipment - controlling*

div	*Sys*	*eqp*	*com*	*core*	*Definition*
1	3	1	3	C	3 liquid-zone light water pumps control
1	3	2	1	C	liquid zone heat exchanger temp detector control
1	3	3	2	C	2 helium compressors control
1	3	4	1	C	hydrogen and oxygen recombination device control

d) *Reactivity adjuster equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	4	1	1	C	adjuster motor drive control
1	4	2	21	C	21 adjuster position sensors control
1	4	3	1	C	adjuster shaft sealing sensor control

e) *Liquid poison equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	5	1	2	C	2 poison solution pumps control
1	5	2	2	C	2 tank poison quantity sensors control
1	5	3	2	C	2 tank level sensors control
1	5	4	2	C	2 tank poison solutions flow sensors control

f) Reactor shutdown equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	6	1	1	C	high in-core neutron flux tripping detector control
1	6	1	1	C	high ion-chamber neutron flux tripping detector control
1	6	1	1	C	low gross coolant flow tripping detector control
1	6	1	1	C	heat transport pressure tripping detector control
1	6	1	1	C	heattransport outlet temperature tripping detector control

1	6	1	1	C	low boiler level tripping detector control
1	6	1	1	C	boiler feedline low pressure tripping detector control
1	6	2	1	C	shutoff rod dropping device control
1	6	2	1	C	shutoff rod redrawing device control
1	6	2	1	C	shutoff rod promptness sensor control
1	6	2	1	C	shutoff hardware interlocking device control

g) *Moderator purification equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	7	1	1	C	ion exchanger flow control valve control
1	7	2	1	C	ion exchanger bypass control valve control
1	7	3	1	C	purification discharge flow sensor control
1	7	4	1	C	filter differential pressure sensors control
1	7	4	5	C	5 ion exchange columns pressure sensors control
1	7	4	1	C	discharge strainer differential pressure sensor control

h) *Moderator cover gas equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	8	1	2	C	2 moderator cover gas safety valves control
1	8	1	4	C	4 calandria rupture discs control
1	8	1	3	C	3 helium-oxygen pressure reducing valves control
1	8	1	1	C	instrument air safety valve control
1	8	1	1	C	instrument air safety valve control
1	8	2	2	C	2 containment isolation valves control
1	8	4	2	C	2 recombination unit preheaters control
1	8	5	1	C	moderator cover gas flow sensor control
1	8	5	1	C	moderator cover gas temperature sensor control
1	8	5	1	C	moderator cover gas pressure sensor control
1	8	6	1	C	cover gas supply isolation valve control
1	8	7	1	C	cover gas deuterium concentration sensor control

i) *Moderator heavy water sampling equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	9	1	1	C	moderator inlet heavy water sampling sensor control
1	9	1	1	C	purification outlet heavy water sampling sensor control
1	9	1	1	C	liquid poison heavy water sampling sensor control
1	9	1	1	C	heavy water collection discharge sensor control
1	9	1	1	C	heavy water recovery outlet sampling sensor control
1	9	2	1	C	heavy water purification sampling pump control
1	9	3	3	C	3 heavy water sampling isolation valves control

j) *Moderator heavy water collection equipment - controlling*

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	10	1	1	C	heavy water collection pump control
1	10	2	1	C	heavy water collection discharge valve control
1	10	3	1	C	heavy water collection level sensor control

4.3.4-2 *Primary Heat Transport Controlling*

a) Heat transport circulating equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	1	1	16	C	16 main heat transport circulating pumps control
2	1	2	16	C	16 main circulating discharge valves control
2	1	3	24	C	24 steam generator isolation valves control
2	1	4	4	C	4 reactor outlet header circuit valves control

b) Feed and bleed and relief equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	2	1	2	C	2 heat transport feed pumps control
2	2	2	2	C	2 bleed condenser heaters control sensors control
2	2	3	1	C	bleed condenser outlet valve control
2	2	4	1	C	bleed condenser off-gas management valve control
2	2	4	2	C	2 bleed condenser off-gas solenoid valves control
2	2	5	1	C	bleed condenser bypass valve control
2	2	5	1	C	bleed condenser inlet valve control
2	2	6	1	C	reactor outlet header pressure sensor control
2	2	6	2	C	2 reactor outlet header feed valves control
2	2	6	2	C	2 reactor outlet header bleed valves control
2	2	6	4	C	4 reactor outlet header cross connect valves control
2	2	7	1	C	bleed condenser pressure sensor control
2	2	7	1	C	reflux condenser control valve control
2	2	7	1	C	spray cooling control valve control
2	2	8	2	C	2 bleed cooler outlet temperature sensors control
2	2	8	2	C	2 bleed cooler outlet service water valves control
2	2	8	2	C	2 loss-of-coolant-accident solenoid valves control
2	2	9	2	C	2 bleed condenser level sensors control
2	2	9	2	C	2 bleed cooler outlet temperature sensors control
2	2	10	1	C	fuelling machine heavy water pressure sensor control
2	2	10	1	C	fuelling machine pressure control valve control
2	2	11	1	C	heat transport circuit overpressure sensor control
2	2	11	1	C	heat transport relief valves control

c) Heat transport purification equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	3	1	1	C	purification bank inlet pressure sensor control
2	3	1	2	C	2 purification bank inlet isolating valve control
2	3	2	1	C	pressure across purification system sensor control
2	3	2	1	C	purification bypass valve control
2	3	3	1	C	purification flow temperature sensor control
2	3	3	1	C	ion exchange resin temperature sensor control
2	3	4	1	C	purification flow pressure override sensor control
2	3	4	1	C	purification pressure relief valve control
2	3	5	1	C	ion exchange lithium ion sensor control

d) Heat transport gland sealing equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	4	1	1	C	gland supply flow sensors control
2	4	1	16	C	16 gland supply circulating pumps control
2	4	1	4	C	4 gland supply shutdown cooling pumps control
2	4	1	4	C	4 gland supply isolating valves control

2	4	2	1	C	gland return flow sensors control
2	4	2	1	C	gland return circulating pumps control
2	4	3	1	C	gland supply shutdown cooling pump control
2	4	4	1	C	gland recirculation cooler isolating valves control

e) Heat transport hydrogen addition equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	5	1	1	C	hydrogen addition pressure sensors control
2	5	1	1	C	hydrogen addition isolating valves control
2	5	1	1	C	hydrogen addition pressure regulating valves control
2	5	2	1	C	hydrogen addition heavy water flow sensor control
2	5	2	1	C	hydrogen addition heavy water flow valve control
2	5	2	1	C	hydrogen addition heavy water isolating valve control
2	5	3	1	C	gas flow sensor control
2	5	3	1	C	pressure switch control

f) Heat transport heavy water collection equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	6	1	1	C	heavy water collection tank level sensor control
2	6	1	4	C	4 heat transport heavy water collection pumps control
2	6	2	1	C	heavy water collection discharge valve control
2	6	3	1	C	leak-proof collection pumps control

g) Heat transport emergency coolant injection equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	7	1	1	C	high-pressure injection flow sensor control
2	7	1	1	C	emergency coolant high-pressure pumps control
2	7	1	1	C	emergency coolant injection valves control
2	7	1	1	C	emergency coolant injection test valves control
2	7	1	1	C	emergency coolant injection isolating valves control
2	7	1	1	C	emergency coolant tank level sensor control
2	7	1	1	C	emergency coolant injection flow sensor control
2	7	2	1	C	re-injection pumps control
2	7	2	1	C	re-injection recovery sump level sensor control
2	7	2	1	C	re-injection isolating valves control
2	7	3	1	C	recirculation flow sensor control
2	7	3	4	C	4 recirculation control valves control
2	7	3	2	C	2 recirculation isolating valves control
2	7	4	1	C	long-term recovery pumps control
2	7	4	1	C	long-term recovery isolating valves control
2	7	5	1	C	overpressure pressure sensors control
2	7	5	1	C	overpressure relief valves control

h) Heat transport heavy water supply equipment - controlling

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	8	1	2	C	2 heavy water supply pumps control
2	8	2	1	C	leak-proof heavy water pump control
2	8	2	1	C	backup tank level sensor control
2	8	3	1	C	thermal trip pump motor control

4.3.5 Creation of Supervising Data Base

This section presents the creation of the data base for the nuclear systems *supervising* core operations, as shown in Figure 4.11 (for a quick illustration, only the first two divisions are listed with key equipment and the remaining three divisions is only listed with one representative equipment).

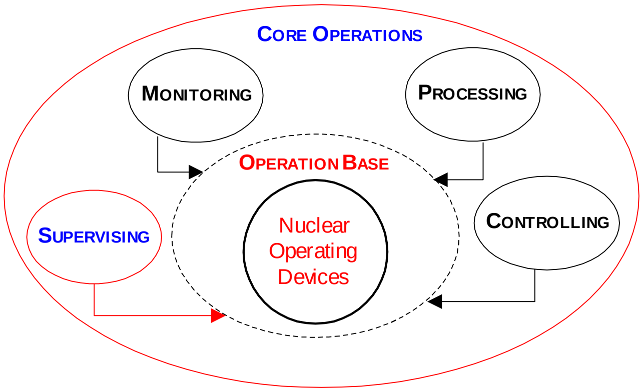


Figure 4.11: Supervising core operations

4.3.5-1 Division-level Supervising

- Reactor-related division – supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	0	0	0	S	calandria & moderator divisional supervising
2	0	0	0	S	primary heat transport & heavy water divisional supervising

- Non-reactor-related division - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
3	0	0	0	S	boiler & steam divisional supervising
4	0	0	0	S	turbine & generator divisional supervising
5	0	0	0	S	condenser & light water divisional supervising

- Multi-division - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1, 2	0	0	0	S	reactor regulating system divisional supervising
3, 4	0	0	0	S	boiler pressure control divisional supervising
1, 3	0	0	0	S	reactor shut down system divisional supervising
1, 5	0	0	0	S	reactor setback system divisional supervising

4.3.5-2 System-level Supervising

- Calandria-moderator divisional systems - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	0	0	S	CANDU reactor flux/power monitoring system supervising
1	2	0	0	S	main moderator control system supervising

1	3	0	0	S	liquid zone control system supervising
1	4	0	0	S	reactivity adjuster control system supervising
1	5	0	0	S	moderator liquid poison control system supervising
1	6	0	0	S	reactor shutdown mechanical control system supervising
1	7	0	0	S	moderator purification control system supervising
1	8	0	0	S	cover gas control system supervising
1	9	0	0	S	moderator heavy water sampling control system supervising
1	10	0	0	S	moderator heavy water collection control system supervising

- Primary heat transport divisional systems - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	1	0	0	S	PHT main control system supervising
2	2	0	0	S	PHT feed bleed relief control system supervising
2	3	0	0	S	PHT purification control system supervising
2	4	0	0	S	PHT gland seal control system supervising
2	5	0	0	S	PHT deuterium addition control system supervising
2	6	0	0	S	PHT heavy-water collection control system supervising
2	7	0	0	S	PHT emergency coolant control system supervising
2	8	0	0	S	PHT heavy water supply control system supervising

- Boiler & steam divisional systems - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
3	1	0	0	S	boiler main steam supply control system supervising
3	2	0	0	S	boiler steam pressure control system supervising
3	3	0	0	S	boiler feedwater control system supervising
3	4	0	0	S	boiler chemical feed control system supervising
3	5	0	0	S	boiler extraction steam control system supervising
3	6	0	0	S	boiler deaerator start-up poison prevent control system supervising
3	7	0	0	S	boiler feedwater heater drains control system supervising
3	8	0	0	S	boiler emergency cooling control system supervising

- Turbine & generator divisional systems - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
4	1	0	0	S	turbine steam control system supervising
4	2	0	0	S	turbine electrohydraulic governor control system supervising
4	3	0	0	S	turbine live steam reheat control system supervising
4	4	0	0	S	turbine gland steam control system supervising
4	5	0	0	S	turbine lp cylinder exhaust cooling control system supervising
4	6	0	0	S	turbine extraction steam drains control system supervising
4	7	0	0	S	turbine generator lubricating control system supervising
4	8	0	0	S	generator hydrogen cooling control system supervising

- Condenser & water divisional systems - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
5	1	0	0	S	condenser main control system supervising
5	2	0	0	S	condenser make up and reject control system supervising
5	3	0	0	S	condenser circulating water filtering control system supervising
5	4	0	0	S	condenser air extraction control system supervising
5	5	0	0	S	service water control system supervising
5	6	0	0	S	service water low pressure control system supervising
5	7	0	0	S	service water high pressure control system supervising
5	8	0	0	S	condenser gland injection control system supervising
5	9	0	0	S	water sampling control system supervising

5	10	0	0	S	emergency water supply control system supervising

4.3.5-3 Calandria-Moderator Equipment Supervising

- *CANDU reactor power control equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	1	1	0	S	ion chamber flux detectors supervising
1	1	2	0	S	in-core flux detectors supervising
1	1	3	0	S	reactor thermal power detectors supervising
1	1	4	0	S	in-core reactor power post-processor supervising
1	1	5	0	S	reactor startup instrumentation supervising

- *Main moderator equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	2	1	0	S	moderator pumps and motors supervising
1	2	2	0	S	moderator heat exchangers supervising
1	2	2	0	S	moderator level detectors supervising

- *Liquid zone equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	3	1	0	S	liquid zone light water pumps supervising
1	3	2	0	S	liquid zone heat exchangers supervising
1	3	3	0	S	helium compressors supervising
1	3	4	0	S	recombination devices supervising

- *Reactivity adjuster equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	4	1	0	S	adjuster motor drives supervising
1	4	2	0	S	adjuster position sensors supervising
1	4	3	0	S	adjuster shaft sealing sensors supervising
1	4	4	0	S	adjuster heavy water cooling sensors supervising

- *Liquid poison equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	5	1	0	S	poison solution pumps supervising
1	5	2	0	S	poison quantity sensors supervising
1	5	3	0	S	tanks level sensors supervising
1	5	4	0	S	poison solution flow sensors supervising

- *Reactor shutdown* equipment - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	6	1	0	S	reactor shutdown tripping detectors supervising
1	6	2	0	S	shutoff rod dropping device supervising
1	6	3	0	S	shutoff rod redrawing device supervising
1	6	4	0	S	shutoff rod promptness sensor supervising
1	6	5	0	S	shutoff hardware interlocking device supervising

- *Moderator purification equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	7	1	0	S	ion exchanger flow control valve supervising
1	7	2	0	S	ion exchanger bypass control valve supervising
1	7	3	0	S	discharge flow sensors supervising
1	7	4	0	S	purification differential pressure sensors supervising

- *Moderator cover gas* equipment - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	8	1	0	S	cover gas overpressure control valves supervising
1	8	2	0	S	containment isolation valves supervising
1	8	3	0	S	helium circulation compressors supervising
1	8	4	0	S	recombination unit preheaters supervising
1	8	5	0	S	cover gas flow, temperature, and pressure sensors supervising
1	8	6	0	S	cover gas supply isolation valves supervising
1	8	7	0	S	deuterium concentration sensor supervising

- *Heavy water sampling equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	9	1	0	S	*heavy water sampling device* supervising
1	9	2	0	S	*heavy water sampling pump* supervising
1	9	3	0	S	*heavy water isolation valves* supervising

- *Heavy water collection equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
1	10	1	0	S	*heavy water collection pump* supervising
1	10	2	0	S	*heavy water collection discharge valve* supervising
1	10	3	0	S	*heavy water level sensor* supervising

4.3.5-4 Primary Heat Transport Equipment Supervising

- *PHT main control equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	1	1	0	S	*heat transport main circulating pumps* supervising
2	1	2	0	S	*main circulating pump discharge valves* supervising
2	1	3	0	S	*steam generator isolation valves* supervising
2	1	4	0	S	*reactor outlet header circuit valves* supervising

- *PHT feed bleed relief equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	2	1	0	S	*heat transport feed pumps* supervising
2	2	2	0	S	*bleed condenser heaters* supervising
2	2	3	0	S	*bleed condenser outlet valve* supervising
2	2	4	0	S	*bleed condenser off-gas management valves* supervising
2	2	5	0	S	*bleed condenser bypass & inlet valves* supervising
2	2	6	0	S	*heat transport reactor outlet feed & bleed valves* supervising
2	2	7	0	S	*reflux condenser & spray cooling valves* supervising
2	2	8	0	S	*bleed cooler outlet temperature control valves* supervising
2	2	9	0	S	*bleed condenser level sensors* supervising
2	2	10	0	S	*fuelling machine heavy water pressure control valve* supervising
2	2	11	0	S	*heat transport main circuit relief valves* supervising

- *PHT purification equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	3	1	0	S	*purification inlet pressure sensor & isolating valves* supervising
2	3	2	0	S	*purification pressure sensors & bypass valve* supervising
2	3	3	0	S	*purification flow temperature sensors* supervising
2	3	4	0	S	*purification flow pressure override sensor* supervising
2	3	5	0	S	*ion exchange lithium ion sensor* supervising

- *PHT gland sealing equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	4	1	0	S	*gland supply flow sensor, pumps and isolating valves* supervising
2	4	2	0	S	*gland return flow sensors and pumps* supervising
2	4	3	0	S	*glands supply shutdown cooling pumps* supervising
2	4	4	0	S	*gland recirculation cooler isolating valves* supervising

- *PHT deuterium control equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	5	1	0	S	*hydrogen addition isolating & regulating valves* supervising
2	5	2	0	S	*heavy water flow sensor & valve* supervising
2	5	3	0	S	*gas flow sensor & pressure switch* supervising

- *PHT heavy-water collection equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	6	1	0	S	*heavy water collection pumps* supervising
2	6	2	0	S	*heavy water collection discharge valve* supervising
2	6	3	0	S	*heavy water collection leak-proof pump* supervising

- *PHT emergency coolant control equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	7	1	0	S	*high-pressure injection sensors, pumps and valves* supervising
2	7	2	0	S	*re-injection sensors, pumps and valves* supervising
2	7	3	0	S	*high-pressure recirculation pumps* supervising
2	7	4	0	S	*long term low pressure recovery pumps* supervising
2	7	5	0	S	*overpressure sensor and relief valves* supervising

- *Heavy water supply equipment* - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
2	8	1	0	S	*heavy water supply pumps* supervising
2	8	2	0	S	*leak-proof heavy water pumps* supervising
2	8	3	0	S	*thermal trip pumps* supervising

4.3.5-5 Boiler & Steam Equipment - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
					Boiler main steam supply key equipment
3	1	1	0	S	steam reject valves control process supervising
					Boiler Steam Pressure Control key Equipment
3	2	1	0	S	boiler steam pressure control process supervising
					Boiler Feedwater key Equipment
3	3	1	0	S	boiler feed pump control process supervising
					Boiler Chemical Feed key Equipment
3	4	1	0	S	hydrazine pump control process supervising
					Boiler Extraction Steam key Equipment
3	5	1	0	S	hp extraction steam dump control process supervising
					Deaerator Start-up & Poison Prevent key Equipment
3	6	1	0	S	deaerator pressure control process supervising
					Boiler Feedwater Heater Drains key Equipment
3	7	1	0	S	feedwater heater drains pumps control process supervising
					Boiler Emergency Cooling Control key Equipment
3	8	1	0	S	boiler feedwater control process supervising

4.3.5-6 Turbine-Generator Equipment - supervising

div	*sys*	*eqp*	*com*	*core*	*Definition*
					Turbine Steam Control key Equipment
4	1	1	0	S	motorized isolating valves control process supervising
					Turbine Electrohydraulic Governor Key Equipment
4	2	1	0	S	shaft acceleration detecting process supervising
					Turbine Live Steam Reheat key Equipment
4	3	1	0	S	reheater drain pump control process supervising
					Turbine Gland Steam key Equipment
4	4	1	0	S	gland steam isolating valve control process supervising
					Turbine LP Cylinder Exhaust Cooling key Equipment
4	5	1	0	S	cooling steam control process supervising
					Turbine Extraction Steam Drains key Equipment
4	6	1	0	S	motorized drain valves control process supervising
					Turbine Generator Lubricating key Equipment
4	7	1	0	S	main lubricating oil pump control process supervising
					Generator Hydrogen Cooling Control key Equipment
4	8	1	0	S	generator hydrogen cooling process supervising

4.3.5-7 Condenser-Light Water Equipment - supervising

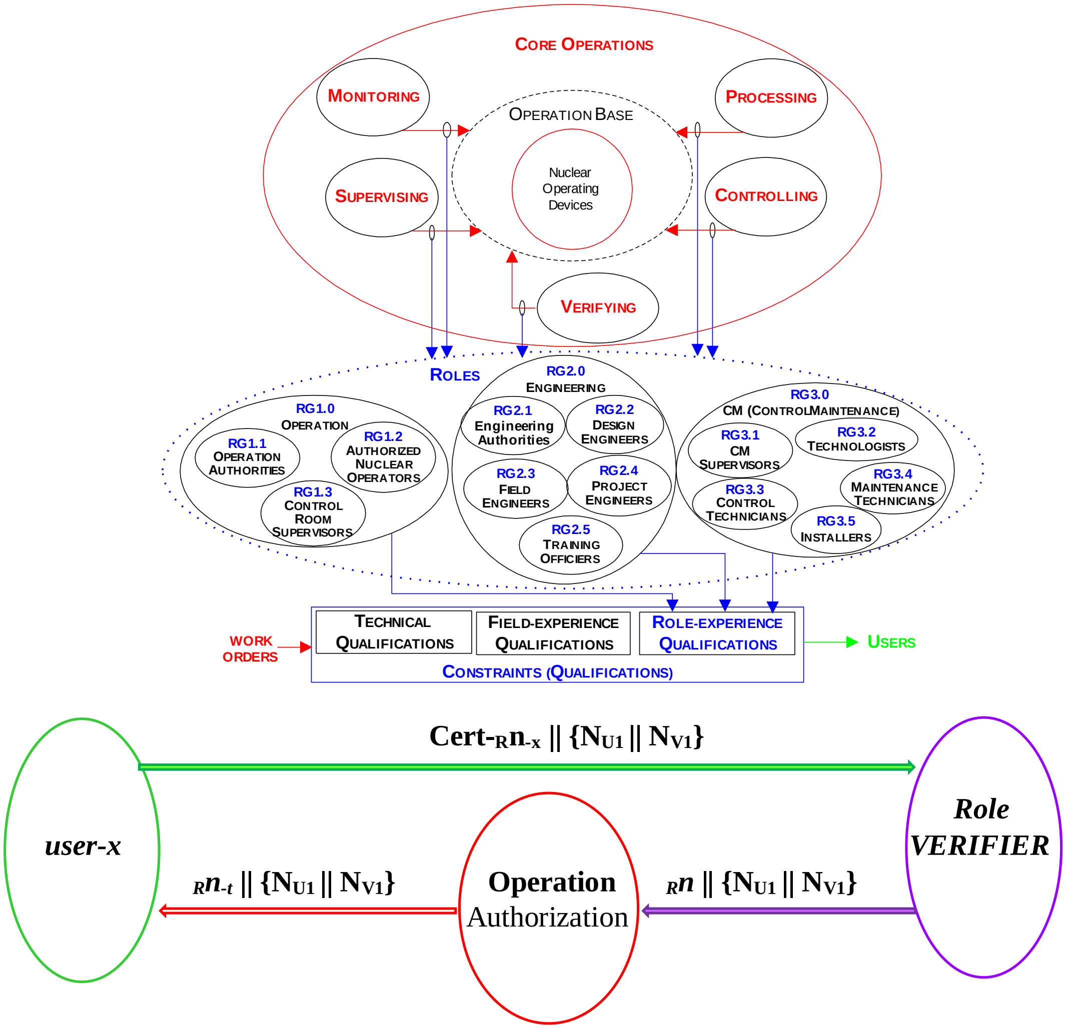
div	*sys*	*eqp*	*com*	*core*	*Definition*
					Condenser Main Control key Equipment
5	1	1	0	S	main condensate extraction pumps control process supervising
					Condenser Make Up and Reject key Equipment
5	2	1	0	S	condensate makeup control process supervising
					Condenser Circulating Water Filtering key Equipment
5	3	1	0	S	condenser debris filtering process supervising
					Condenser Air Extraction key Equipment
5	4	1	0	S	vacuum pumps control process supervising
					Service Water Supply key Equipment
5	5	1	0	S	service water pumps control process supervising
					Service Water Low Pressure key Equipment
5	6	1	0	S	low pressure pumps control process supervising
					Service Water High Pressure key Equipment
5	7	1	0	S	high pressure pumps control process supervising
					Condenser Gland Injection key Equipment
5	8	1	0	S	gland seal pumps control process supervising
					Water Sampling Analysis key Equipment
5	9	1	0	S	central sample collection process supervising
					Emergency Water Supply key Equipment
5	10	1	0	S	EWS pump station process supervising

4.4 SNP Access Qualifications Base

This section presents the certificates base for role, field, and technical qualifications.

4.4.1 Creation of Role Qualification Certificates Base

The following presents the certificates base for the role qualifications, as shown in Figure 4.12.



Core Operations
Monitoring
Processing
Operation Base
Nuclear Operating Devices
Supervising
Controlling
Verifying
Roles
RG2.0 Engineering
RG2.1 Engineering Authorities
RG2.2 Design Engineers
RG2.3 Field Engineers
RG2.4 Project Engineers
RG2.5 Training Officiers
RG1.0 Operation
RG1.1 Operation Authorities
RG1.2 Authorized Nuclear Operators
RG1.3 Control Room Supervisors
RG3.0 CM (ControlMaintenance)
RG3.1 CM Supervisors
RG3.2 Technologists
RG3.3 Control Technicians
RG3.4 Maintenance Technicians
RG3.5 Installers
Work Orders
Technical Qualifications
Field-Experience Qualifications
Role-Experience Qualifications
Constraints (Qualifications)
Users
Cert-$_{R}$n$_{-x}$ || {N$_{U1}$ || N$_{V1}$}
user-x
Role VERIFIER
$_{R}$n$_{-t}$ || {N$_{U1}$ || N$_{V1}$}
Operation Authorization
$_{R}$n || {N$_{U1}$ || N$_{V1}$}

Figure 4.12: Role qualification certificates

*4.4.1-1 **RG1**: Operation Roles*

RG1.1 – Operation authorities

***Cert-**$_{R1.1.1-x}$*	directors of operation
***Cert-**$_{R1.1.2-x}$*	operation department managers
***Cert-**$_{R1.1.3-x}$*	senior operation administrators

RG1.2 – Control room supervising operators

Cert-$_{R1.2.1\text{-}x}$	control-room duty managers
Cert-$_{R1.2.2\text{-}x}$	control-room shift managers
Cert-$_{R1.2.3\text{-}x}$	control-room supervising operators
Cert-$_{R1.2.4\text{-}x}$	control-room operators

RG1.3 – Authorized nuclear operators

Cert-$_{R1.3.1\text{-}x}$	senior authorized nuclear operators
Cert-$_{R1.3.2\text{-}x}$	authorized nuclear operators
Cert-$_{R1.3.3\text{-}x}$	nuclear operators

4.4.1-2 ***RG2****: Engineering Roles*

RG2.1 – Engineering authorities

Cert-$_{R2.1.1\text{-}x}$	director of engineering
Cert-$_{R2.1.2\text{-}x}$	department managers
Cert-$_{R2.1.3\text{-}x}$	section managers

RG2.2 – Design engineers

Cert-$_{R2.2.1\text{-}x}$	design authority
Cert-$_{R2.2.2\text{-}x}$	design managers
Cert-$_{R2.2.3\text{-}x}$	design team leads
Cert-$_{R2.2.4\text{-}x}$	design verifiers
Cert-$_{R2.2.5\text{-}x}$	senior design engineers
Cert-$_{R2.2.6\text{-}x}$	design engineers
Cert-$_{R2.2.7\text{-}x}$	design analysts

RG2.3 – Field engineers

Cert-$_{R2.3.1\text{-}x}$	system responsible engineers
Cert-$_{R2.3.2\text{-}x}$	senior station engineers
Cert-$_{R2.3.3\text{-}x}$	reactor room engineers
Cert-$_{R2.3.4\text{-}x}$	station engineers
Cert-$_{R2.3.5\text{-}x}$	equipment room engineers
Cert-$_{R2.3.6\text{-}x}$	turbine floor engineers
Cert-$_{R2.3.7\text{-}x}$	boiler room engineers

RG2.4 – Project engineers

Cert-$_{R2.4.1\text{-}x}$	project engineering managers
Cert-$_{R2.4.2\text{-}x}$	senior project engineers
Cert-$_{R2.4.3\text{-}x}$	project engineers

RG2.5 – Training Officers

Cert-$_{R2.5.1\text{-}x}$	senior training officers
Cert-$_{R2.5.2\text{-}x}$	training officers

4.4.1-3 ***RG3****: CM (Control Maintenance) Roles*

RG3.1 – CM supervisors

Cert-$_{R3.1.1\text{-}x}$	first line managers
Cert-$_{R3.1.2\text{-}x}$	CM supervisors

RG3.2 – Technologists

Cert-$_{R3.2.1\text{-}x}$	senior technologists
Cert-$_{R3.2.2\text{-}x}$	control technologists
Cert-$_{R3.2.3\text{-}x}$	commissioning technologists
Cert-$_{R3.2.4\text{-}x}$	maintenance technologists

RG3.3 – Control technicians

Cert-$_{R3.3.1\text{-}x}$	senior control technicians
Cert-$_{R3.3.2\text{-}x}$	control technicians

RG3.4 – Maintenance technicians

Cert-$_{R3.4.1\text{-}x}$	senior maintenance technicians
Cert-$_{R3.4.2\text{-}x}$	maintenance technicians

RG3.5 – Installation technicians

Cert-$_{R3.5.1\text{-}x}$	senior station installation technicians
Cert-$_{R3.5.2\text{-}x}$	station installation technicians
Cert-$_{R3.5.3\text{-}x}$	contractor supervising installers
Cert-$_{R3.5.4\text{-}x}$	contractor installers

4.4.2 Creation of Field Qualification Certificates Base

The following presents the certificates base for the field qualifications, as shown in Figure 4.13.

*4.4.2-1 **FG1**: On-Line Division-Level Operations*

Cert-$_{F1.1\text{-}x}$	on-line reactor regulating operations
Cert-$_{F1.2\text{-}x}$	on-line reactor shutdown operations
Cert-$_{F1.3\text{-}x}$	on-line moderator regulating operations
Cert-$_{F1.4\text{-}x}$	on-line unit power regulating operations
Cert-$_{F1.5\text{-}x}$	on-line boiler pressure regulating operations
Cert-$_{F1.6\text{-}x}$	on-line electrohydraulic turbine governing operations
Cert-$_{F1.7\text{-}x}$	on-line generator exciter/voltage regulating operations

*4.4.2-2 **FG2**: On-Line System-Level Operations*

FG2.1 – Operations on CANDU calandria & moderator systems

Cert-$_{F2.1\text{-}1\text{-}x}$	on-line CANDU reactor flux/power operations
Cert-$_{F2.1\text{-}2\text{-}x}$	on-line main moderator operations
Cert-$_{F2.1\text{-}3\text{-}x}$	on-line liquid zone operations
Cert-$_{F2.1\text{-}4\text{-}x}$	on-line reactivity adjuster operations
Cert-$_{F2.1\text{-}5\text{-}x}$	on-line moderator liquid poison operations
Cert-$_{F2.1\text{-}6\text{-}x}$	on-line moderator purification operations
Cert-$_{F2.1\text{-}7\text{-}x}$	on-line cover gas operations

Cert-$_{F2.1\text{-}8\text{-}x}$	on-line moderator heavy water sampling operations
Cert-$_{F2.1\text{-}9\text{-}x}$	on-line moderator heavy water collection operations

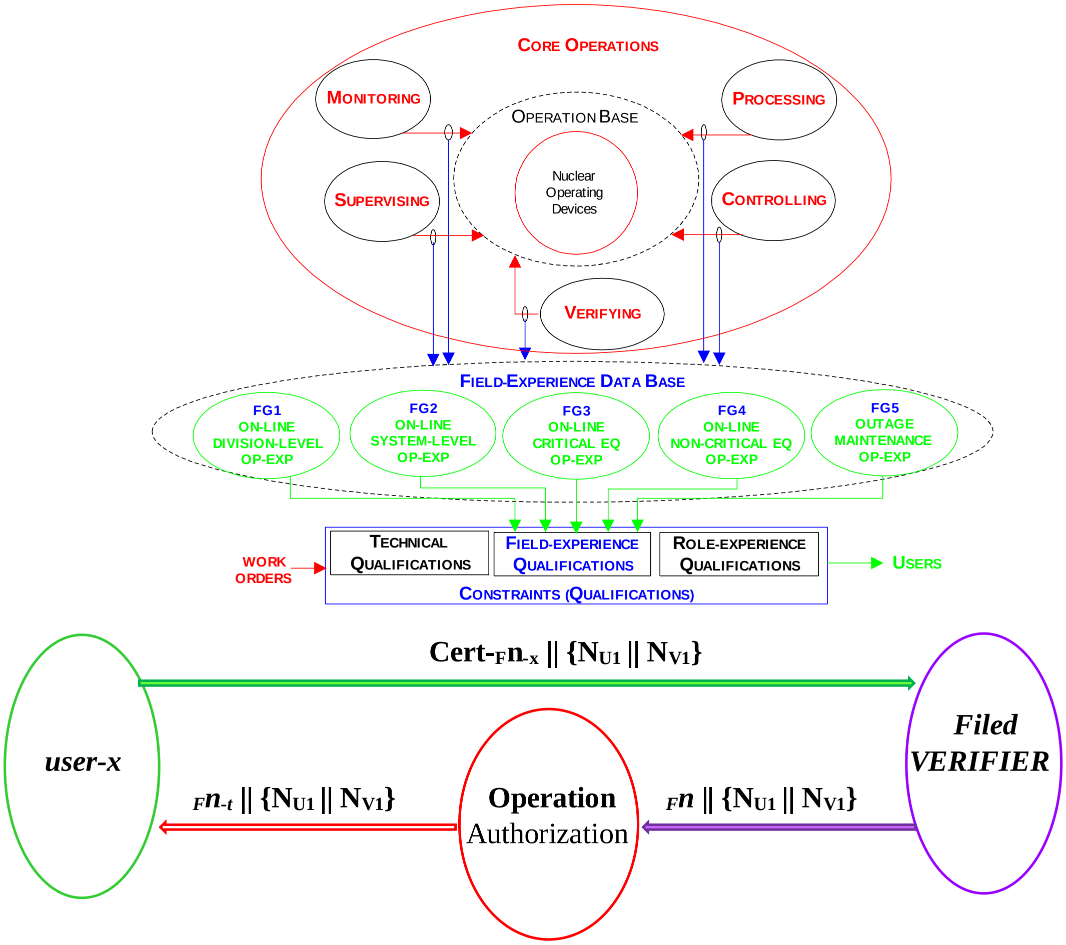

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
FIELD-EXPERIENCE DATA BASE
FG1 ON-LINE DIVISION-LEVEL OP-EXP
FG2 ON-LINE SYSTEM-LEVEL OP-EXP
FG3 ON-LINE CRITICAL EQ OP-EXP
FG4 ON-LINE NON-CRITICAL EQ OP-EXP
FG5 OUTAGE MAINTENANCE OP-EXP
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
USERS
CONSTRAINTS (QUALIFICATIONS)
Cert-$_{F}$n$_{-x}$ || {N$_{U1}$ || N$_{V1}$}
user-x
Filed VERIFIER
$_{F}$n$_{-t}$ || {N$_{U1}$ || N$_{V1}$}
Operation Authorization
$_{F}$n || {N$_{U1}$ || N$_{V1}$}

Figure 4.13: Field qualification certificates

FG2.2 – Operations on primary heat transport & heavy water systems

Cert-$_{F2.2\text{-}1\text{-}x}$	on-line heat transport main control operations
Cert-$_{F2.2\text{-}2\text{-}x}$	on-line heat transport feed bleed relief operations
Cert-$_{F2.2\text{-}3\text{-}x}$	on-line heat transport purification operations
Cert-$_{F2.2\text{-}4\text{-}x}$	on-line heat transport gland seal operations
Cert-$_{F2.2\text{-}5\text{-}x}$	on-line heat transport deuterium addition operations
Cert-$_{F2.2\text{-}6\text{-}x}$	on-line heat transport heavy-water collection operations
Cert-$_{F2.2\text{-}7\text{-}x}$	on-line heat transport emergency coolant operations
Cert-$_{F2.2\text{-}8\text{-}x}$	on-line heavy water supply operations

FG2.3 – Operations on boiler & steam systems

Cert-$_{F2.3\text{-}1\text{-}x}$	on-line boiler main steam supply operations
Cert-$_{F2.3\text{-}2\text{-}x}$	on-line boiler steam pressure operations
Cert-$_{F2.3\text{-}3\text{-}x}$	on-line boiler feedwater operations
Cert-$_{F2.3\text{-}4\text{-}x}$	on-line boiler chemical feed operations
Cert-$_{F2.3\text{-}5\text{-}x}$	on-line boiler extraction steam operations

Cert-F2.3-6-x	on-line boiler deaerator start-up & poison prevent operations
Cert-F2.3-7-x	on-line boiler feedwater heater drains operations
Cert-F2.3-8-x	on-line boiler emergency cooling operations

FG2.4 – Operations on turbine & generator systems

Cert-F2.4-1-x	on-line turbine steam operations
Cert-F2.4-2-x	on-line turbine electrohydraulic governor operations
Cert-F2.4-3-x	on-line turbine live steam reheat operations
Cert-F2.4-4-x	on-line turbine gland steam operations
Cert-F2.4-5-x	on-line turbine low pressure cylinder exhaust cooling operations
Cert-F2.4-6-x	on-line turbine extraction steam drains operations
Cert-F2.4-7-x	on-line turbine generator lubricating operations
Cert-F2.4-8-x	on-line generator hydrogen cooling operations

FG2.5 – Operations on condenser & light water systems

Cert-F2.5-1-x	on-line condenser main control operations
Cert-F2.5-2-x	on-line condenser make up and reject operations
Cert-F2.5-3-x	on-line condenser circulating water debris operations
Cert-F2.5-4-x	on-line condenser air extraction control operations
Cert-F2.5-5-x	on-line service water operations
Cert-F2.5-6-x	on-line service water low pressure operations
Cert-F2.5-7-x	on-line service water high pressure operations
Cert-F2.5-8-x	on-line condenser gland injection operations
Cert-F2.5-9-x	on-line water sampling operations
Cert-F2.5-10-x	on-line emergency water supply operations

4.4.2-3 **FG3**: *On-line Critical Equipment Operations*

Cert-F3.1-x	on-line critical equipment testing
Cert-F3.2-x	on-line critical equipment calibration or adjustment
Cert-F3.3-x	on-line critical equipment commissioning
Cert-F3.4-x	on-line critical equipment monitoring

4.4.2-4 **FG4**: *On-line non-Critical Equipment Operations*

Cert-F4.1-x	on-line non-critical equipment testing
Cert-F4.2-x	on-line non-critical equipment calibration or adjustment
Cert-F4.3-x	on-line non-critical equipment commissioning
Cert-F4.4-x	on-line non-critical equipment monitoring

4.4.2-5 **FG5**: *Outage Equipment Operations*

Cert-F5.1-x	outage critical system testing
Cert-F5.2-x	outage critical equipment testing
Cert-F5.3-x	outage critical equipment commissioning
Cert-F5.4-x	outage equipment testing
Cert-F5.5-x	outage equipment commissioning
Cert-F5.6-x	outage equipment installation
Cert-F5.7-x	outage general maintenance

4.4.3 Creation of Technical Qualification Certificates Base

The following presents the certificates base for the technical qualifications, as shown in Figure 4.14.

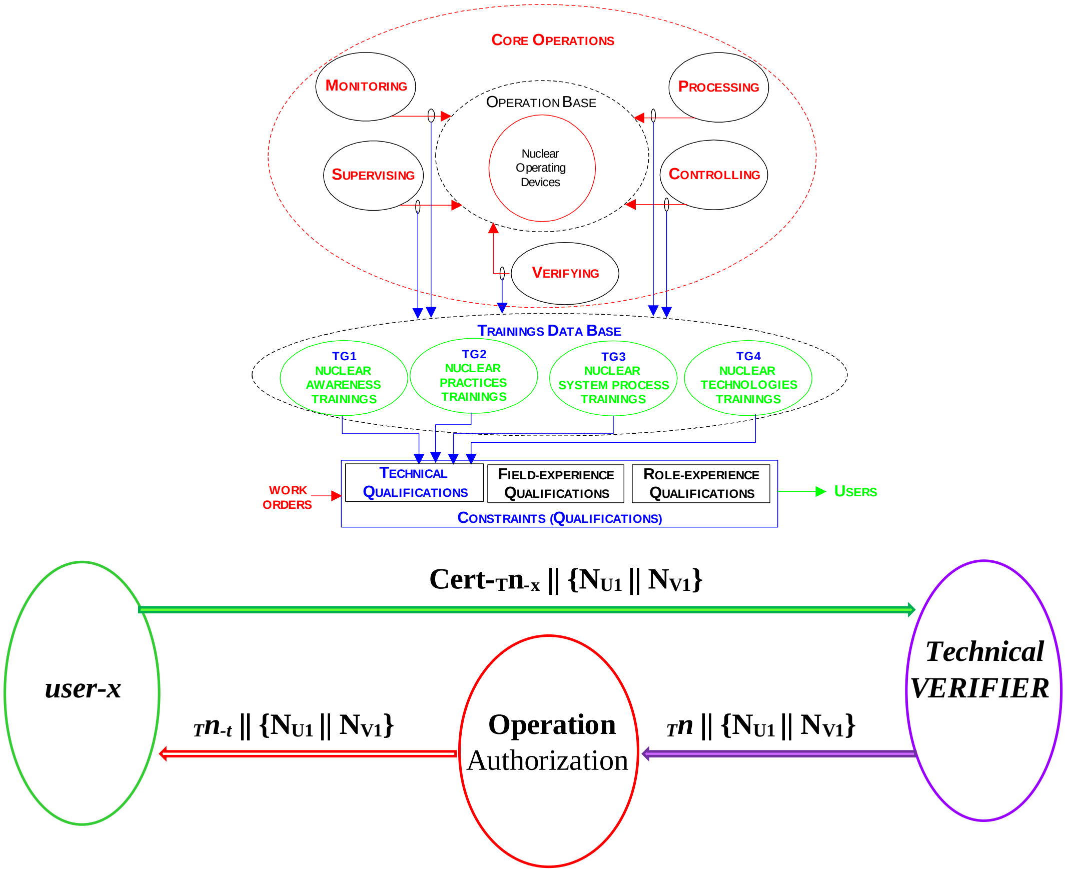

CORE OPERATIONS
MONITORING
PROCESSING
OPERATION BASE
Nuclear Operating Devices
SUPERVISING
CONTROLLING
VERIFYING
TRAININGS DATA BASE
TG1 NUCLEAR AWARENESS TRAININGS
TG2 NUCLEAR PRACTICES TRAININGS
TG3 NUCLEAR SYSTEM PROCESS TRAININGS
TG4 NUCLEAR TECHNOLOGIES TRAININGS
WORK ORDERS
TECHNICAL QUALIFICATIONS
FIELD-EXPERIENCE QUALIFICATIONS
ROLE-EXPERIENCE QUALIFICATIONS
CONSTRAINTS (QUALIFICATIONS)
USERS
Cert-$_T$n$_{-x}$ || {N$_{U1}$ || N$_{V1}$}
user-x
Technical VERIFIER
$_T$n$_{-t}$ || {N$_{U1}$ || N$_{V1}$}
Operation Authorization
$_T$n || {N$_{U1}$ || N$_{V1}$}

Figure 4.14: Technical qualification certificates

*4.4.3-1 **TG1**: Nuclear Awareness Trainings*

TG1.1 – Nuclear worker general awareness trainings

Cert-$_{T1.1.1-x}$	basic nuclear safety awareness certificate
Cert-$_{T1.1.2-x}$	basic nuclear emergency response awareness certificate
Cert-$_{T1.1.3-x}$	basic nuclear work protection awareness certificate
Cert-$_{T1.1.4-x}$	basic nuclear physical security awareness certificate
Cert-$_{T1.1.5-x}$	basic nuclear environment awareness certificate
Cert-$_{T1.1.6-x}$	WHMIS awareness certificate
Cert-$_{T1.1.7-x}$	nuclear code of conduct awareness certificate
Cert-$_{T1.1.8-x}$	nuclear corporate safety rules awareness certificate
Cert-$_{T1.1.9-x}$	nuclear quality program awareness certificate
Cert-$_{T1.1.10-x}$	fire protection awareness certificate

TG1.2 – Nuclear safety awareness trainings

Cert-$_{T1.2.1-x}$	radiological risk identification certificate
Cert-$_{T1.2.2-x}$	nuclear orange 1 badge certificate
Cert-$_{T1.2.3-x}$	nuclear orange 2 badge certificate

Cert-$_{T1.2.4\text{-}x}$	nuclear orange 3 badge certificate
Cert-$_{T1.2.5\text{-}x}$	radiation protection compressed gases awareness certificate
Cert-$_{T1.2.6\text{-}x}$	falling object prevention awareness certificate
Cert-$_{T1.2.7\text{-}x}$	lift truck operator certificate
Cert-$_{T1.2.8\text{-}x}$	confined space work safety certificate
Cert-$_{T1.2.9\text{-}x}$	respiratory protection certificate
Cert-$_{T1.2.10\text{-}x}$	asbestos awareness certificate

TG1.3 – Nuclear information, cyber security, OPEX awareness trainings

Cert-$_{T1.3.1\text{-}x}$	nuclear cyber security awareness certificate
Cert-$_{T1.3.2\text{-}x}$	nuclear information management awareness certificate
Cert-$_{T1.3.3\text{-}x}$	nuclear document management and corporate filing certificate
Cert-$_{T1.3.4\text{-}x}$	nuclear record management awareness certificate
Cert-$_{T1.3.5\text{-}x}$	nuclear record retention and disposition awareness certificate
Cert-$_{T1.3.6\text{-}x}$	nuclear station condition records trending analysis certificate
Cert-$_{T1.3.7\text{-}x}$	nuclear emergency response manager OPEX updates awareness certificate
Cert-$_{T1.3.8\text{-}x}$	nuclear operations support manager OPEX updates awareness certificate
Cert-$_{T1.3.9\text{-}x}$	nuclear health physics manager OPEX updates awareness certificate
Cert-$_{T1.3.10\text{-}x}$	nuclear technical support manager OPEX updates awareness certificate
Cert-$_{T1.3.11\text{-}x}$	nuclear safety manager OPEX updates awareness certificate
Cert-$_{T1.3.12\text{-}x}$	nuclear resource deployment manager OPEXupdates awareness certificate
Cert-$_{T1.3.13\text{-}x}$	nuclear security advisor OPEX updates awareness certificate
Cert-$_{T1.3.14\text{-}x}$	nuclear emergency recovery director OPEX updates awareness certificate
Cert-$_{T1.3.15\text{-}x}$	nuclear emergency operations coordinator OPEX awareness certificate

*4.4.3-2 **TG2:** Nuclear Practices Trainings*

TG2.1 – Nuclear work protection certificates

Cert-$_{T2.1.1\text{-}x}$	CANDU nuclear processing certificate
Cert-$_{T2.1.2\text{-}x}$	basic nuclear theory certificate
Cert-$_{T2.1.3\text{-}x}$	nuclear process instrumentation & control certificate
Cert-$_{T2.1.4\text{-}x}$	level 1 or level 2 work protection certificates
Cert-$_{T2.1.5\text{-}x}$	level 3 or level 4 work protection certificates
Cert-$_{T2.1.6\text{-}x}$	level 5 or level 6 work protection certificates
Cert-$_{T2.1.7\text{-}x}$	level 7 or level 8 work protection certificates
Cert-$_{T2.1.8\text{-}x}$	level 9 work protection certificate
Cert-$_{T2.1.9\text{-}x}$	nuclear station condition records awareness certificate
Cert-$_{T2.1.10\text{-}x}$	confined space work protection control-maintenance authority certificate
Cert-$_{T2.1.11\text{-}x}$	nuclear work control awareness certificate

TG2.2 – Nuclear environmental management certificates

Cert-$_{T2.2.1\text{-}x}$	environment qualification engineering introductory certificate
Cert-$_{T2.2.2\text{-}x}$	material management environment qualification certificate
Cert-$_{T2.2.3\text{-}x}$	nuclear operators and maintainers environment qualification certificate
Cert-$_{T2.2.4\text{-}x}$	nuclear waste management introductory level certificate
Cert-$_{T2.2.5\text{-}x}$	nuclear waste management intermediate level certificate
Cert-$_{T2.2.6\text{-}x}$	nuclear waste incineration certificate
Cert-$_{T2.2.7\text{-}x}$	radioactive material transportation awareness certificate
Cert-$_{T2.2.8\text{-}x}$	used nuclear fuel management awareness certificate

TG2.3 – Nuclear proof of practices certificates

Cert-$_{T2.3.1-x}$	nuclear maintenance authority proof of practice certificate
Cert-$_{T2.3.2-x}$	respirator medical assessment proof of practice certificate
Cert-$_{T2.3.3-x}$	nuclear green/yellow badge proof of practice certificate
Cert-$_{T2.3.4-x}$	nuclear holder of record proof of practice certificate
Cert-$_{T2.3.5-x}$	class I, II or III industrial lift truck proof of practice certificate
Cert-$_{T2.3.6-x}$	class IV, V or VII industrial lift truck proof of practice certificate
Cert-$_{T2.3.7-x}$	gas tungsten or shield metal arc welding proof of practice certificate
Cert-$_{T2.3.8-x}$	flux core or gas metal arc welding proof of practice certificate
Cert-$_{T2.3.9-x}$	instrument tube or stud welding proof of practice certificate
Cert-$_{T2.3.10-x}$	capacitor discharge proof of practice certificate

4.4.3-3 ***TG3****: Nuclear Process Basics Trainings*

TG3.1 – Nuclear engineering fundament certificates

Cert-$_{T3.1.1-x}$	basic nuclear fluid mechanics certificate
Cert-$_{T3.1.2-x}$	basic nuclear thermodynamics certificate
Cert-$_{T3.1.3-x}$	intermediate nuclear thermodynamics certificate
Cert-$_{T3.1.4-x}$	advanced nuclear thermodynamics certificate
Cert-$_{T3.1.5-x}$	basic nuclear mechanics certificate
Cert-$_{T3.1.6-x}$	nuclear pump mechanics certificate
Cert-$_{T3.1.7-x}$	basic nuclear electric awareness certificate
Cert-$_{T3.1.8-x}$	radiation detection certificate
Cert-$_{T3.1.9-x}$	nuclear pH monitoring certificate
Cert-$_{T3.1.10-x}$	nuclear conductivity metering certificate
Cert-$_{T3.1.11-x}$	nuclear ion chromatography awareness certificate
Cert-$_{T3.1.12-x}$	nuclear materials awareness certificate

TG3.2 – Nuclear process maintenance certificates

Cert-$_{T3.2.1-x}$	foreign material exclusion awareness certificate
Cert-$_{T3.2.2-x}$	nuclear maintenance first line management certificate
Cert-$_{T3.2.3-x}$	nuclear pressure boundary materials awareness certificate
Cert-$_{T3.2.4-x}$	nuclear reactor regulating system introductory level certificate
Cert-$_{T3.2.5-x}$	nuclear emergency coolant injection system introductory level certificate
Cert-$_{T3.2.6-x}$	nuclear reactor shutdown systems introductory level certificate
Cert-$_{T3.2.7-x}$	nuclear negative pressure control system introductory level certificate
Cert-$_{T3.2.8-x}$	nuclear control room upgrade awareness certificate
Cert-$_{T3.2.9-x}$	nuclear control room troubleshooting procedure certificate
Cert-$_{T3.2.10-x}$	nuclear process correct component verification certificate
Cert-$_{T3.2.11-x}$	nuclear equipment/tooling tracking awareness certificate
Cert-$_{T3.2.12-x}$	nuclear maintenance risk management certificate
Cert-$_{T3.2.13-x}$	nuclear maintenance authority certificate

4.4.3-4 ***TG4****: Nuclear Technologies Trainings*

TG4.1 – Nuclear process exclusive technology certificates

Cert-$_{T4.1.1-x}$	operating policies and principles exclusive certificate
Cert-$_{T4.1.2-x}$	CANDU reactor modulator process exclusive certificate
Cert-$_{T4.1.3-x}$	primary heat transport process exclusive certificate
Cert-$_{T4.1.4-x}$	boiler steam generation process exclusive certificate
Cert-$_{T4.1.5-x}$	turbine-generator process exclusive certificate
Cert-$_{T4.1.6-x}$	condenser and water process exclusive certificate

TG4.2 – Nuclear composite systems technology certificates

Cert-$_{T4.2.1\text{-}x}$	automatic generator voltage regulating system technical certificate
Cert-$_{T4.2.2\text{-}x}$	digital electrohydraulic turbine governing system technical certificate
Cert-$_{T4.2.3\text{-}x}$	smart valve positioning system process access

TG4.3 – Nuclear discrete process control technology certificates

Cert-$_{T4.3.1\text{-}x}$	smart control valves technical certificate
Cert-$_{T4.3.2\text{-}x}$	smart valve positioners technical certificate
Cert-$_{T4.3.3\text{-}x}$	smart control relays technical certificate
Cert-$_{T4.3.4\text{-}x}$	smart protective relays technical certificate
Cert-$_{T4.3.5\text{-}x}$	smart pump drives technical certificate
Cert-$_{T4.3.6\text{-}x}$	smart flow regulators technical certificate
Cert-$_{T4.3.7\text{-}x}$	smart temperature regulators process access
Cert-$_{T4.3.8\text{-}x}$	smart motor drives process access
Cert-$_{T4.3.9\text{-}x}$	smart uninterruptable power supplies technical certificate
Cert-$_{T4.3.10\text{-}x}$	smart motor control centers technical certificate

TG4.4 – Nuclear discrete monitoring technology certificates

Cert-$_{T4.4.1\text{-}x}$	smart monitoring devices technical certificate
Cert-$_{T4.4.2\text{-}x}$	smart radiation monitoring devices technical certificate
Cert-$_{T4.4.3\text{-}x}$	smart metering devices technical certificate
Cert-$_{T4.4.4\text{-}x}$	ion-chamber reactor flux detection technical certificate
Cert-$_{T4.4.5\text{-}x}$	in-core reactor flux detection technical certificate
Cert-$_{T4.4.6\text{-}x}$	reactor thermal power detection technical certificate
Cert-$_{T4.4.7\text{-}x}$	flow transmitters technical certificate
Cert-$_{T4.4.8\text{-}x}$	pressure transmitters technical certificate
Cert-$_{T4.4.9\text{-}x}$	level transmitters technical certificate
Cert-$_{T4.4.10\text{-}x}$	temperature transmitters technical certificate
Cert-$_{T4.4.11\text{-}x}$	signal transmitters technical certificate
Cert-$_{T4.4.12\text{-}x}$	signal conditioning technical certificate

Chapter 5

SNP DESIGNS PERFORMANCE EVALUATION

This thesis research has proposed a fundamental nuclear practices change, of the first-of-the-kind total network-based nuclear operations. There are no particularly suitable methods available, after exhaustive research, for the evaluation of the innovative *SNP* designs developed in this thesis. For this kind of situations, it would be a good approach for finding an evaluation methodology is referenced to the original objectives of the fundamental change. The two major objectives of the *Security-integrated Nuclear Process*, ***SNP*** designs developed in this thesis are economic & efficiency advancements and safety & security enhancements for nuclear modernization. The performance evaluation presented in this chapter is built upon these two objectives.

For the evaluation of the tremendous economic & efficiency advancement of the *SNP* designs, this thesis research creates a cost model termed ***NCM***, the *Nuclear Cost Model* for the current nuclear practices and establishes it as a reference base for the *SNP* design performance analysis, and creates another model termed ***CSM***, the *Cost Saving Model* for the analytical evaluation of the new *SNP* designs in terms of cost savings opportunity. This chapter presents these two models and also presents the numerical analysis of the *SNP* designs using these models.

For the evaluation of the safety & security enhancements of the *SNP* designs, the previous chapters have already described the significance of the safety and security aspects of the *SNP* designs, from time to time while the development of these designs were being presented. This chapter presents the numerical assessments of the network pre-access authentication process for the nuclear network access control as designed in this thesis research.

This chapter presents:

Section 5.1:	This section creates *NCM* the *nuclear cost models* for the current nuclear practices and establishes a reference base for the *SNP* designs analysis. This section presents the numerical evaluation of the cost models on the current nuclear practices, places the focus of the nuclear design analysis in proper order of magnitude of significance, and finally creates a meaningful and practical reference base for nuclear practice changes comparison.

Section 5.2: This section presents an overall assessment of the whole process of the new *SNP* access control designed in this thesis research, in three aspects: the *SNP* design is to provide an innovative network base for carrying out the nuclear operations in an efficient way; the *Operation-Based Access Control OBAC* design is to improve the nuclear work process; and the *Nuclear Operation Access Authentication NOAA* design is to enhance the nuclear process operation security.

Section 5.3: This section presents the creation of *CSM* the *cost saving models* for the analytical evaluation of the new *SNP* designs, in terms of cost savings opportunity, as for the time being the best measure of the merit of a practice change for performing the same or better functions as the existing ones in the industry is the *cost savings* that the new change can bring in.

Section 5.4: This section presents the numerical analysis of the performance of the *SNP* designs developed in this thesis research. This section demonstrates with numerical computations, the four types of characteristics as a measure of the merit of the practice changes in terms of cost savings. They are: the incremental cost saving contributed by the *SNP*, the accumulative cost saving contributed by *SNP*, the incremental cost saving contributed by the *Smart Process Controllers* (*SPC*), the accumulative cost saving contributed by *SPC*, and the total accumulative cost saving contributed by both the implementation of the *SNP* and the installation of the *SPC*.

Section 5.5: This section presents the analysis of *NOAA*, the operation-based authentication access and *APP*, the authentication pre-access protocol. The analysis includes numerical evaluation and simulation assessment.

5.1 Creation of Reference Base for Nuclear Designs Performance Analysis

The most appropriate measure of the merit of practice changes for performing the same or better functions as the existing ones in the industry is the *cost saving* that the new changes can bring in and for the nuclear industry specifically, the *safety* and *security* that the new changes can enhance, as the nuclear safety & security practical designs and cost savings are the emphasis of this thesis research.

This section creates *NCM*, the *nuclear cost models* for the current nuclear practices evaluations and establishes a reference base for the *SNP* designs analysis. For establishment of the analysis reference base, the nuclear equipment maintenance is used. The nuclear equipment maintenance includes setting adjustments, calibrations, replacements, etc. Most of the equipment maintenances are carried out during the nuclear unit outage; some may be carried out during the unit forced outage due to some events; some may be carried out during the on-line live operations.

This section presents the numerical evaluation of the cost models on current nuclear practices, places the focus of the nuclear design change analysis in proper order of magnitude of significance supported, and finally creates a meaningful and practical reference base for nuclear design changes comparisons.

5.1.1 NCM: Nuclear Cost Models

The following develops 5 *NCM* models for the nuclear equipment maintenance, as a reference base for nuclear design changes performance comparison.

NCM_1: Base Cost of Equipment Maintenance on Scheduled Nuclear Unit Outage

Nuclear Conditions for Modelling:

The equipment maintenance is usually carried out during the nuclear unit outage, of which the equipment will be re-calibrated or replaced if the calibration fails. During the outage, all equipment likely will undergo the maintenance of various kinds or degrees regardless of the operating status of particular equipment.

Parameters of Modelling:

Tp_{so} = **T**ime for **p**reparation of equipment maintenance for **s**cheduled **o**utage

Tm_{so} = **T**ime for **m**aintenance of equipment for **s**cheduled **o**utage

Np_{so} = **N**umber of labour for **p**reparation of equipment maintenance for **s**cheduled **o**utage

Nm_{so} = **N**umber of labour for **m**aintenance of equipment for **s**cheduled **o**utage

Rp_{so} = **R**ate (average) of labour for **p**reparation of maintenance for **s**cheduled **o**utage

Rm_{so} = **R**ate (average) of labour for **m**aintenance of equipment for **s**cheduled **o**utage

$Rrev$ = **R**ate of loss of **rev**enue

Cem = **C**ost of **e**ngineering designs and **m**aterials

Cost Model for Scheduled Outage Maintenance as Base:

$$NCM\_1 = Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so} + Tm_{so} \times Rrev + Cem$$

The above cost expression includes the maintenance preparation cost, the maintenance execution cost, loss of revenue, and engineering & materials cost.

NCM_2: Additional Cost due to On-line Equipment Maintenance

Nuclear Conditions for Modelling:

The on-line equipment maintenance decisions may depend upon the criticality of the function of the equipment in the nuclear process.

The equipment maintenance cannot be delayed if the physical field assessment demonstrates that the equipment deficiency or malfunction is going to cause a catastrophic failure of certain nuclear systems or even may potentially cause a nuclear safety event, then an on-line equipment maintenance may be initiated for fixing the deficiency of that equipment.

The on-line equipment maintenance can be initiated if the equipment performance deficiency of minor nature being alarmed or recorded during the on-line live operation, and the physical field assessment indicates that minor adjustments on the equipment settings are feasible/implementable and also are allowable by the established operation procedures for that equipment within the specified conditions.

Parameters of Modelling:

Tp_{on} = **T**ime for **p**reparation of **on**-line maintenance of equipment

Tm_{on} = **T**ime for **on**-line **m**aintenance of equipment

Np_{on} = **N**umber of labour for **p**reparation of **on**-line maintenance of equipment

Nm_{on} = **N**umber of labour for **on**-line **m**aintenance of equipment

R_{on} = **R**ate (average) of labour for **on**-line maintenance

C_{eam} = **C**ost of **e**ngineering designs and **m**aterials

Cost Model for On-line Maintenance:

$$NCM\_2 = (Tp_{on} \times Np_{on} + Tm_{on} \times Nm_{on}) \times R_{on} + C_{eam}$$

The above cost expression, in additional to ***NCM_1*** (the cost of routine scheduled outage maintenance that is not to be altered), includes the on-line maintenance preparation cost, the on-line maintenance execution cost, and the on-line engineering & materials cost (however, there is no additional loss of revenue for this on-line maintenance, as the nuclear unit still continues running and producing electricity).

NCM_3: Additional Cost due to Forced-Outage Equipment Maintenance

Conditions for Modelling:

The on-line equipment maintenance cannot be initiated if the physical field assessment shows that the performance deficiency during the live operation substantially exceeds the permitted ranges, of which the on-line adjustment is not allowed or is not supported by the established procedure.

The equipment maintenance cannot be delayed if the physical field assessment demonstrates that the equipment deficiency or malfunction are going to cause a catastrophic failure of certain nuclear systems or even may potentially cause a nuclear safety event, then a forced outage has to be initiated for fixing the deficiency of that equipment.

Also a forced outage needs to be initiated if there is a significant nuclear event that endangers the safety operation of the reactor.

Parameters of Modelling:

Tp_{fo} = **T**ime for **p**reparation of **f**orced-**o**utage maintenance of equipment

Tm_{fo} = **T**ime for **f**orced-**o**utage **m**aintenance of equipment

Np_{fo} = **N**umber of labour for **p**reparation of **f**orced-**o**utage maintenance of equipment

Nm_{fo} = **N**umber of labour for **f**orced-**o**utage **m**aintenance of equipment

R_{fo} = **R**ate (average) of labour for **f**orced-**o**utage maintenance

$Rrev$ = **R**ate of loss of **rev**enue

C_{eam} = **C**ost of **e**ngineering, **a**dministration, and **m**aterials

Cost Model for Forced Outage Maintenance:

$$NCM\_3 = (Tp_{fo} \times Np_{fo} + Tm_{fo} \times Nm_{fo}) \times Rm_{fo} + Tm_{fo} \times Rrev + C_{eam}$$

The above cost expression, in additional to ***NCM_1*** (the cost of routine scheduled outage maintenance that is not to be altered), includes the forced-outage maintenance preparation cost, the forced-outage maintenance execution cost, the forced-outage engineering & materials cost, and an additional loss of revenue due to the forced outage.

NCM_4: Additional Cost due to Delayed Equipment Maintenance

Conditions for Modelling:

The equipment maintenance may be delayed until the scheduled outage if the equipment deficiency is tolerable for the on-going operation conditions under which the equipment is being operated, upon a satisfactory physical field assessment.

If the equipment maintenance can be delayed until the scheduled outage, it is desirable not to carry out any on-line maintenance as it could increase the chance of expensive forced outage. Then, the equipment will be put on alert and will be under intensive monitoring for further maintenance decisions.

For critical equipment, there is usually a two-out-three implementation of physical devices and control logics in the nuclear process, such that if two out of three independent equipment of the same kind fail, then the function of these equipment is declared to be unavailable or fail. Under this failure condition, the physical field assessment is carried out to determine the equipment maintenance decision.

The equipment maintenance can be delayed until the scheduled outage even if a particular equipment fails but its failure will not cause an immediate nuclear safety concern or will not cause a nuclear system failure as its backup equipment takes over the control or operation.

Parameters of Modelling:

T_{ed} = **T**ime for **e**valuating of **d**elayed maintenance of equipment

T_{md} = **T**ime for **m**onitoring of **d**elayed maintenance of equipment

N_{em} = **N**umber of labour for **e**valuating and **m**onitoring of delayed maintenance of equipment

R_{em} = **R**ate (average) of labour for **e**valuating and **m**onitoring of delayed maintenance

Cost Model for Delayed Maintenance:

$$NCM\_4 = (T_{ed} + T_{md}) \times N_{em} \times R_{em}$$

The above cost expression, in additional to ***NCM_1*** (the cost of routine scheduled outage maintenance that is not to be altered), includes the delayed maintenance evaluation cost, the delayed maintenance monitoring cost (however, there is no additional loss of revenue or materials cost, as the equipment maintenance is delayed.

NCM_5: Equivalent Annual Cost for Equipment Maintenance

Conditions for Modelling:

It is useful to have an expression of the average annual cost for nuclear equipment maintenance in a nuclear unit.

Parameters of Modelling:

F_{so} = **F**requency for carrying out the **s**cheduled **o**utage for maintenance

F_{on} = **F**requency for carrying out the **on**-line maintenance

F_{fo} = **F**requency for carrying out the **f**orced **o**utage

F_{de} = **F**requency for carrying out the **de**layed outage

Average Annual Cost Model:

$$NCM\_5 = F_{so} \times NCM\_1 + F_{on} \times NCM\_2 + F_{fo} \times NCM\_3 + F_{de} \times NCM\_4$$

Table 5.1 summarizes the cost models for the current nuclear equipment maintenances, where the cost *NCM_1* is the base cost; *NCM_2* and *NCM_3* and *NCM_4* are additional costs above the base cost.

Table 5.1: Cost models for current maintenance

NCM_1 =	*Base Cost for Scheduled-outage Maintenance* $Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so} + Tm_{so} \times Rrev + C_{eam}$
NCM_2 =	*Additional Cost due to On-line Maintenance* $(Tp_{on} \times Np_{on} + Tm_{on} \times Nm_{on}) \times R_{on} + Ceam$
NCM_3 =	*Additional Cost due to Forced-outage Maintenance* $(Tp_{fo} \times Np_{fo} + Tm_{fo} \times Nm_{fo}) \times Rm_{fo} + Tm_{fo} \times Rrev + C_{eam}$
NCM_4 =	*Additional Cost due to Delayed Maintenance* $(T_{ed} + T_{md}) \times N_{em} \times R_{em}$
NCM_5 =	*Average Annual Cost for Maintenance* $F_{so} \times NCM\_1 + F_{on} \times NCM\_2 + F_{fo} \times NCM\_3 + F_{de} \times NCM\_4$

5.1.2 Numerical Evaluation of NCM, Nuclear Cost Models for Reference Base

This section presents the numerical evaluation of *NCM,* the *nuclear cost models* developed above.

The following estimates are to put the focus of the nuclear design analysis in the suitable *order of magnitude* of significance that further investigations are recommended for fine tuning, and to form a practical reference base for nuclear practice changes comparison.

5.1.2-1 ***Estimate on Base Cost per Outage per Unit***

- *Estimate on Cost per Outage due to Loss of Revenue*

A refurbished nuclear units generate over 800 MW/unit at an estimated rate of over \$60/MW/hr with 24 hr/day as a base-line operation, and its daily revenue will be > 800MW/unit × \$60/MW/hr × 24hr/day = \$1.15 million/day/unit. Other nuclear units generate electricity at an estimated lower rate of ≈ 70% that is \$0.8million/day/unit.

Estimate the rate of loss of revenue: $Rrev$ = \$0.8 million/day/unit.

The average duration of one scheduled outage > 25 days.

Estimate the time for maintenance per scheduled outage: Tm_{so} = 25 days

Estimate on loss of revenue per outage: $Tm_{so} \times Rrev = 25 \times 0.8 =$ \$20 million/outage/unit

- *Estimate on Cost of Labour per Outage*

The average labour rate is > \$80/hour. Estimate Rp_{so} = \$80/hr

The rate increases by ≈ 25% due to overtime. Estimate Rm_{so} = \$100/hr

The average number of CM staff for preparation > 15/unit. Estimate Np_{so} = 15/hr/unit

The average number of CM staff for outage maintenance > 60/unit. Estimate Nm_{so} = 60/hr/unit

The average duration of preparation between outages > 80 days. Estimate Tp_{so} = 1920 hr

The average duration of one outage > 25 days. Estimate Tm_{so} = 600 hr

Estimate on cost of labour per outage: $Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so}$

$= 1920 \times 15 \times 80 + 600 \times 60 \times 100 =$ \$5.904 million/outage/unit

The average estimated cost of engineering and materials ≈ 10% of the CM labour cost.

Estimate on cost of engineering and others: C_{eam} = \$0.590 million/outage/unit

- *Base Cost*

$NCM\_1 = (Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so}) + (Tm_{so} \times Rrev) + Cem = 5.904+20+0.590$

= \$26.494 million/outage/unit

5.1.2-2 **Estimate on Additional Cost due to On-line Maintenance**

- *Estimate on Cost of Labour per On-line Maintenance*

The average labour rate is > \$80/hour.

The rate increases by ≈ 25% due to overtime for on-line maintenance. Estimate R_{on} = \$100/hr

The average number of CM staff for preparation > 15/unit. Estimate Np_{so} = 15/hr/unit

The average number of CM staff for on-line maintenance > 20/unit. Estimate Nm_{so} = 20/hr/unit

The average duration of preparation for on-line maintenance > 2 days. Estimate Tp_{so} = 48 hr

The average duration of on-line maintenance > 1 days. Estimate Tm_{so} = 24 hr

Estimate on cost of labour per on-line maintenance: $(Tp_{on} \times Np_{on} + Tm_{so} \times Nm_{so}) \times R_{on}$
= (48×15 + 24×20) ×100 = \$0.12 million/on-line maintenance/unit

The average cost of engineering, administration, and materials ≈ 20% of the CM labour cost.

Estimate on cost of engineering and others: C_{eam} = \$0.024 million/on-line maintenance/unit

- *Additional Cost due to On-line Maintenance*

NCM_2 = 0.12+0.024 = \$0.144 million/on-line maintenance/unit

5.1.2-3 **Estimate on Additional Cost due to Forced Outage**

- *Estimate on Cost per Forced Outage due to Loss of Revenue*

Estimate the rate of loss of revenue: $Rrev$ = \$0.8 million/day/unit.

The average duration of one forced outage > 5 days. Estimate: Tm_{so} = 5 days

Estimate on loss of revenue per forced outage:
$Tm_{so} \times Rrev$ =5×0.8 = \$4.0 million/forced-outage/unit

- *Estimate on Cost of Labour per Forced Outage*

The average labour rate is > \$80/hour.

The rate increases by ≈ 25% due to overtime for forced outage. Estimate R_{fo} = \$100/hr

The average number of CM staff for forced-outage preparation>30/unit. Estimate Np_{so} = 30/hr/unit

The average number of CM staff for forced-outage maintenance>60/unit. Estimate Nm_{so}=60/hr/unit

The average duration of preparation for forced outage > 1 day. Estimate Tp_{so} = 24 hr

The average duration of one forced outage > 5 days. Estimate Tm_{so} = 120 hr

Estimate on cost of labour per forced outage:
$(Tp_{fo} \times Np_{fo} + Tm_{fo} \times Nm_{fo}) \times R_{fo}$ = (24×30+120×60×100 = \$0.792 million/forced-outage/unit

The average cost of engineering, administration, and materials ≈ 15% of the CM labour cost.

Estimate on cost of engineering and others: C_{eam} = \$0.119 million/forced-outage/unit

- *Additional Cost due to Forced Outage*

NCM_3 = 4.0 + 0.792 +0.119 = \$4.911 million/forced-outage/unit

5.1.2-4 ***Estimate on Additional Cost due to Delayed Maintenance***

- *Estimate on Cost of Labour per Delayed Maintenance*

The average labour rate is > \$80/hour. Estimate R_{em} = \$80/hr

The average number of CM staff for evaluating and monitoring>15/unit. Estimate N_{em} = 15/hr/unit

The average duration of evaluating delayed maintenance > 1 days. Estimate T_{ed} = 24 hr

The average duration of monitoring delayed maintenance > 5 days. Estimate T_{md} = 120 hr

Estimate on cost of labour per delayed maintenance:
$(T_{ed} + T_{md}) \times N_{em} \times R_{em}$ = (24 + 120) × 15 × 80 = \$0.173 million/delayed-maintenance/unit

- *Additional Cost due to Delayed Maintenance*

NCM_4 = \$0.173 million/delayed-maintenance/unit

5.1.2-5 ***Estimate on Average Annual Cost for Maintenance***

- *Estimate on Frequencies for 4 types of Nuclear Equipment Maintenance*

The frequency for scheduled outage is once (1) per 2.5 years. Estimate F_{so} = 1/2.5yr

The frequency for on-line maintenance is twice (2) per year. Estimate F_{on} = 2/yr

The frequency for forced outage is once (1) per 6 years. Estimate F_{fo} = 1/6yr

The frequency for delayed maintenance is three times (3) per year. Estimate F_{de} = 3/yr

- *Average Annual Cost for Maintenance*

Annual cost from scheduled outage maintenance:

$F_{so} \times NCM\_1 = (1/2.5) \times 26.494 = \$10.598$ million/year

Annual cost from on-line maintenance:

$F_{on} \times NCM\_2 = 2 \times 0.144 = \$0.288$ million/year

Annual cost from forced maintenance:

$F_{fo} \times NCM\_3 = (1/6) \times 4.911 = \$0.819$ million/year

Annual cost from delayed maintenance:

$F_{de} \times NCM\_4 = 3 \times 0.173 = \$0.519$ million/year

Total average Annual cost from all types of maintenance:

$NCM\_5 = 10.598 + 0.288 + 0.819 + 0.519 = \$12.224$ million/year

Table 5.2 summarizes the cost data for the current equipment maintenances, where *NCM_1* is the base cost; *NCM_2*, *NCM_3* and *NCM_4* are additional costs above the base cost.

Table 5.2: Cost models for current maintenance

NCM_1 =	*Base Cost* = $26.494 million/outage/unit
NCM_2 =	*Additional Cost* = $0.144 million/on-line maintenance/unit
NCM_3 =	*Additional Cost* = $4.911 million/forced-outage/unit
NCM_4 =	*Additional Cost* = $0.173 million/delayed-maintenance/unit
NCM_5 =	*Annual Cost* = *$12.224 million/year/unit*

Note: Table 5.2 shows that whenever an outage is involved, the cost will be high. Therefore, the operation should avoid or minimize the occurrence of any outage if possible.

5.2 An Overall Assessment of New SNP Access Control

This section presents an overall assessment of the whole process of the new *SNP* access control designed in this thesis research. There are three aspects in this thesis design focus: the *SNP* design provides an innovative network base for carrying out the nuclear operations in an efficient way; the operation-based access control *OBAC* design is to enhance the nuclear work process; and the *Nuclear Operation Access Authentication NOAA* design is to enhance the nuclear process operation security. The assessment of the designs of *SNP*, *OBAC*, and *NOAA* are provided below.

5.2.1 Assessment of SNP Network Data Base

The formation of this data base is based on the physical installations, equipment specifications, operation records, training records, etc. This data base is a live data base that means the data base is to be updated, as required such as when a new device is installed, an equipment is replaced, the operation conditions/procedures are changed, etc. However, once the complete data base is formed, the continuous update effort is minimal but essential.

The network data base, once established, is always available for any nuclear operation use and whenever it is needed. This data base can reduce the burden of the supervisor for searching for the experience and technical qualifications of the user, can eliminate the possibility of errors involving wrong person/equipment and the serious nuclear consequences, and can shorten the work process particularly for time-critical on-line maintenance or during a nuclear event.

The cost for the initial establishment of the *SNP* network data base is a ***one-time capital cost*** and the cost for continuous update is minimal. The total cost for the complete *SNP* network data base is insignificant when compared to the continuous expensive current nuclear practices as illustrated in the section above. However, the cost savings and associated benefits for the use of the *SNP* network data base are tremendous.

5.2.2 Assessment of SNP Mapping of Operations to Requirements

The *SNP-OBAC* mapping is to be conducted by several teams of authorized operators, technical managers, supervisors, engineers, technical experts, experienced field staff, etc. The mapping data base is also a live data base that is to be continuously updated to ensure its currency and accuracy.

The *SNP-OBAC* mapping improves the weakness of the current mapping practice for matching a nuclear work order to its requirements as well as the qualifications of the person to be assigned to carry out that work order. Of the current nuclear practices, the mapping is dependent on the discretions of the supervisors. The supervisors have to perform exhaustive searches in order to ensure the correctness of the mapping and the matching of the implementers' qualifications to the work orders. The supervisor has to do this for each work order.

The *SNP-OBAC* mapping, once the mapping system is established, is always available for any nuclear operation use and whenever it is needed. The *SNP-OBAC* mapping system provides an "instantaneous" mapping for the user whenever the user wants to use without feeling of any delay as the mapping by the computer takes a tiny fraction of a second to complete.

The ***operational cost*** for using the *SNP-OBAC* mapping system is insignificant and negligible, as compared to the current practice carried out by the supervisors.

5.2.3 Assessment of Authentication of Users' Access Qualifications

The *user-x* is required to submit his/her certifications to the network authentication server running on *NOAA* the *Nuclear Operation Access Authentication* algorithm designed in this thesis research. The server will issue a time-stamped access code for each certification that passes the authentication. The access code is valid for the time period specified for increased security. If the *user-x* is assigned to carry out several work tasks within a period of time and some tasks have the same and overlapping requirements, the user does not have to repeat the authentications for the overlapping requirements if their access codes are still valid for the time of access.

The ***operational cost*** for using the *NOAA* authentication system is insignificant and negligible, as compared to the current practice carried out by the supervisors for validation of the user's both experience and technical qualifications against the work order requirements.

5.2.4 Assessment of Secure Access to Nuclear Process and Operations

The assessment of this stage is to be detailed in the following section.

5.3 Creation of CSM: *Cost Saving Models* for Analytical Evaluation of SNP Designs

The most appropriate measure of the merit of a practical process/design change for performing the same or better functions as the existing one in the industry is the *cost savings* that the new design can bring in. This section presents the creation of *CSM* the *cost saving models* for the analytical evaluation of the new *SNP* designs, in terms of cost savings opportunity (followed with a numerical analysis in the next section).

5.3.1 Cost Saving Opportunity

As of today there are thousands of analog or discrete digital devices of old technology still operating in the nuclear plant and these devices generally require intensive labour care. Even if equipment made of newer network-based technology have been installed but their networking capability is not used, these equipment are then treated of no difference from the old devices. Similarly, the current practices for processing of nuclear operation data are fairly inefficient, labour-intensive and costly, due to numerous analog or discrete digital devices of old technology still operating in the nuclear plant or newer equipment with their networking capability limited due to safety and security concerns.

The new designs of *SNP*, *OBAC*, and *NOAA* are developed in this thesis research to address the security aspect of using the network-based intelligent process controls for the nuclear operations. Once the security concern is resolved, today's Smart Process Controllers (*SPC*) that have networking capability with intelligent features of central data processing, equipment/systems operations optimizing and coordinating, predictive maintenance scheduling, etc. can be used to substantially improve the nuclear operations, resulting in efficient and reliable nuclear process with significant cost savings.

In the nuclear industry, the acceptance of any initial changes/modifications such as configuration modification, new procedures, new devices, new systems, etc. is fairly slow. But, once the change is accepted, the adaption will be progressively fast. From years of experiences in nuclear design, nuclear commissioning, nuclear field engineering, nuclear modification & project management, etc., the successful changes are to be implemented in a progressive and accelerative fashion. The cost savings are to be realized in a similar fashion and can be modelled as follows.

5.3.2 *CSM for SNP Implementation*

a) *Accumulative Saving from SNP*

The operation savings from the implementation of the *SNP* designs can increase with time in progressive and accelerative fashion, and the accumulative savings from the *SNP* can be modelled as:

$$\textbf{\textit{CSM}}_{\text{-}SNP}: \boxed{\boldsymbol{S_{SNP}} = \sum_{i=0}\left\{\boldsymbol{R_{SNP}} \times \left[\boldsymbol{limit}\,{}_{\mathbf{0}}^{\boldsymbol{P_{max}}}\boldsymbol{P_0}\left(\boldsymbol{e}^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right)\right] \times \boldsymbol{\Delta t_{SNP}}\right\}}$$

Parameters:

$\boldsymbol{S_{SNP}}$ = operation savings from the implementation of the *SNP* designs that simplify significantly the work order process and document control.

$\boldsymbol{P_{max}}$ = maximum amount of documentation to be changed.

$\boldsymbol{P_0}$ = initial amount of documentation to be changed for accounting the start of this saving process.

$\boldsymbol{\Delta t_{SNP}}$ = average time interval between the major changes of documentation due to the *SNP* implementation.

$\boldsymbol{\tau_{SNP}}$ = time constant for the change of documentation due to the *SNP* implementation.

$\boldsymbol{R_{SNP}}$ = rate of operation saving benefited from the *SNP* implementation per document per year

$$\left[limit\,{}_{0}^{P_{max}}P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right)\right] \Rightarrow \text{ If } P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right) > P_{max}, \text{ then set } P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right) = P_{max}.$$

b) *Steady-State Annual Saving from SNP*

Initially, the annual saving benefited from the SNP designs increases rapidly as the amount of documentation change increases. Finally, when all the documentations have been changed, the annual saving reaches the steady state. Therefore, when $P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right) = P_{max}$, the annual saving is the highest that is the steady-state annual saving.

$$\textbf{\textit{CSM}}_{\textbf{\textit{Annual-SNP}}}: \boxed{\begin{aligned} &A\_\boldsymbol{S_{SNP}} = \boldsymbol{R_{SNP}} \times \boldsymbol{P_{max}} \\ &\Rightarrow \boldsymbol{R_{SNP}} = A\_\boldsymbol{S_{SNP}} \div \boldsymbol{P_{max}} \end{aligned}}$$

5.3.3 CSM for SPC Implementation

a) *Accumulative Saving from SPC*

The operational savings from the implementation of *SPC* devices can increase with time in progressive and accelerative fashion and can be modelled as:

***CSM*-SPC:**

$$\boxed{\boldsymbol{S_{SPC} = \sum_{j=0}\left\{R_{SPC} \times \left[limit\,{}_{0}^{D_{max}} D_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right)\right] \times \Delta t_{SPC}\right\}}}$$

Parameters:

$\boldsymbol{S_{SPC}}$ = operation savings from the implementation of the *SPC* smart devices that simplify significantly the nuclear operation process and equipment maintenance, and most importantly reduce the occurrence of expensive forced outages as well as shorten the duration of scheduled outages, resulting in significant savings.

$\boldsymbol{D_{max}}$ = maximum number of nuclear devices to be changed.

$\boldsymbol{D_0}$ = initial number of devices to be changed for accounting the start of this saving process.

$\boldsymbol{\Delta t_{SPC}}$ = average time interval between the major installations of new *SPC* smart devices due to the *SNP* implementation and most likely between the scheduled outages.

$\boldsymbol{\tau_{SPC}}$ = time constant for the change of the amount of *SPC* installations due to the *SNP* implementation.

$\boldsymbol{R_{SPC}}$ = rate of operation saving benefited from the *SPC* implementation (upon the availability of the *SNP* designs developed in this thesis research) per device per year.

$$\left[limit\,{}_{0}^{D_{max}} P_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right)\right] \Rightarrow \text{ If } D_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right) > D_{max}, \text{ then set } D_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right) = D_{max}.$$

b) *Steady-State Annual Saving from SPC*

Initially, the annual saving benefited from the SPC devices can increase rapidly as the amount of devices installation increases. Finally, when all the devices have been installed, the annual saving reaches the steady state. Therefore, when $D_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right) = D_{max}$, the annual saving is the highest that is the steady-state annual saving.

CSM$_{\text{Annual-SPC}}$:

$$\boxed{\begin{aligned} &A\_\boldsymbol{S_{SPC}} = \boldsymbol{R_{SPC}} \times \boldsymbol{D_{max}} \\ &\Longrightarrow \boldsymbol{R_{SPC}} = A\_\boldsymbol{S_{SPC}} \div \boldsymbol{D_{max}} \end{aligned}}$$

The total amount of the operation saving from the implementations of the *SNP* and *SPC* is the sum of the above-mentioned savings.

CSM$_{\text{-SNP+SPC}}$: *Total Savings from SNP and SPC*

$$\boxed{\boldsymbol{S_{Total}} = \boldsymbol{S_{SNP}} + \boldsymbol{S_{SPC}}}$$

5.3.4 Contributing Factors for CSM from SNP Designs

In the current nuclear generating station, most of the nuclear devices/equipment are being operated, monitored, data processed, and maintained in the older traditional fashions. The current practices for the execution of nuclear equipment maintenance are fairly inefficient, labour-intensive and costly, from today's smart system and technology point of view. The *SNP* designs are developed to improve these traditional nuclear practices. The *SNP* design aims to increase the efficiency of equipment maintenance, reduce the number of outages particularly those unscheduled forced outages, and minimize the duration of each outage.

The *SNP* cost is a one-time cost and is only a small fraction of one day forced outage. The *SNP* design may avoid some forced outages and each forced outage may take a few days to complete. The *SNP* design may reduce substantially the duration of each scheduled outage that may take a month to complete. Therefore the cost of *SNP* is insignificant compared to the potential savings that it brings to the nuclear plant.

The following identifies the contributing factors (**CF_n**) for the cost savings created by the implementation of the *SNP* designs.

5.3.3-1 **CF_1** *- Contributing Factor of SNP for Maintenance Initiation*

Current state: When the performance of an equipment deteriorates out of its designed tolerance, an alarm will be initiated. The alarm of critical or emergency nature will draw an immediate attention of the control & maintenance (CM) staff who is responsible of this equipment. If the alarm is of minor nature, the CM staff will notice it during the routine work process. After the CM staff receive the equipment alarm, the staff start the physical field assessment. The field assessment could be fairly complex if the equipment is nuclear-safety-related equipment, or its installation is the radiation active zone, or its maintenance affects substantially other equipment, or even the inspection of its deficiency may impact on the health operations of other equipment.

CF_1: The *SNP* designs will facilitate the intelligent features of smart equipment to make the equipment performance information readily available for the preparer to use for review of equipment performance track records and for assessment of the equipment deficiency. This eliminates the physical collection of equipment performance and physical field assessment of the equipment deficiency conditions.

Current state: If the physical field assessment carried out by the CM staff indicates that the equipment deficiency can be fixed with minor adjustments and such minor adjustments on the equipment settings are feasible/implementable and also are allowable by the established operation procedures for that equipment within the specified conditions, then the CM staff will prepare paper work for the initiation of an on-line live equipment maintenance.

CF_1: The *SNP* designs will expedite the paper work for the initiation of an on-line maintenance as all the required data are readily available at the CM staff's desk-top computer.

5.3.3-2 **CF_2** *- Contributing Factor of SNP for Delayed Maintenance Preparation*

Current state: If the physical field assessment shows that the equipment performance deficiency during the live operation substantially exceeds the permitted ranges, of which the on-line adjustment is not allowed or is not supported by the established procedure, then the CM staff will prepare paper work for reporting the findings to their superiors for maintenance decisions.

CF_2: The *SNP* designs will expedite the CM staff's paper work and will facilitate the supervisors' maintenance decisions, as all the data that the CM staff or their supervisors need to know for reporting or making decisions are readily available at their desk-top computers.

Current state: If the field assessment shows that the equipment deficiency is tolerable for the on-going operation conditions under which the equipment is being operated and the equipment maintenance can be delayed until the scheduled outage, then the CM staff will put the equipment on alert for intensive monitoring of any further performance deterioration and prepare paper work for reporting the conditions to their superiors for further actions.

CF_2: The *SNP* designs will facilitate the monitoring of the alarmed equipment with instantaneous information in the office environment.

5.3.3-3 ***CF_3*** *- Contributing Factor of SNP for On-Line Maintenance Preparation*

Current state: If the field assessment demonstrates that the equipment maintenance cannot be delayed because the equipment deficiency or malfunction are going to cause a catastrophic failure of certain nuclear systems or even may potentially cause a nuclear safety event, then the CM staff may recommend an on-line equipment maintenance or may report to their superiors for immediate actions if the deficiency condition is very severe that a forced outage may be warranted. The CM staff will prepare paper work if they recommend an on-line equipment maintenance.

The paper work and preparation time required for initiating an on-line equipment maintenance depends on the conditions of the equipment deficiency and its impacts on other equipment. It can be a simple scenario that the CM staff will collect equipment performance information, conduct observations on the equipment deficiency, carry out field assessment of the deficiency conditions and impacts on other equipment, prepare an on-line equipment maintenance plan, prepare a back-out plan when the performance of deficient equipment or affected nuclear systems starts to deteriorate, and submit the whole on-line equipment maintenance plan to an independent verifier for verification.

***CF_3*:** The *SNP* design will significantly expedite the preparation of the equipment maintenance plan. The time saving is especially important for the on-line live equipment maintenance as first, the equipment can resume rapidly its normal health operation and second, the longer the equipment deficiency is not corrected then the higher probability the deficiency may cause adverse impacts on other equipment or systems.

Current state: If the conditions of the equipment deficiency and its impacts on other equipment are beyond the scope of the CM staff's responsibility or their capability, the preparation of the on-line equipment maintenance may involve engineering department's input. Then in additional to the above preparation work list, the CM staff will provide the equipment performance information to the engineering department, and seek advices from the engineering staff, and incorporate the advices into their on-line equipment maintenance plan.

***CF_3*:** The *SNP* design will facilities the communication and data transfer between the CM staff and the engineering staff and in fact, all the equipment data that the engineering staff need to use for formation of advices are readily available at their desk-top computers.

5.3.3-4 ***CF_4*** *- Contributing Factor of SNP for Maintenance Verification*

Current state: The equipment maintenance decisions and plans are required to be verified and accepted by an independent verifier. The verifier usually has extensive experiences on the subject equipment and is responsible for the technical contents of the maintenance plan. The verifier will:

- review the equipment maintenance plan,
- review equipment performance information relative to the plan,
- verify the plan that it can address the equipment deficiency conditions, and
- verify the plan that it has no foreseeable adverse impact on other equipment or other nuclear systems by reviewing relative documents, records, etc.

However, considerable amount of time is often spent in the verification process as the verifiers are required to conduct an independent verification by examining all related information and technical data.

***CF_4*:** The *SNP* design will expedite the verification work progress as all the information/data that the verifiers need are readily available to their desk-top computers. Also the verifier can review the equipment deficiency data independently and simultaneously at the time the preparation of the maintenance plans by the CM staff are close to complete that can significantly speed up the verification of on-line maintenance.

5.3.3-5 ***CF_5*** *- Contributing Factor of SNP for Maintenance Approval*

Current state: The maintenance decisions and plans after passing the verification are to be sent to the approvers for the final approval before the maintenance is executed. The approvers are usually in the senior management positions. The responsibility of the approvers is to ensure the plan satisfying nuclear regulations. The approver will:

- check the qualifications of the preparer, relative to the nature of the maintenance plan,
- check the qualifications of the verifier, with respect to the subject matter,
- check the maintenance plan to ensure it do not violate any nuclear regulations

However, considerable amount of time is often spent in the approval process as the approvers are required to conduct the above-mentioned staff's qualifications and nuclear regulations checks.

***CF_5*:** The *SNP* design also will expedite the approval work as the approver can review the preparer's qualification and the verifier's expertize while the maintenance plan is being prepared, as their qualifications are made readily available with the *SNP* design. The approver can examine the maintenance plan with respect to the nuclear regulations while the plan is being verified.

5.3.3-6 ***CF_6*** *- Contributing Factor of SNP for Maintenance Execution*

Current state: To date in the nuclear plant, the implementation of an equipment maintenance requires equipment maintenance plans, work orders, maintenance work plans execution, and the operation authority's acceptance for return to services after the maintenance work. The equipment maintenance plan preparation has been mentioned above.

The formation of a work order is similar to, but much simpler than, that of a maintenance plan, and it still requires a preparer, a verifier, and an approver.

The execution of a maintenance work plan requires two teams (at least of two persons): one team for carrying out the maintenance work that includes installation, commissioning for new replacements, and testing; the other team for carrying out independent checking, monitoring, recording, etc.

The maintenance work order implementation is to be verified independently by the nuclear operators, and the completion of the work order requires the acceptance of the nuclear operation authority.

***CF_6*:** The *SNP* is designed to facilitate the equipment maintenance execution, to expedite the preparation, verification, and approval of work order, to speed up the equipment replacements or adjustments, including commissioning, testing, etc., and to accelerate the acceptance by the operation authority for the return of the equipment to services after maintenance.

5.3.3-7 ***CF_7*** *- Contributing Factor of SNP for Equipment Monitoring and Data Processing*

Current state: The nuclear devices are divided in small groups of similar technical functions, of close locations, or of the same nuclear systems. Then a certain number of nuclear operators/technical staff forming a team are responsible for a certain number of groups of nuclear devices. The formation of a team of nuclear operators responsible for a particular group of nuclear devices primarily depends on the discretions of the supervising management staff according to their understanding of the candidates' credential, trainings, and experiences, versus the requirements for the monitoring of the group of devices.

***CF_7*:** The *SNP* is designed to increase the correctness and efficiency of formation of a team of operators responsible for certain groups of nuclear devices monitoring. This can reduce the reliance on the supervisors' discretions on the candidates' information (credential, training, experiences, etc.) that were "available" to them or they have to conduct an exhaustive search for the sufficient required information.

Current state: Each team of nuclear operators work in shifts, with backup staff of the same required levels of trainings, for the 24-hour nuclear power electricity generation. The team of nuclear operators have been intensively trained with the detailed *operation* knowledge of the devices that they are responsible for monitoring, but not necessary with the in-depth or wide breadth technical knowledge of the type of devices that they are assigned with responsibility. This may increase the difficulty of transferring responsibility of handling similar type of devices to them.

***CF_7*:** The *SNP* is designed to expand the availability of qualified operators for backups of a large number of groups of devices' monitoring by forming a *SNP* network base of which the required qualifications of a candidate can be verified automatically, instead of depending on the supervisors' decisions. This is equivalent to reduction of the backup reserve requirements, leading to significant cost saving and/or work environment improvement such as flexible vacation allocation.

Current state: Each team performs daily routine checks either in the control room for critical signals monitoring or by conducting physical walkdowns to the device installations. Each team carries out daily routine recordings and data logs according to the established operation procedure. Each record involves three technical personnel: preparer, verifier, and approver. As most of the nuclear devices are discrete in implementations, the data collections from these devices become labour-intensive burdens. It is not uncommon that paper chart recorders are still in use for trend recordings of certain nuclear operation performances.

***CF_7*:** The *SNP* is designed to improve the efficiency of the nuclear devices monitoring and reduce the amount of monitoring work that includes reduction of physical walkdowns and daily routine recording effort, with the devices' data readily available from the formation of the *SNP* network.

Current state: If any data being recorded exceed their specified/expected ranges, the team will report them to their superiors for decisions, following the established procedures. However, this may considerably delay the remedy decisions or the damage controls. In case of nuclear event happening, the team will follow the established procedures and will make as many recordings as the nuclear conditions permit, particularly the safety of the team staff.

***CF_7*:** The *SNP* is designed to increase the awareness of the nuclear devices or systems' abnormal performance or out-of-range data and responsiveness to such conditions, through the *SNP* network base. Increase, during a nuclear event, the capability and the amount of data collection for post-event analysis. This can speed up the event resolution.

Current state: As of today there are still numerous analog or discrete digital devices of old technology operating in the nuclear plant, this severely limits the opportunity of central processing of data from all nuclear devices for operations optimization and coordination, and predictive maintenance scheduling.

CF_7: The *SNP* is designed to address the security aspect of using the network-based process control for nuclear operations, with the new designs of *SNP*, *OBAC*, and *NOAA* developed in this thesis research. Once the security concern is resolved, today's smart process control equipment that have networking capability with intelligent features of central data processing, equipment/systems operations optimizing and coordinating, predictive maintenance scheduling, etc. can be used to substantially improve the nuclear operations, resulting in efficient and reliable nuclear process with significant cost savings.

5.3.3-8 *Combined Contributing Factor of SNP to Reduction of Annual Maintenance Cost*

The above-mentioned seven (7) factors created by the *SNP* designs will make various contributions to the reduction of the annual maintenance cost of a nuclear unit. In additional, their contributions may vary with time along the progress of the implementation of the *SNP* designs and the execution of the designs in the actual nuclear operations. The combined contributing factor can be expressed as:

$$\boldsymbol{CF_{combined}} = \{\boldsymbol{CF_1},\ \boldsymbol{CF_2},\ \boldsymbol{CF_3},\ \boldsymbol{CF_4},\ \boldsymbol{CF_5},\ \boldsymbol{CF_6},\ \boldsymbol{CF_7}\}$$

After the *SNP* designs are successfully implemented, the *final* contribution of the combined factor to the reduction of the annual maintenance cost of one nuclear unit can be expressed as:

$$\boxed{\begin{aligned} A\_\boldsymbol{S}_{final} &= \boldsymbol{CF_{combined}} \times NCM\_5 \\ &= \boldsymbol{CF_{combined}} \times \{ \boldsymbol{F_{so}} \times \boldsymbol{NCM\_1} + \boldsymbol{F_{on}} \times \boldsymbol{NCM\_2} + \boldsymbol{F_{fo}} \times \boldsymbol{NCM\_3} + \boldsymbol{F_{de}} \times \boldsymbol{NCM\_4} \} \end{aligned}}$$

5.4 Numerical Analysis of SNP Designs Performance

This section presents the numerical analysis of the performance of the *SNP* designs developed in this thesis research. This section also demonstrates, with numerical computations, the four types of characteristics as a measure of the merit of the designs in terms of the cost saving, and they are: the incremental cost saving contributed by the *SNP*, the accumulative cost saving contributed by *SNP*, the incremental cost saving contributed by the *SPC*, the accumulative cost saving contributed by *SPC*, and the total accumulative cost saving contributed by both the implementation of the *SNP* and the installation of the *SPC*.

5.4.1 NCM, the *Reference Base for Design Analysis*

As a reference base for analysis of new designs developed in this thesis research, Table 5.3 summarize the cost models and numerical evaluation of the current practices of nuclear equipment maintenances for the four (4) typical nuclear operating conditions as discussed in section 5.1.

Table 5.3: Cost models and evaluations for current maintenance

Scheduled-outage *NCM_1*	$Tp_{so} \times Np_{so} \times Rp_{so} + Tm_{so} \times Nm_{so} \times Rm_{so} + Tm_{so} \times Rrev + C_{eam}$ = 1920×15×80 + 600×60×100 + 25×800,000 + 590,000 = *\$26.494 million/outage/unit*
On-line maintenance *NCM_2*	$(Tp_{on} \times Np_{on} + Tm_{on} \times Nm_{on}) \times R_{on} + Ceam$ = (48×15 + 24×20) ×100 + 24,000 = *\$0.144 million/on-line maintenance/unit*
Forced-outage *NCM_3*	$(Tp_{fo} \times Np_{fo} + Tm_{fo} \times Nm_{fo}) \times Rm_{fo} + Tm_{fo} \times Rrev + C_{eam}$ = (24×30 + 120×60) × 100 + 5 × 800,000 + 119,000 = *\$4.911 million/forced-outage/unit*
Delayed maintenance *NCM_4*	$(T_{ed} + T_{md}) \times N_{em} \times R_{em}$ = (24 + 120) × 15 × 80 = *\$0.173 million/delayed-maintenance/unit*
Annual Cost NCM_5	$F_{so} \times NCM\_1 + F_{on} \times NCM\_2 + F_{fo} \times NCM\_3 + F_{de} \times NCM\_4$ = (1/2.5)×26.494 + 2×0.144 + (1/6)×4.911 + 3×0.173 = 10.598 + 0.288 + 0.819 + 0.519 = \$12.224 million/year/unit

Table 5.3 shows that whenever an outage is involved, the cost becomes very high. The operations therefore should avoid or minimize the occurrence of any outage whenever/wherever possible. This table is to be utilized as a reference base for the analysis of the *SNP* designs in the following sections.

5.4.2 Numerical Evaluation of CSM, the *Cost Saving Models*

The most appropriate measure of the merit of a practical process/design change for performing the same or better functions as the existing one in the industry is the *cost saving* that the new design can bring in. The following present a numerical analysis of the new *SNP* designs, in terms of cost savings.

Table 5.4 summarizes *CSM*, the *cost savings models* created in this thesis research. The models are used to carry out the numerical analysis of the *SNP* designs.

Table 5.4: CSM, the cost saving models

S_{SNP}	$= \sum_{i=0} \left\{ R_{SNP} \times \left[limit\,_{0}^{P_{max}} P_0 \left(e^{\frac{i \times \Delta t_{SNP}}{\tau_{SNP}}} \right) \right] \times \Delta t_{SNP} \right\}$
S_{SPC}	$= \sum_{j=0} \left\{ R_{SPC} \times \left[limit\,_{0}^{D_{max}} D_0 \left(e^{\frac{j \times \Delta t_{SPC}}{\tau_{SPC}}} \right) \right] \times \Delta t_{SPC} \right\}$
S_{Total}	$= S_{SNP} + S_{SPC}$
A_S_{SNP}	$= R_{SNP} \times P_{max}$
A_S_{SPC}	$= R_{SPC} \times D_{max}$
R_{SNP}	$= A\_S_{SNP} \div P_{max}$
R_{SPC}	$= A\_S_{SPC} \div D_{max}$
A_S_{final}	$= CF_{combined} \times NCM\_5$

*5.4.2-1 Estimate on Implementation portion of **CSM-$_{SNP}$** cost savings*

$$CSM_{\text{-}SNP}\text{:}\quad S_{SNP} = \sum\nolimits_{i=0}\left\{R_{SNP} \times \left[limit\,_0^{P_{max}} P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right)\right] \times \Delta t_{SNP}\right\}$$

The implementation portion of *CSM-$_{SNP}$* is the total amount of documentation that have been implemented in the *i*-th time interval: $P_i = P_0\left(e^{\frac{i\times\Delta t_{SNP}}{\tau_{SNP}}}\right)$. The average time interval between the major changes of documentation due to the *SNP* implementation is estimated as: Δt_{SNP} = 0.5yr. The initial amount of documentation to be changed for accounting the start of this saving process is estimated as: P_0 = 10 packages. Once the first set of documents is accepted through the *SNP*, the rate of the acceptance of the following documents will be progressive and accelerative. The next (0.5yr later) amount of documentation is estimated to be increased by 20%: P_1 - P_0 = 12 packages. The time constant for the change of documentations due to the *SNP* implementation can be computed:

$$P_1 = P_0\left(e^{\frac{(i=1)\times\Delta t_{SNP}}{\tau_{SNP}}}\right) \implies 10 + 12 = 10 \times e^{\frac{1\times 0.5}{\tau_{SNP}}} \implies \tau_{SNP} = 0.63415\,yr$$

The maximum amount of documentation to be changed is estimated as: P_{max} = 800 packages. Then, the expression of CSM-$_{SNP}$ can be simplified as:

Saving from SNP: $\quad S_{SNP} = \sum_{i=0}\left\{R_{SNP} \times \left[lim\,_0^{800}\, 10 \times e^{0.7885\times i}\right] \times 0.5\right\}$

where $\frac{i\times\Delta t_{SNP}}{\tau_{SNP}} = \frac{i\times 0.5}{0.63415} = 0.7885 \times i$ and R_{SNP} is to be found in the following section.

The number of time intervals i_{Pmax} needed for the completion of all the documentation changes can be computed as follows: $800 = 10 \times e^{0.7885\times i_{pmax}} \implies i_{pmax} = 5.557 \approx 6\ (next\ integer)$

Therefore the estimated time to complete the change of all documentation is 6 × 0.5 = 3 yr.

*5.4.2-2 Estimate on Installation portion of **CSM-$_{SPC}$** cost savings*

$$CSM_{\text{-}SPC}\text{:}\quad S_{SPC} = \sum\nolimits_{j=0}\left\{R_{SPC} \times \left[limit\,_0^{D_{max}} D_0\left(e^{\frac{j\times\Delta t_{SPC}}{\tau_{SPC}}}\right)\right] \times \Delta t_{SPC}\right\}$$

The implementation portion of *CSM-$_{SPC}$* is the total amount of installations that have been installed in the *j*-th time interval: $D_j = P_0\left(e^{\frac{j\times\Delta t_{SNP}}{\tau_{SNP}}}\right)$. The major installations of new *SPC* smart devices due to the *SNP* implementation most likely occur during the scheduled outage. Therefore the average time interval between the major SPC installations is estimated as: Δt_{SPC} = 2.5yr. The initial number of nuclear devices to be changed for accounting the start of this saving process is estimated as: D_0 = 25 devices. Once the first set of installation is successful, the rate of the installations will be progressive and accelerative. The number of installations in the next outage of 2.5 years later is estimated to increase by 3 times: D_1 - D_0 = 75 devices. The time constant for the change of the amount of *SPC* installations due to the *SNP* implementation can be computed as follows:

$$D_1 \;=\; D_0\left(e^{\frac{(j=1)\times\Delta t_{SPC}}{\tau_{SPC}}}\right) \;\Longrightarrow\; 25+75=25\;\times\;e^{\frac{1\times 2.5}{\tau_{SNP}}} \;\Longrightarrow\; \tau_{SNP}=1.8034\,yr$$

The maximum number of devices to be changed is estimated as: D_{max} = 4000 devices. Then, the expression of *CSM-*$_{SNP}$ can be simplified as:

Saving from SPC: $S_{SPC} = \sum_{j=0}\left\{R_{SNP} \times \left[lim\,{}_0^{4000} 25 \times e^{1.3863\times j}\right] \times\; 2.5\right\}$

where $\frac{j\times\Delta t_{SNP}}{\tau_{SNP}} = \frac{j\times 2.5}{1.8034} = 1.3863 \times j$ and R_{SPC} is to be found in the following section.

The number of time intervals j_{Dmax} needed for the completion of all the installations can be computed as follows: $4000 = 25 \;\times\; e^{1.3863\times i_{Dmax}} \;\Longrightarrow\; j_{Dmax} = 3.661 \;\approx 4\;(next\ integer)$

Therefore the time to complete the change of all documentation is 4 × 2.5 = 10 yr.

5.4.2-3 Estimate the rates of savings in ***CSM-***$_{SNP}$ *and* ***CSM-***$_{SNP}$

The *final* contribution of the *SNP* design for the reduction of the annual maintenance cost per nuclear unit is: *A_S*$_{final}$ = $CF_{combined}$ × *NCM_5*

In addition to increased security and safety benefits to the nuclear operations, the reduction of the annual maintenance cost per unit is expected to be 35%, that is: $CF_{combined}$ = 0.35

A_S$_{final}$ = 0.35 ×\$12.224 = \$4.2784 million/year/unit

Estimate the contributions from the *SNP* implementation and the *SPC* installation are in the ratio of 6:4 as the paper work for nuclear operation is heavy. Therefore, the estimated steady-state annual cost saving from the implementation of the *SNP* designs is:

A_S$_{SNP}$ = 0.6 × 4.2784 = \$2.5670 million/yr/unit

The estimated steady-state annual cost saving from the installation of the *SPC* (provided that the *SNP* designs have already been implemented) is:

A_S_{SPC} = 0.4 × 4.2784 = \$1.7114 million/yr/unit

Estimate the rate of saving in the *Model-*$_{SNP}$ is: $R_{SNP} = A\_S_{SNP} \div P_{max}$

R_{SNP} = \$2.5670million/yr/unit ÷ 800 documents = \$3208.8/document/unit

Estimate the rate of saving in the *Model-*$_{SPC}$ is: $R_{SPC} = A\_S_{SPC} \times \Delta t_{SPC} \div D_{max}$

R_{SNP} = \$1.7114million/yr/unit ÷ 4000 devices = \$427.85/device/unit

5.4.3 Numerical Evaluation of accumulative savings from the SNP and SPC

The following presents an illustrating of the accumulative savings from the *SNP* and *SPC*.

5.4.3-1 Estimate Accumulative Saving from SNP

The model of the accumulative saving from the *SNP* is:

$$\boldsymbol{S_{SNP}} = \sum_{\boldsymbol{i=0}}\left\{\boldsymbol{R_{SNP}} \times \left[\boldsymbol{limit}\,_{\boldsymbol{0}}^{\boldsymbol{P_{max}}}\boldsymbol{P_0}\left(\boldsymbol{e}^{\frac{\boldsymbol{i\times\Delta t_{SNP}}}{\boldsymbol{\tau_{SNP}}}}\right)\right] \times \boldsymbol{\Delta t_{SNP}}\right\}$$

Use the values estimated in section 5.4.2, the model above can be evaluated as follows:

$$\boldsymbol{S_{SNP}} = \sum_{i=0}\left\{3208.8 \times \left[limit\,_{0}^{800}\, 10 \times e^{0.7885\times i}\right] \times 0.5\right\} \qquad \text{where } i_{Pmax} = 5.557$$

$$= \sum_{i=0}^{i=5}\left\{3208.8 \times 10 \times e^{0.7885\times i} \times 0.5\right\} + \sum_{i=6}\{3208.8 \times 800 \times 0.5\}$$

$$= \sum_{i=0}^{i=5}\left\{0.016044 \times e^{0.7885\times i}\right\} + \sum_{i=6} 1.2835 \quad \$M$$

5.4.3-2 Estimate Accumulative Saving from SPC

The model of the accumulative saving from the *SPC* is:

$$\boldsymbol{S_{SPC}} = \sum_{\boldsymbol{j=0}}\left\{\boldsymbol{R_{SPC}} \times \left[\boldsymbol{limit}\,_{\boldsymbol{0}}^{\boldsymbol{D_{max}}}\boldsymbol{D_0}\left(\boldsymbol{e}^{\frac{\boldsymbol{j\times\Delta t_{SPC}}}{\boldsymbol{\tau_{SPC}}}}\right)\right] \times \boldsymbol{\Delta t_{SPC}}\right\}$$

Use the values estimated in section 5.4.2, the model above can be evaluated as follows:

$$\boldsymbol{S_{SPC}} = \sum_{j=0}\left\{427.85 \times \left[limit\,_{0}^{4000}\, 25 \times e^{1.3863\times j}\right] \times 2.5\right\} \qquad \text{where } j_{Dmax} = 3.661$$

$$= \sum_{j=0}^{j=3}\left\{427.85 \times 25 \times e^{1.3863\times j} \times 2.5\right\} + \sum_{j=4}\{427.85 \times 4000 \times 2.5\}$$

$$= \sum_{j=0}^{j=3}\left\{0.026741 \times e^{1.3863\times j}\right\} + \sum_{j=4} 4.2785 \quad \$M$$

5.4.3-3 Estimate Total Accumulative Saving from SNP and SPC

The total amount of the operation saving from the implementations of the *SNP* and *SPC* is the sum of the above-mentioned savings: $\boldsymbol{S_{Total}} = \boldsymbol{S_{SNP}} + \boldsymbol{S_{SPC}}$

$$\boldsymbol{S_{Total}} = \sum_{i=0}^{i=5}\left\{0.016044 \times e^{0.7885\times i}\right\} + \sum_{i=6} 1.2835 + \sum_{j=0}^{j=3}\left\{0.026741 \times e^{1.3863\times j}\right\} + \sum_{j=4} 4.278\ 5\$\mathrm{M}$$

5.4.4 Numerical Analysis of the SNP Designs

This section presents the numerical analysis of the *SNP* designs. The following summarizes the numerical expressions of cost savings for the nuclear analysis.

Accumulative Cost Saving contributed by SNP

$$S_{SNP} = \sum_{i=0}^{i=5}\{0.016044 \times e^{0.7885\times i}\} + \sum_{i=6} 1.2835$$

Accumulative Cost Saving contributed by SPC (*upon availability of SNP*)

$$S_{SPC} = \sum_{j=0}^{j=3}\{0.026741 \times e^{1.3863\times j}\} + \sum_{j=4} 4.2785$$

Total Accumulative Cost Savings

$$S_{Total} = S_{SNP} + S_{SPC}$$

Incremental Cost Saving contributed by SNP

$$\Delta S_{SNP} = \begin{cases} 0.016044 \times e^{0.7885\times i} & 0 \le i \le 5 \\ 1.2835 & 6 \le i \end{cases}$$

Incremental Cost Saving contributed by SPC

$$\Delta S_{SPC} = \begin{cases} 0.026741 \times e^{1.3863\times j} & 0 \le j \le 3 \\ 4.2785 & 4 \le j \end{cases}$$

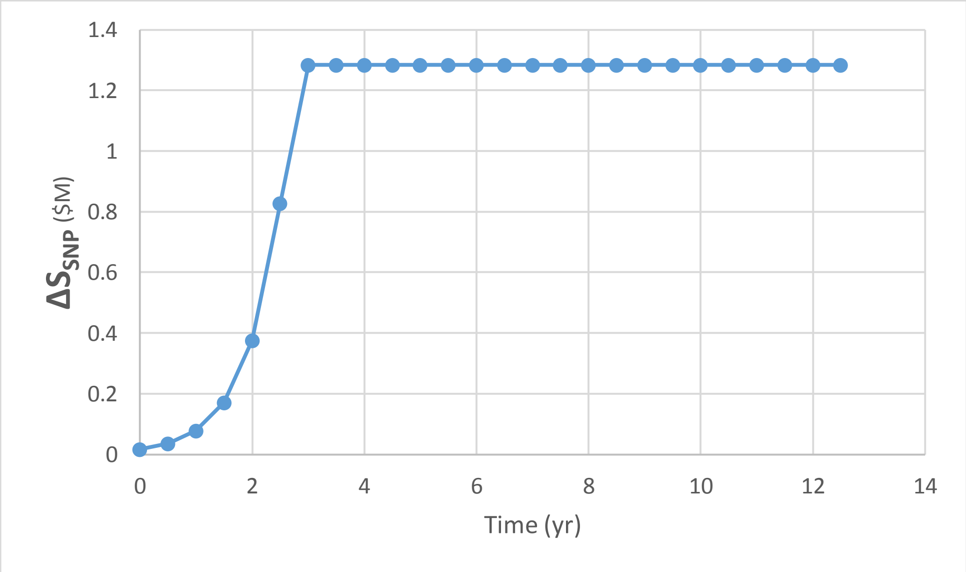
Table 5.5 shows the numerical computations of the cost savings. This table shows the calculated values of ΔS_{SNP}, ΔS_{SNP}, ΔS_{SPC}, S_{SPC}, and S_{Total} with the use of the expressions above.

The plots of these values are given in Graphs 5.1 to 5.5.

Graph 5.1 shows ΔS_{SNP}, the incremental cost saving contributed by the *SNP*. This incremental saving initially increases exponentially until the 6th time interval that is the 3rd year from the start of the use of the SNP designs. Then from the 3rd year, this saving remains no change as all the documentation have been changed, and therefore the incremental saving also remains unchanged.

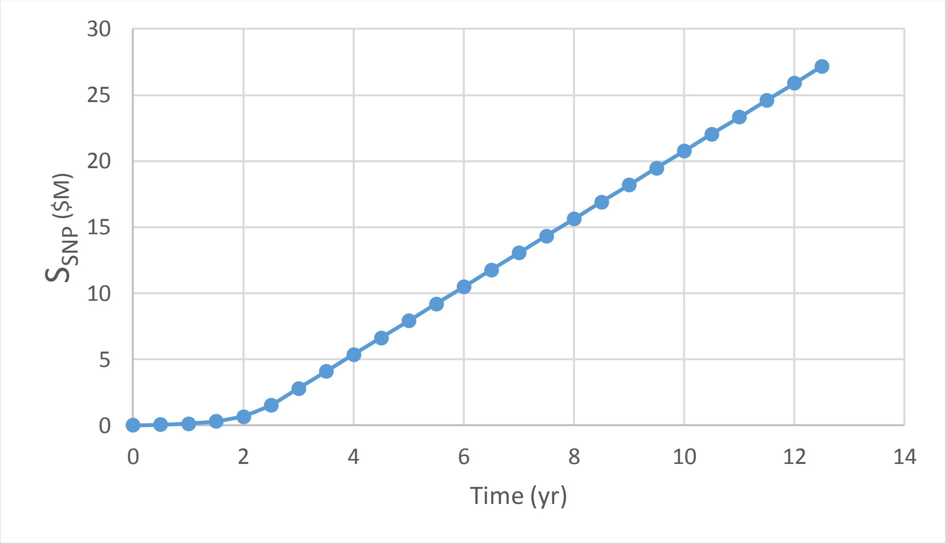
Table 5.5: Numerical evaluation of cost savings

t (yr)	i	ΔS_{SNP}	S_{SNP}	j	ΔS_{SPC}	S_{SPC}	S_{Total}
0	0	0.016044	0.016044	0	0.026741	0.026741	0.042785
0.5	1	0.035298	0.051342			0.0320892	0.0834312
1.0	2	0.07766	0.129002			0.0374374	0.1664394
1.5	3	0.17086	0.299862			0.0427856	0.3426476
2.0	4	0.3759	0.675762			0.0481338	0.7238958
2.5	5	0.82703	1.502792	1	0.10696	0.133701	1.636493
3.0	6	1.2835	2.786292			0.155093	2.941385
3.5	7	1.2835	4.069792			0.176485	4.246277
4.0	8	1.2835	5.353292			0.197877	5.551169
4.5	9	1.2835	6.636792			0.219269	6.856061
5.0	10	1.2835	7.920292	2	0.42786	0.561561	8.481853
5.5	11	1.2835	9.203792			0.647133	9.850925
6.0	12	1.2835	10.48729			0.732705	11.219997
6.5	13	1.2835	11.77079			0.818277	12.589069
7.0	14	1.2835	13.05429			0.903849	13.958141
7.5	15	1.2835	14.33779	3	1.7115	2.273061	16.610853
8.0	16	1.2835	15.62129			2.615361	18.236653
8.5	17	1.2835	16.90479			2.957661	19.862453
9.0	18	1.2835	18.18829			3.299961	21.488253
9.5	19	1.2835	19.47179			3.642261	23.114053
10.0	20	1.2835	20.75529	4	4.2785	6.551561	27.306853
10.5	21	1.2835	22.03879			7.407261	29.446053
11.0	22	1.2835	23.32229			8.262961	31.585253
11.5	23	1.2835	24.60579			9.118661	33.724453
12.0	24	1.2835	25.88929			9.974361	35.863653
12.5	25	1.2835	27.17279	5	4.2785	10.830061	38.002853



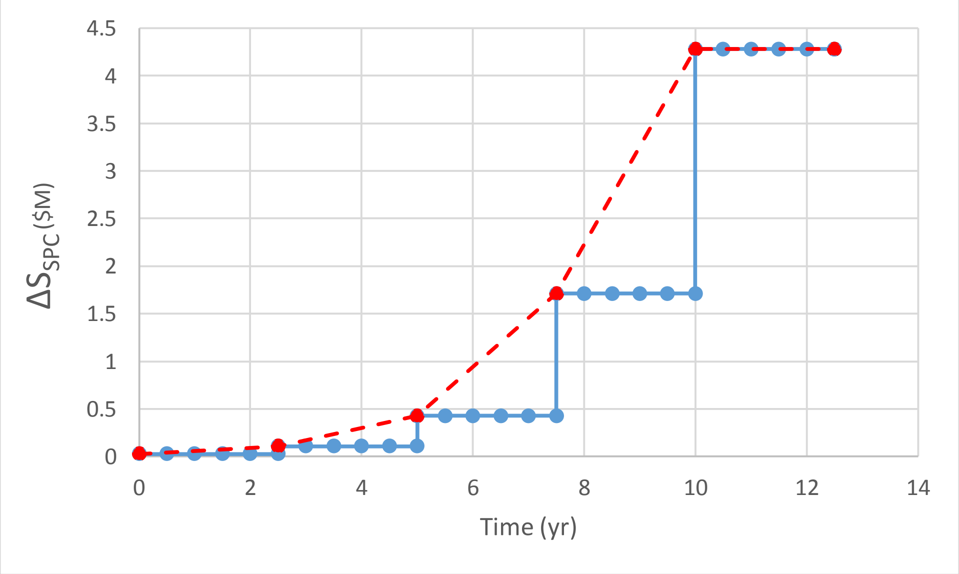
Graph 5.1: Incremental cost saving contributed by SNP

Graph 5.2 shows S_{SNP}, the accumulative cost saving contributed by SNP. It shows the accumulative saving initially increases exponentially until the 3rd year, and then this saving increases linearly.



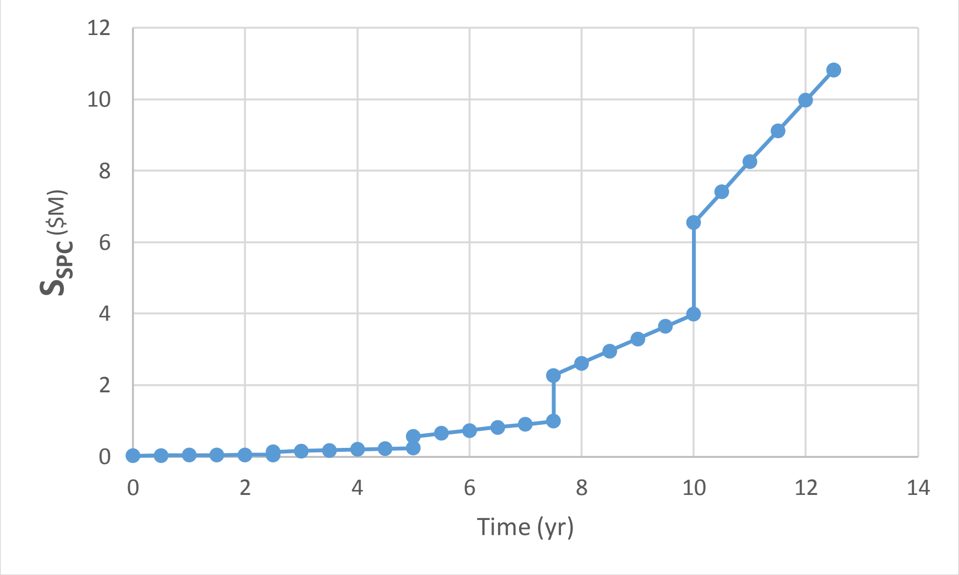
Graph 5.2: Accumulative cost saving contributed by SNP

Graph 5.3 shows ΔS_{SPC}, the incremental cost saving contributed by the SPC. This incremental saving initially increases exponentially until the 4th time interval that is the 10th year from the start of the use of the SPC devices, as shown in the red-dotted line (the blue line shows the actual increments that is stepwise as the scheduled outages occur on an average of 2.5 years). Then from the 10th year, this saving remains no change as all the documentations have been changed, and therefore the incremental saving also remains unchanged.



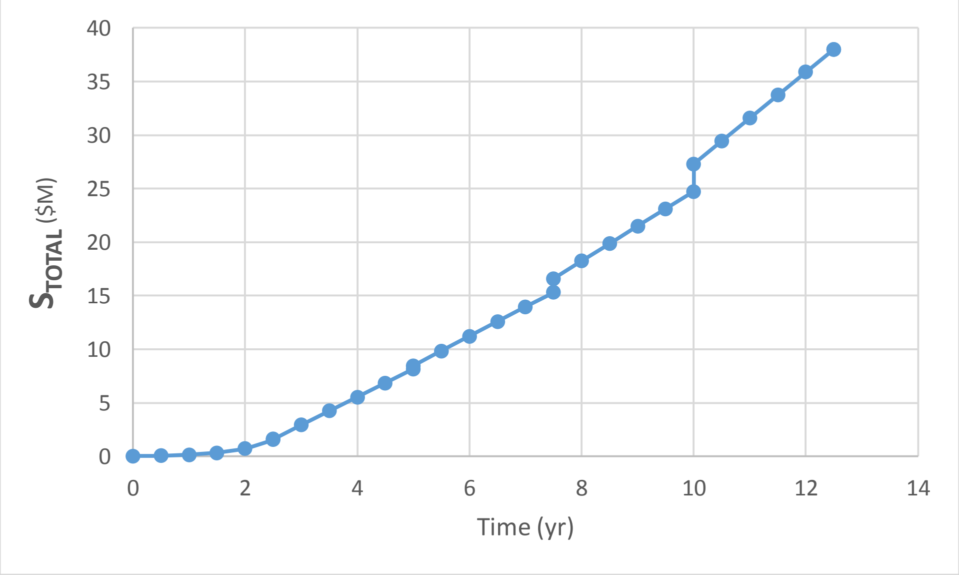
Graph 5.3: Incremental cost saving contributed by SPC

Graph 5.4 shows S_{SPC}, the accumulative cost saving contributed by *SPC*. It can be seen from this graph that the accumulative saving initially increases exponentially until the 10th year, and then this saving increases linearly.



Graph 5.4: Accumulative cost saving contributed by SPC

Graph 5.5 shows $\boldsymbol{S_{Total}}$, the total accumulative cost saving contributed from both the *SNP* and the *SPC*. This accumulative saving also has the general characteristic of the above graphs with an exponential increase initially and with linear increase afterwards.



Graph 5.5: Total accumulative cost savings

5.5 NOAA Design Performance Analysis

This section presents the analysis of the *Nuclear Operation Access Authentication*, ***NOAA*** and its *Authentication Pre-access Protocol*, ***APP***. The analysis includes numerical evaluation and simulation assessment.

5.5.1 Authentication for SNP network access

The new ***NOAA*** access authentication system and its ***APP*** pre-access protocol designed in this thesis for access to the *SNP* network is to minimize the latency of the authentication protocol, specifically to minimize the burden of message exchanges between the user and the verifier and key operations by the user and the verifier while achieving high resilient to all kinds of possible attacks. Figure 5.1 illustrates the access of a *nuclear worker-x* to the *SNP* network.

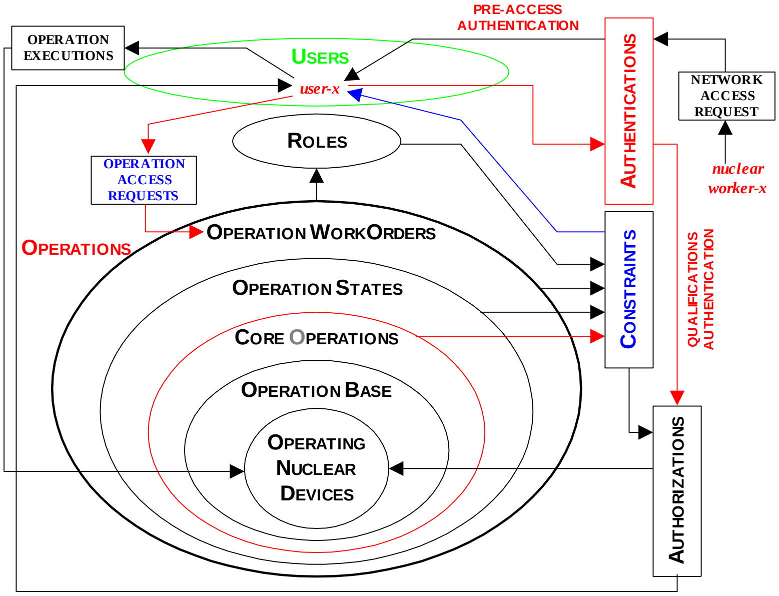


Figure 5.1: *nuclear worker-x* and *user-x* access to *SNP* network

The following shows the 5-*step* ***APP***, authentication pre-access protocol design that offers a simple and high efficient authentication for a *nuclear worker-x* for access to the *SNP* network.

Step-1: The *nuclear worker-x*, W_x sends its certificate ($Cert\text{-}_{W-x}$) that contains W_x's public key (PK_{Wx}), certificate identity, expire date, etc. (ID_{Wx}), and optional text ($Text_{Wx}$) to the verifier *V*:

Message$_{Wx-1}$: **$Cert\text{-}_{W-x}$ (ID_{Wx}, PK_{Wx}, $Text_{Wx}$)**

Step-2: *V* verifies the digital signature of $Cert\text{-}_{W-x}$ using the Station Certificate Authority's public key;

V generates two nonces N_{Vx1} and N_{Vx2}, if $Cert\text{-}_{W\text{-}x}$ is verified;

V encrypts the two nonces using W_x's public key PK_{Wx}, and sends the encrypted values to W_x:

Message$_{\text{Vx-1}}$: $\boldsymbol{E_{PKWx}\{N_{Vx1} \| N_{Vx2}\}}$

Step-3: W_x decrypts Message$_{\text{V-1}}$ to obtain N_{Vx1} and N_{Vx2} using W's private key;

W_x generates two nonces N_{Wx1} and N_{Wx2};

W_x encrypts the nonces using V's public key PK_V, and sends the encrypted values to V:

Message$_{\text{Wx-2}}$: $\boldsymbol{E_{PKV}\{N_{Wx1} \| N_{Wx2} \| N_{Vx2}\}}$

Step-4: V decrypts Message$_{\text{W-2}}$ to obtain N_{Wx1}, N_{Wx2} and N_{Vx2} using V's private key;

V sends N_{Wx2} to W_x for declaring "*W_x is authenticated by V*", if N_{Vx2} is the correct one that was sent by V in *Step-2*.

Message$_{\text{Vx-2}}$: $\boldsymbol{N_{Wx2}}$

Step-5: W_x sends N_{Vx2} to V for declaring "*V is authenticated by W_x*"

Message$_{\text{Wx-3}}$: $\boldsymbol{N_{Vx2}}$

This is the first and most important defense for the security of the nuclear process network and subsequently the safety of the nuclear operations. This 5-step *APP* can be illustrated with Figure 5.2.

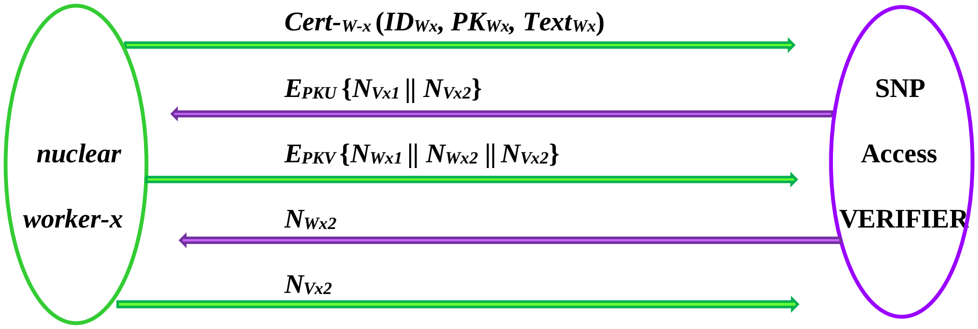


Figure 5.2: Pre-access authentication for *nuclear worker-x*

5.5.2 APP Design Performance Analysis

This section presents the *NOAA-APP* design analysis. The basic prerequisite for a nuclear process network operation is to ensure secure, reliable, and efficient data delivery. In the development of network protocols, the latency consideration is more important than the throughput consideration. The performance of the APP protocol design is compared to the existing protocol using both numerical evaluation and simulation assessment. The Transport Layer Security (TLS) is a representative authentication protocol used for electrical power systems as recommended by IEC61850. The following presents a comparison of the APP versus the TLS by means of numerical analysis and commercial software simulations.

5.5.2-1 Numerical Evaluation of APP versus TLS

The performance of the protocols can be measured in terms of:

- communication costs, which indicate the number of messages exchanged between a authentication server and a user to complete in an authentication session;
- computation costs, which are the latency (in milliseconds) incurred by the security operations, such as encryption using public key (Epub), decryption using public key (Dpub), generation of a digital signature (Gsig), verification of a digital signature (Vsig) and hashing (Hash).

Table 5.6 lists the above security operations (Epub, Dpub, Gsig, Vsig, Hash), the current state-of-the-art algorithms implementing these operations, and the computation time each of these algorithms incurs (the first, second and third columns, respectively) [18]. The fourth and fifth columns of Table 5.6 list the numbers of security operations that the APP and the TLS perform, respectively. By multiplying the computation cost of each operation (from the third column) and the number of times it is executed, and summing up the costs of all operations executed by a protocol, the total computation cost is obtained as shown in the third last row of Table 5.6. The computation cost of the APP is less than that of the TLS [Appendix I].

Table 5.6: Computation and communication costs

Operations	**Algorithms**	**Time (ms)**	**APP**	**TLS**
Epub	RSA[19]	1.42	2	1
Dpub	RSA	33.3	2	1
Gsig	ECDSA[20]	11.6	0	1
Vsig	ECDSA	17.2	1	3
Hash	SHA-2[21]	0.009	0	4
Total computation cost(ms)			86.6	97.9
Number of messages			5	5
Authentication latency (ms)			86.6 + 5*d*	97.7+5*d*

The second last row of Table 5.6 lists the number of messages exchanged in each protocol. The authentication latencies shown in the last row are the sums of computation costs and communication delays, where d is the average delay of a one transmission incurred by a message. The delay of the APP is 86.6+5d ms versus 97.7+5d ms for the TLS. The gain for the APP over the TLS is due to a reduction of public key operations of the APP.

5.5.2-2 Simulation Assessment of APP versus TLS

The protocol performance metric is the authentication delay (latency), which is measured as the time between a user's transmission of an authentication request to an authentication server and the receipt of an acceptance confirmation. A commercial software QualNet, version 5.2 [22], is employed for the simulation. Two sets of tests are conducted to measure the authentication latency, as a function of:

a) Number of users - measure average authentication latency of the APP and the TLS and measure the average latency by varying the group size from 10 to 60. The simulation results are to be presented in graphs. For each data point in a graph, run the simulation 10 times using 10 different random seeds and obtain the average rekeying latency. The maximum authentication delay and the maximum value among all users are recorded.

b) Background traffic load - measure the average authentication latency of the APP and the TLS in the presence of the background traffic.

Four cases of simulation tests are carried out:

Case 1: Measure the average authentication latency of the APP and the TLS as a function of the number of users in one network, *Net-1*. This network has one node as the authentication server (AS) placed in the center of the network. The number of users varies from 10 to 60.

Case 2: Measure the maximum authentication latency of the APP and the TLS as a function of the users, using the network, *Net-1*.

Case 3: Measure the average authentication latency of the protocols in the presence of the background traffic in another network, *Net-2*. This network has one node as the AS placed in the center of the network. Another node is added as a source to transmit the background traffic of the file transfer protocol (FTP) to the AS. This node is not counted as a user. The number of users is selected to be 60. The data rate of the FTP varies from 0 to 50Mbits per second selected for the simulations.

Case 4: Measure the maximum authentication latency of the APP and the TLS as a function of the background traffic, using the network, *Net-2*.

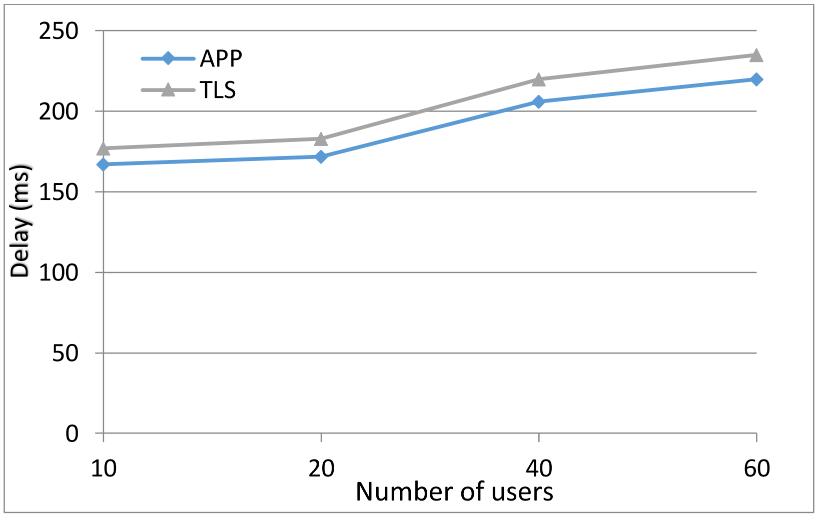
Table 5.7 summarizes the conditions of the simulation test cases. In all the test cases, the user nodes are randomly distributed in the networks. In order to test the scalability of the protocols, all the users present in the network send authentication requests to the AS simultaneously.

Table 5.7: Simulation parameters for 4 test cases

Test Cases	Network	Configuration	Users	Background	Results
Case 1	Net-1	one AS	10-60	0	Graph 5.6
Case 2	Net-1	one AS	10-60	0	Graph 5.7
Case 3	Net-2	one AS, one FTP	60	0-50MBits/s	Graph 5.8
Case 4	Net-2	one AS, one FTP	60	0-50MBits/s	Graph 5.9

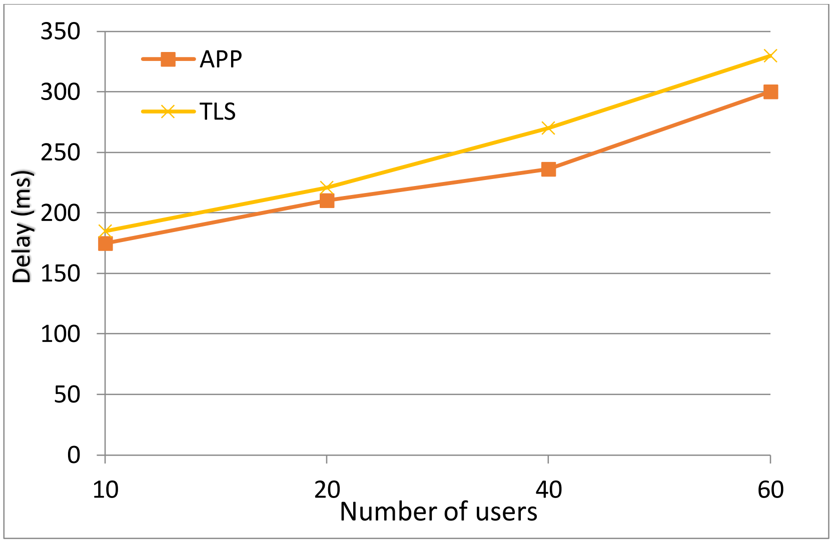
Simulation results of the 4 test cases are given in Graphs 5.6 to 5.9 below:

Graph 5.6 shows the average authentication latency of the APP versus the TLS as the function of the number of users. When there are only 10 users in the network, the average latency of the APP and the TLS are 167.6ms and 177.2ms, respectively. For more than 10 users, the workload and the channel contention at the server increases more. In these cases, the APP offers lower average latency than that of the TLS, because the APP requires less message exchanges than that of TLS that is 5 versus 10 as shown in the second last row of Table 5.6. As the number of the users increases, the average authentication latency of both the APP and the TLS increases. In the case of 60 users, the average authentication latency of the APP and the TLS are 220.1ms and 235.5ms, respectively. The average authentication latency of the APP is 6.3% lower than that of the TLS.



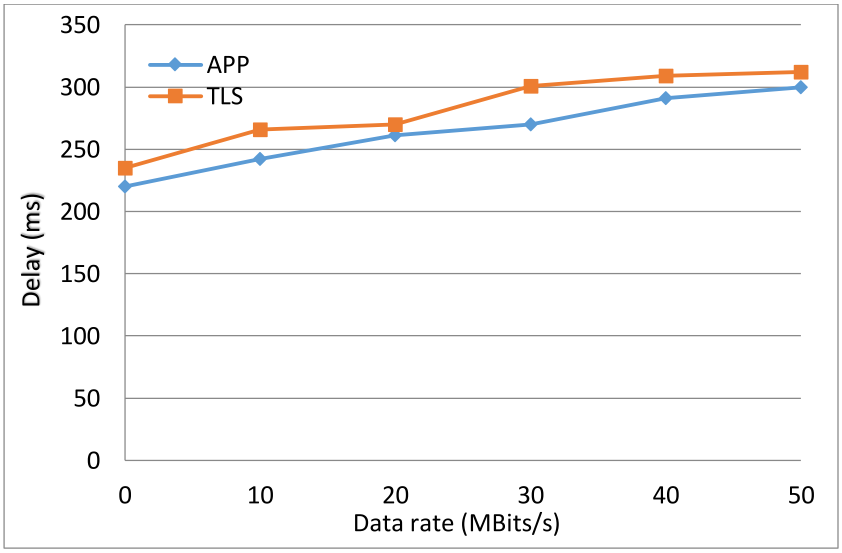
Graph 5.6: Average latency of APP via TLS - function of number of users

Graph 5.7 shows that the maximum authentication latency of both the APP and the TLS. Given that 60 users request authentication with the same AS, the maximum latency of the APP and the TLS are 299.7ms and 331.6ms, respectively. The amounts of cryptographic computation performed by the APP and the TLS are similar that is 86.6ms versus 97.7ms as shown in the last row of Table 5.6. This shows that the gain of the APP over the TLS is mainly due to their difference on the communication costs.



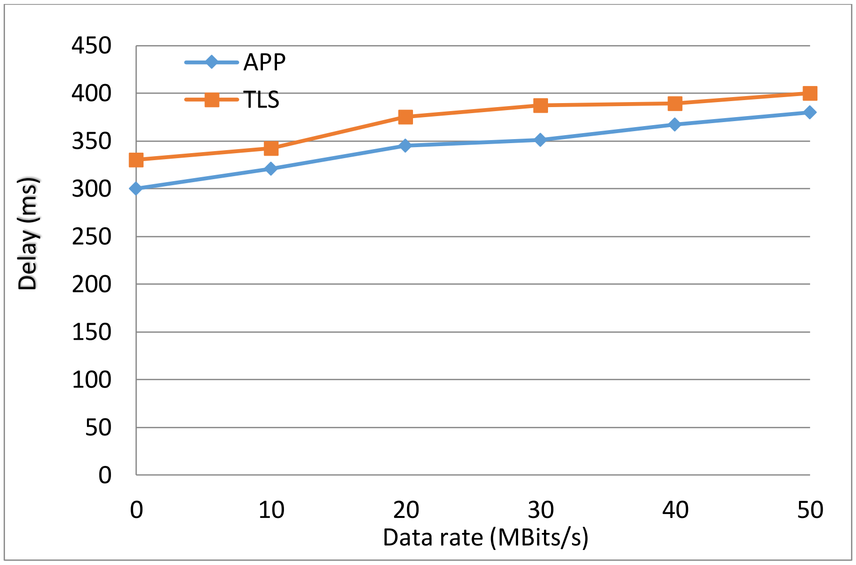
Graph 5.7: Maximum latency of APP via TLS- function of number of users

Test case 3 is to demonstrate how the background traffic may affect the average authentication latency and the maximum authentication latency when 60 users request to be authenticated at the same time. Graph 5.8 shows the average authentication latency as the function of data rate that varies from 10Mbits/s to 50Mbits/s. The data rate of 0 means that there is no background traffic. As the data rate increases, the average authentication latency of users is enlarged. The higher data rate implies more background traffic to be processed by the AS and more channel contention be around the AS, resulting in a longer delay.



Graph 5.8: Average latency of APP via TLS - function of traffic load

Graph 5.9 shows the maximum authentication latency when the number of users is 60. The data rates vary from 10Mbits/s to 50Mbits/s. As the data rate increases, the maximum authentication latency of the APP and the TLS increases. The higher data rate implies more background traffic to be processed by the AS and more channel contention be around the AS, resulting in a longer delay.



Graph 5.9: Maximum latency of APP via TLS - function of traffic load

NOAA Security Resilience: The new design of ***NOAA*** authentication is resilient to cyber-attacks, in particular the forgery attacks and replay attacks, as illustrated below.

NOAA Resilience to Forgery Attacks: The forgery attack is an attack in which an attacker deliberately manipulates data. This type of attacks can be prevented by using digital signatures and message encryption. The public key certificate for the NOAA authentication uses digital signature to prevent forgery attacks. The digital signature ensures that user's certificate is protected against modifications and that counterfeit messages are infeasible to be fabricated. Any unauthorized changes to the content of the certificate will result in an incorrect signature value because the attacker does not know Certificate Authority's private key to forge the user's original certificate. The NOAA authentication use encryption to prevent forgery attacks. The encrypted messages are protected against modifications. Any changes to the content of the messages will result in the messages that are unable be decrypted successfully by the recipient.

NOAA Resilience to Replay Attacks: An attacker records messages of an ongoing authentication session and then replays these messages in the future in an attempt to be successfully authenticated and possibly gain access to the network as the legitimate user. An attacker may replay the user's messages to gain access to the network or replay the verifier's messages to impersonate the verifier. The NOAA prevents the replay attacks by using nonces. A nonce is a random number that is only used for one time [14]. A new message must use newly generated nonces and must not repeat using those that have been sent previously. If a message with nonces was lost or damaged, the message is retransmitted, but the retransmitted message must use newly generated nonces.

Chapter 6

CONCLUSION

This thesis research has been successfully completed, with several contributions to the field of thesis investigations, specifically the creations of ***SNP*** (*Security-integrated Nuclear Process network base*), ***OBAC*** (*Operation Based Access Control*), ***NOAA*** (*Nuclear Operation Access Authentication*), and ***CSM*** (*Cost Savings Models*) as fundamental developments for contributions to nuclear operations modernization, with increased operation security and efficiency, and subsequently nuclear safety, radiation free working environment, and significant cost savings in the daily nuclear operations.

Any research target for a noteworthy change of current nuclear practices would be tremendously challenging but very rewarding for its success. As mentioned in this thesis introduction, it is extremely challenging to be able to dig out any tangible research data including any significant nuclear process deficiencies, issues, events and their causes in the real nuclear generating facilities, because the nuclear industry is substantially "*closed*" due to their conservative ways of handling public safety concerns, particularly with respect to radiation exposures and nuclear events/accidents, in additional to risk potentials inherent with the operating nuclear systems.

Nevertheless, the success for a significant change of current practices is very rewarding as from the design analysis presented in chapter 5, the nuclear operation cost saving could be millions of dollars per nuclear unit per year, in addition with increased nuclear safety to human and environment that is priceless.

The feasibility of the ground-breaking designs of *SNP*, *OBAC*, and *NOAA* for the nuclear application has been illustrated in this thesis. The significance of these new designs has been evaluated using the new cost evaluating functions by comparing the *CSM* contributed by designs of *SNP*, *OBAC*, and *NOAA* with the reference base model *NCM*.

A representative detail for the practical development of the *SNP* network base created in this research, with respect to the real nuclear unit and live operation environment, has been provided in this thesis.

The new *OBAC* design of operation-oriented has overcome the limitations of RBAC (role-based access control) that is the current standard network access control if the RBAC is to be used for the real-time nuclear process control operations. This new *OBAC* design has been illustrated for handling the very complex nuclear operation access controls and the architecture of this design is generic. Therefore, the new

OBAC design not only is suitable for nuclear application but also is certainly applicable for other operation-access control applications.

The new *NOAA* design offers efficient authentication services to protect the security of the nuclear operation network and effectively eliminates the nuclear security concerns, which removes the major roadblock in the progression of nuclear process operations modernization. This new *NOAA* design performs two stages of security checks: the first one is designed for the pre-operation access check to ensure only the authorized personnel is allowed to enter into the nuclear operation network; the second one is for the access qualification check to ensure only the qualified personnel is allowed to execute the nuclear operation. Like the *OBAC*, the protocol for this new *NOAA* design is in a simple and generic form and is applicable for other operation-access control applications in addition for the nuclear use primarily focused in this thesis.

This thesis research creates *CSM*, the *cost saving models* and *NCM*, the *nuclear cost models*. These nuclear-related cost saving models are the first of the kind and simple to use. These models are to be useful for economic assessment of future practical researches in the nuclear area as well as for generating numerical data for support of future theoretical researches regarding their potential real-world realization in the economic aspect.

This chapter presents a summary of the completed major research work, major research contributions, and future work recommendations.

6.1 Major Research Work Completed

The following presents a summary of major tasks accomplished in this thesis research.

1) All the targets set forth along with this thesis research have been completed. Specifically, this thesis' new designs of *SNP*, *OBAC*, and *NOAA* (*APP* + *AQP*) possess the following targeted features:
    - A novel concept and implementable method for effective eliminating the security concerns for access to nuclear process in the nuclear operations modernization
    - A new effective methodology of secure deployment of modern smart equipment for nuclear process upgrades; a revolutionary-type of changes for the nuclear generating practices to significantly reduce the current human-intensive maintenance and operation practices in the existing nuclear plants, with the use of today's available intelligent (smart) technologies
    - A practical innovative access control to new smart nuclear processers with networking capability for online diagnosis and online adjustments, in order to shorten the outage requirements that directly render to tremendous savings;
    - An innovative security-integrated system for nuclear process controls that facilities the functioning of state-of-the-art intelligent features of modern process controlling equipment with networking capability for central data processing, operations optimizing and coordinating, and predictive maintenance scheduling
    - A new security-integrated nuclear practice that can significantly benefit the nuclear industry as well as can be accepted by this "closed" industry

2) As the existing network access controls are not particularly suitable for the real-time nuclear operations, the development of a new design is needed. The new *OBAC* design for security control of access to nuclear operation has been developed.

3) The illustration of the new *OBAC* design for the nuclear operation execution access controls has been completed. The *OBAC* design has been illustrated for the mappings of the equipment monitoring, data processing, and maintenance work orders to the standard nuclear operations, the mappings of the nuclear operations to the experience requirements represented by the official nuclear roles and users' positions, and the mappings of the nuclear operations to the technical requirements represented by the nuclear trainings. Also the *OBAC* design for mapping of nuclear operation observations or view supervisions to the standard nuclear operations has been illustrated.

4) As the major gridlock in the progress of nuclear operation modernization has been the security concerns of using smart equipment with networking capability for central data processing, operations optimizing and coordinating, predictive maintenance scheduling, etc., the development of a suitable secure measure to protect the nuclear operation is needed. The new *NOAA* design has been developed for this need.

5) This new *NOAA* design performs two stages of security checks: the first one is designed for pre-operation access check to ensure only the authorized personnel is allowed to enter into the nuclear operation network; the second one is qualification check to ensure only the qualified personnel can execute the nuclear operation. The illustration of the *NOAA* design checks has been provided.

6) As of today, a secure nuclear network base has not been available. Therefore the intelligent features of modern process control equipment/systems cannot be utilized in the efficient and secure way, and a secure and practical nuclear network base is needed. The *SNP* network base is designed for this need.

7) The implementable of the ground-breaking design of *SNP* has been illustrated in this thesis. A representative detail for the practical development of the *SNP* network base created in this research, with respect to the real nuclear unit and live operation environment, has been provided in this thesis.

8) Without a measure for comparison, the significance and feasibility of the ground-breaking designs of *SNP*, *OBAC*, and *NOAA* for the nuclear application is not easy to be recognized, and such a measure has not been available. Therefore, this thesis research has developed *NCM*, the *nuclear cost models* for the current nuclear practices and *CSM*, the *cost saving models* for the contributions from the new designs developed in this thesis research.

6.2 Major Research Contributions

The following lists the major contributions from this thesis research.

Creation of SNP: The creation of the new *SNP network base* is to facilitate the use of the intelligent features of state-of-the-art smart equipment with networking capability for central data processing, operations optimizing and coordinating, predictive maintenance scheduling, etc. for nuclear operation modernization. This is ground-breaking design and the first of the kind in the nuclear environment for a full transformation of traditional nuclear practices to a modern network-based nuclear practices.

Creation of Network Base: This thesis research creates the nuclear operation network base that include core operations base, technical qualification base, field qualification base, and role qualification base.

New design of OBAC: The new *OBAC* design has been illustrated for its effective control of access for carrying out the nuclear equipment operations and maintenance work orders as well as nuclear system performance supervisions. The architecture of this *OBAC* is operation-oriented/centered and it can overcome the limitation of RBAC the standard network access control for the real-time process control operations. This new *OBAC* design has been illustrated for handling the very complex nuclear operation access control and the architecture of this design is generic. Therefore, the new *OBAC* design is not only suitable for nuclear application but also certainly applicable for other applications.

New design of NOAA: The design of nuclear process access authentication must be, for real-time nuclear operations that are critical due to nuclear safety, high efficient and resilient to attacks. The design objective for nuclear access authentication is to minimize the latency of the authentication protocol, specifically to minimize the burden of message exchanges between the user and the verifier and key operations by the user and the verifier while achieving high resilient to all kinds of possible attacks. The new *NOAA* has fulfilled this design objective.

New design of APP & AQP: This new *NOAA* design performs two stages of security checks: the first one with the use of the new *APP* protocol is designed for pre-operation access check to ensure only the authorized personnel is allowed to enter into the nuclear operation network; the second one with the use of the new *AQP* protocol is qualification check to ensure only the qualified personnel can execute the nuclear operations.

Creation of CSM and NCM: This thesis research creates *CSM*, the *cost saving models* and *NCM*, the *nuclear cost models*. These nuclear-related cost saving models are the first of the kind and simple to use, as well as has not been found available elsewhere. These models are to be useful for economic assessment of future practical researches in the nuclear area as well as for generating numerical data for support of future theoretical researches regarding their potential real-world realization in the economic aspect.

6.3 Future Work

The focus of this thesis research is on the nuclear area. To carry research in the nuclear environment, two aspects are recommended:

On the planning and preparation aspect, it is recommended to prepare a very long term research plan, with sufficient resources, patience, good planning, and absolutely careful decision with well-calculated data or repeatedly assessments for making any actions in the nuclear plant, because it will take a fairly long time and very detailed proof for a change in the nuclear plan. In particular, the research in this thesis calls for a significant fundamental change. An action with any minor insufficient preparation/data may be thrown away, the action or work plan may be terminated, and the researcher may lose all the opportunity to conduct research in the nuclear plant.

On the technical aspect, the research laid out in this thesis is worthwhile to continue because the research findings in this thesis are very promising, the rewarding for success is tremendous in terms of financial and contributions to nuclear safety.

Specific Recommended Research Directions

- *Research for precise nuclear costs-evaluation models*:

  CSM and *NCM* are first-of-the-kind cost models developed in this thesis for economic assessments of transformation of current nuclear practices. It is recommended to further develop nuclear economic assessment models with increased accuracy if preferably based on statistical collections of actual nuclear operations' economic data, as pre-, during, and post-implementations of the nuclear practices transformations.

- *Extend secure accesses from networks external to the nuclear site*:

  OBAC and *NOAA* are the new access control and authentication developed in this thesis for nuclear operation network secure access controls, primarily designed for the local networks within the nuclear site/station. It is recommended to extend the secure accesses from network external to the nuclear site, but this will significantly increase the network access cyber-security requirements.

- *Develop robust network algorithms for speedy access responses to any nuclear events*:

  SNP is the first-of-the-kind security-integrated nuclear process developed in this thesis for secure network access to nuclear operations, primarily with the focus on network access controls. It is recommended to enhance the access responses in case of any nuclear events.

APPENDIX

TLS AUTHENTICATION PROTOCOL

The TLS Handshake Protocol involves the following steps:

(1) A client sends a ClientHello message specifying the TLS protocol version it supports, a random number C , and a list of suggested cipher suites, such as encryption algorithm, hash function, etc.

(2) The server responds with a ServerHello message, containing the chosen protocol version, a random number S and cipher suite from the choices offered by the client. The server sends its certificate and may request a certificate from the client, so that the connection can be mutually authenticated.

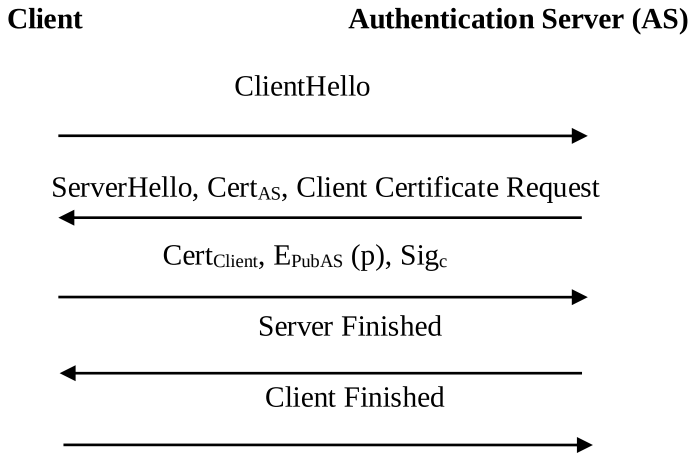
(3) The client responds with a certificate message, which contains the client's certificate. The client sends a random number p, and p is encrypted using the public key of the server certificate.

The client sends a signature over the third message using the client's certificate's private key. This signature can be verified by using the client's public key. This lets the server know that the client has access to the private key of the certificate and thus owns the certificate. Server authenticates the client.

(4) The server now sends a *Finished* message, containing a hash over the server's id and the random numbers used in the previous handshake messages including c, s, and p.

The server will attempt to verify the hash of the server's *Finished* message. If the verification is successful, the client authenticates the AS. If the verification fails, the handshake is considered to have failed and the connection should be torn down.

(5) Finally, the client sends its own *Finished* message containing a hash over the client's id and the random numbers used in the previous handshake messages including c, s, and p. The client performs the same the step (4) to verify it.


Client
Authentication Server (AS)
ClientHello
ServerHello, Cert_{AS}, Client Certificate Request
Cert_{Client}, E_{PubAS} (p), Sig_c
Server Finished
Client Finished

REFERENCES

[1] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, 2013

[2] ANSI INCITS 359-2004, Role Based Access Control, 2004.

[3] Helen Cheung, Celia Li, Ye Yu, Cungang Yang, Privacy Protection for Role-Based Access Control in Service Oriented Architecture, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.

[4] Helen Cheung, Cungang Yang, A Secure Electronic Payment Protocol for Wireless Mesh Networks, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014.

[5] Ravi S. Sandhu, et al., Role-Based Access Control: A Multi-Dimensional View, IEEE publication 1063-9527B, 1994.

[6] 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.

[7] 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.

[8] 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.

[9] Mohammad A. Al-Kahtani, Ravi Sandhu, Rule-Based RBAC with Negative Authorization, Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC’04), 2004.

[10] 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

[11] 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.

[12] 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.

[13] John Bethencourt, Amit Sahai, Brent Waters, Ciphertext-Policy Attribute-Based Encryption, IEEE Symposium on Security and Privacy (SP'07), 2007.

[14] Elisa Bertino, Ravi Sandhu, Database Security - Concepts, Approaches, and Challenges, IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 1, January-March 2005.

[15] Guangsen Zhang, Manish Parashar, Dynamic Context-aware Access Control for Grid Applications, Proceedings of the Fourth International Workshop on Grid Computing (GRID’03), 2003.

[16] Matthew J. Moyer, Mustaque Ahamad, Generalized Role-Based Access Control, IEEE publication, 1063-6927/0, 2001.

[17] 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.

[18] 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

[19] 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.

[20] 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.

[21] Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang, A Formal Virtual Enterprise Access Control Model, IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans, Vol. 38, No. 4, July 2008.

[22] IECStandard,IEC61850:Communication Networks and Systems in Substations.

[23] The Smart Grid Interoperability Panel –Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR7628(2010) 1–597.

[24] Till Mossakowski, Michael Drouineaud, A Temporal-Logic Extension of Role-Based Access Control Covering Dynamic Separation of Duties, Proceedings of the 10th International Symposium on Temporal Representation and Reasoning and Fourth International Conference on Temporal Logic (TIME-ICTL’03), 2003.

[25] http://en.wikipedia.org/wiki/Transport_Layer_Security.

[26] Rafae Bhatti, Rafae Bhatti, Arif Ghafoor, A Trust-based Context-Aware Access Control Model for Web-Services, Proceedings of the IEEE International Conference on Web Services ICWS, 2004

[27] http://en.wikipedia.org/wiki/Kerberos_(protocol).

[28] RSA,"RSA SecurID Two-factor Authentication," 2011, www.rsa.com/products/securid/ sb/10695_SIDTFA_SB_0210.pdf.

[29] D. Forsberg, Y.Ohba, B.Patil, H.Tschofenig, "Protocol for Carrying Authentication and Network Access(PANA)," RFC5191, 2008.

[30] Y.Jiang, C.Lin, X.Shen and M.Shi, "Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks," IEEE Transactionon Wireless Communications, 2006.

[31] IEEE, "Part11:Wireless Medium Access Control (MAC) and Physical Layer specifcations: Medium Access Control (MAC) Security Enhancement," IEEE Standard 802.11i, 2003.

[32] M. Fouda, Z. Md. Fadlullah, N. Kato, R. Lu, and X. Shen, "Towards a light-weight message authentication mechanism tailored for smart grid communications," in *Proc. IEEE INFOCOM'11-SCNC*, Shanghai, China, Apr. 2011.

[33] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, ''An Efficient Merkle Tree Based Authentication Scheme for Smart Grid,'' IEEE Syst. J., DOI: 10.1109/JSYST.2013.2271537.

[34] http://en.wikipedia.org/wiki/Cryptographic_nonce

[35] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[36] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information System, March 2006.

[37] NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.

[38] NIST SP 800-28, Guidelines on Active Content and Mobile Code, October 2001.

[39] NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002.

[40] NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.

[41] NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems, May 2004.

[42] NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, Aug 2002.

[43] NIST SP 800-53 Revision 1, Recommended Security Controls for Federal Information Systems, July 2006.

[44] NIST SP 800-61, Computer Security Incident Handling Guide, January 2004.

[45] ISA SP99 Glossary.

[46] AGA 12, Cryptographic Protection of SCADA Communications.

[47] API 1164, Pipeline SCADA Security, Second Edition.

[48] ISO/IEC 7498: Information processing systems – Open System Interconnection – Basic reference Model, Part 2: Security Architecture.

[49] IEC/PAS 62409, Real-time Ethernet for Plant Automation, ed 1.0, (2005-06).

[50] IEC/PAS 62410, Real-time Ethernet SERCOS III, ed. 1.0 (2005-08).

[51] The Automation, Systems, and Instrumentation Dictionary, 4th Edition, ISA, 2003.

[52] ANSI/ISA-5.1-2009, Instrumentation Symbols and Identification.

[53] ANSI/ISA-51.1-1979 - (R1993) - Process Instrumentation Terminology.

[54] ANSI/ISA-75.05.01-2000, Control Valve Terminology.

[55] ANSI/ISA-84.00.01, 2004.

[56] ANSI/ISA-88.01-1995 - Batch Control Part 1: Models and Terminology.

[57] Bailey, David, and Wright, Edwin, Practical SCADA for Industry, IDC Technologies, 2003.

[58] Boyer, Stuart, SCADA Supervisory Control and Data Acquisition, 2nd Edition, ISA, 1999.

[59] Erickson, Kelvin, and Hedrick, John, Plant Wide Process Control, Wiley & Sons, 1999.

[60] Falco, Joe, et al., IT Security for Industrial Control Systems, NIST IR 6859, 2003, http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf.

[61] Axel Kern, Advanced Features for Enterprise-Wide Role-Based Access Control, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC’ 02), 2002

[62] Eric Yuan, Jin Tong, Attributed Based Access Control (ABAC) for Web Services, Proceedings of the IEEE International Conference on Web Services (ICWS’05), 2005

[63] Tomoya Enokido, Makoto Takizawa, Makoto Takizawa, Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005

[64] www.candu.org/candu_reactors (Internet)

[65] RFC 4949, Internet Security Glossary, Version 2, August 2007, http://www.rfc-editor.org/rfc/rfc4949.txt

[66] National Information Assurance (IA) Glossary, CNSS Instruction no. 4009, revised June 2006

[67] Eric Freudenthal, Tracy Pesin, Lawrence Port, dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments, Proceedings of the 22 nd International Conference on Distributed Computing Systems (ICDCS’02), 2002

[68] Mohammad A. Al-Kahtani, Ravi Sandhu, A Model for Attribute-Based User-Role Assignment, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC.02), 2002

[69] Roosdiana Wonohoesodo, Zahir Tari, A Role based Access Control for Web Services, Proceedings of the 2004 IEEE International Conference on Services Computing (SCC’04), 2004

[70] Fujun Feng, et al., A Trust and Context Based Access Control Model for Distributed Systems, A Trust and Context Based Access Control Model for Distributed Systems, The 10th IEEE International Conference on High Performance Computing and Communications, 2008