RISK-INFORMED NUCLEAR SAFEGUARDS OF PYROPROCESSING FOR ADVANCED NUCLEAR FUEL CONCEPTS

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Nuclear Engineering

in the

College of Graduate Studies

University of Idaho

by

Jieun Lee

Major Professor: Robert Borrelli, Ph.D.

Committee Members: Michael Haney, Ph.D.; Leslie Kerby, Ph.D.

Department Administrator: Richard Christensen, Ph.D.

August 2018

Authorization to Submit Thesis

This thesis of Jieun Lee, submitted for the degree of Master of Science with a Major in Nuclear Engineering and titled "RISK-INFORMED NUCLEAR SAFEGUARDS OF PYROPROCESSING FOR ADVANCED NUCLEAR FUEL CONCEPTS," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____Date_____
Robert Borrelli, Ph.D.

Committee Members: _____Date_____
Michael Haney, Ph.D.

_____Date_____
Leslie Kerby, Ph.D.

Department Administrator: _____Date_____
Richard Christensen, Ph.D.

Abstract

The thesis contains one published paper and two journal papers under review. Chapter 1 introduces the high reliability safeguards approach to remotely handled nuclear processing facilities, particularly for a commercial-scale pyroprocessing facility. This safeguardability model was developed from a design-driven perspective, for fuel fabrication first. It uses a discrete event simulation modeling framework. Quantification of risk within the context of safeguards-by-design with the metric of false alarm probability is a unique feature. Chapter 2 discusses upgrades on the current safeguards model, including the sensitivity analysis performed by varying multiple facility input parameters and the advanced nuclear accounting methodologies. Chapter 3 proposes the hazard and operability analysis of a pyroprocessing facility. The first study identified hazards, operability issues, and severe accident scenarios. It also mitigated their consequences with the corresponding protection methods. In addition, nuclear material accounting locations were determined to optimize facility designs for safeguardability. The detailed summaries of papers are shown in sub-abstracts in the following three chapters.

Acknowledgements

I sincerely thank to Dr. R.A. Borrelli, an assistant professor of Nuclear Engineering at the University of Idaho, for the guidance and encouragement to pursue this project. I greatly appreciate his prompt response to my requests for technical expertise, particularly on the concept of safeguardability.

I would like to express my thanks to other committees, Dr. Leslie Kerby and Dr. Michael Haney, a research assistant professor of Nuclear Engineering at the Idaho State University and an assistant professor of Computer Science at the University of Idaho respectively, for help on the code development and reviewing my thesis paper.

I also thank Dr. Yoon Il Chang, an Argonne distinguished fellow, Dr. Supathorn Phongikaroon, an associate professor of Mechanical and Nuclear Engineering at the Virginia Commonwealth University, and Michael Shaltry for providing technical expertise on the pyroprocessing technologies.

Special thanks to Dr. Steve Skutnik, a professor of Nuclear Engineering at the University of Tennessee, and Dr. Katy Huff, an assistant professor of Nuclear, Plasma, and Radiological Engineering at the University of Illinois, for constructive conversation and advice on developing my research.

Table of Contents

List of Figures

List of Tables

Chapter 1: High Reliability Safeguards Approach to Remotely Handled Nuclear Processing Facilities: Use of Discrete Event Simulation for Material Throughput in Fuel Fabrication

"High Reliability Safeguards Approach to Remotely Handled Nuclear Processing Facilities: Use of Discrete Event Simulation for Material Throughput in Fuel Fabrication." *Nuclear Engineering and Design* vol. 324, 2017, pp. 54-66.

1.1 Abstract

The future, sustainable use of nuclear energy will require a transition to advanced nuclear energy systems. Some of these systems will utilize remotely handled facilities in which batch-type processing will occur in hot cells. These handling procedures, as well as differences in physical and chemical composition of the special nuclear material, create new challenges to safeguardability. The focus area of the High Reliability Safeguards is the continual development of methodologies and approaches which address the safeguardability of the advanced fuel cycle from a design-driven perspective. There is a need to develop models that can quantitatively assess the safeguardability of proposed facility designs. Herein is presented progress made in regards to a first-build, material throughput model using a discrete event simulation modeling framework for the fuel fabrication system in a pyroprocessing facility. This model takes advantage of the synergy between safeguards, safety, and security when designing a nuclear handling facility. A commercial pyroprocessing facility is used as an example system. The intent of the model is to determine if nuclear materials accounting can potentially serve as a metric for safeguardability in facility designs.

1.2 Introduction

1.2.1 Motivation

Many nations are expanding nuclear power in order to enhance energy security, grow the economy, or address climate change [1], [2]. Ensuring resource sustainability will require a transition to advanced nuclear energy systems (NESs). Nuclear fuel for some

of the advanced NESs will be fabricated in remotely-handled facilities in which batch-type processing will occur in heavily-shielded hot cells. For the advanced NESs, special nuclear material (SNM) is in both different physical and chemical form than that of the contemporary fuel cycle. This gives rise to new challenges in terms of integrating safeguards, safety, and security (3S) with facility design; i.e., safeguardability, or safeguards- and security-by-design [3], [4]. To this end, the High Reliability Safeguards (HRS) focus area is continuing to develop research directions in order to address the safeguardability of advanced fuel cycle concepts from a design-driven perspective [5], [6]. A commercial pyroprocessing facility is used as an example system. The intent is to build a model for material throughput that is flexible in terms of accommodating multiple facility designs, where each can be tested in terms of safeguardability.

Designing a safeguardable model is complex. The use of hot cells to process materials provides passive security, and other security measures from analogous facilities can also be applied to a pyroprocessing facility. For safety, a standard probabilistic risk assessment will be performed and likely required as part of the licensing process. This is discussed briefly at the end of this paper as part of future work. While there are issues with the pyroprocessing facility - perhaps with lack of knowledge in terms of new failure modes and failure frequencies, or how materials might be transferred if there are multiple hot cells - the risk assessment framework is well-known and an established tool for safety analysis. Here, the focus is primarily on safeguards-by-design and how materials accounting can be applied within the context of safeguardability.

Nearly all of the safeguards' knowledge and experience for commercial facilities is largely based on aqueous materials processing facilities. The pyroprocessing facility will not have an accountability tank to determine SNM concentration in the materials, nor can the system be flushed out in order to 'reset' plant inventory. Held-up material then becomes a unique challenge. It must be removed from equipment and accurately accounted for periodically in a way that does not impinge on operational goals.

As part of HRS, a quantitative assessment measure of the safeguardability of proposed designs that will be widely acceptable and based on established principles common to safeguards, safety, and security is needed. Prior HRS-related work focused on functional components of facility design by modeling the spontaneous fission of ^{244}Cm [7], [8], [9]. Results for the dose rate of processed materials in the system fell below the IAEA self-protecting standard. This is a non-negligible physical protection risk for the facility that should be addressed during conceptual design phases, thus highlighting the importance of facility design to safeguardability. Additionally, study

of the hot cell wall design showed that occupational safety can be maintained for the pyroprocessing facility comparable to analogous facilities. Therefore, storage buffers, maintenance, or even personnel areas can be designed near process cells. This can considerably reduce the overall facility footprint if physical space is a design constraint.

1.2.2 Current Work

The overall intent of HRS is to provide a systematic methodology that can integrate proliferation resistance and physical protection measures, equally weighted with safety and physical security, while optimizing practical design approaches and operational goals. The primary operational goal is that the operator will have a target quantity as to the amount of material that would need to be processed over a given time period; e.g., for the Rokkasho reprocessing facility in Japan, it is expected that 800 tons of used fuel would be processed over a year. That is not to imply that a pyroprocessing facility would process the same amount, but that there would be a similar goal.

For a pyroprocessing facility, each subsystem processes batches with different weights for different lengths of time. This will be a challenge to nuclear materials accounting (NMA). Poor accounting could result in numerous false alarms; while resolvable, subsequent time delays will affect operational goals. Additionally, poor accounting could fail to detect an actual diversion event. A discrete event simulation (DES) modeling framework is useful for safeguardability assessment. A discrete event model describes a state space that contains state variables. The occurrence of an 'event' drives the transition of the state variable [10]. The transition occurs in a discrete time interval, and the state space remains unaffected in between occurrences. The state transition is assumed to be instantaneous. Events can be triggered sequentially and can occur asynchronously in the state space. DES lends itself to modeling batch-type processes like pyroprocessing. DES can model materials flow for arrival, storage, processing, and transfer, as well as disrupted equipment and material flow states that result from maintenance or off-normal events of varying frequency.

This paper presents the first build of a facility process model using DES. The purpose is twofold. First, the model is established for bulk flow in the fuel fabrication process based on DES principles. This will serve as the architecture for the eventual, full system model. Second, with this model, the use of the probability of the false alarm anomalies; i.e., the Type I error [11], [12], as a metric for safeguardability assessment is tested. The Type I error is already widely applied as a safeguards measure for nuclear materials

accounting. A Type I error occurs when an analysis of the accounting system indicates that some quantity of nuclear material is missing; i.e., diverted, but in actuality no diversion has occurred. There are not yet any suggested IAEA goals for use of this metric for the advanced fuel cycle. This allows for some latitude in studying how to use it within the context of safeguardability [5], [6].

Initiating events, which can lead to a false alarm, arise from a breach in safeguards, safety, or security. Here, the focus is on equipment failures, which occur during normal operation. If such an event leads to a false alarm, an IAEA inspection and facility mass balance would likely be required to resolve the anomaly, costing time and resources [5]. Therefore, at a high-level, the facility operator would have a strong interest in designing the facility to achieve low false alarm probabilities. Criteria for a safeguardability metric is also discussed in this paper. Use of the Type I error as a metric for safeguardability assessment takes advantage of the synergy between all 3S when designing a nuclear materials handling facility. Therefore, in the larger context, the overall intent is to provide a process model that allows for different conceptual facility designs, where each could exhibit different frequencies for the Type I error, and this can provide a measure of the safeguardability of each design.

1.3 Background

1.3.1 Pyroprocessing Technical Details

Used uranium oxide fuel is treated electrochemically at high temperatures in order to produce a metal fuel alloy. Materials are pyrophoric and must be processed in hot cells with an inert atmosphere. The pyroprocessing flowsheet used to build this model is shown in Figure 1.1. The main subsystems are voloxidation, electroreduction, electrorefining, electrowinning/cadmium distillation, and metal fuel fabrication. Used fuel is first chopped, and cladding is mechanically stripped. Voloxidation then transforms UO_2 pellets to U_3O_8 powder. Subsequently, electroreduction converts the powder to metal in $LiCl$-Li_2O salt at 650^oC, where alkali metal and alkaline earth fission products remain in the salt [13], [14], [15], [16]. Cs, Sr, and all volatile species are removed. Electrorefining extracts uranium metal on a cathode [15], and graphite is typically used. Electrowinning extracts TRU metal on a liquid cadmium cathode [14], [17], [18]. Noble metal fission products remain on the anode. Both processes use $LiCl$-KCl salt at 500 ^oC. Lanthanides remain in the salt.

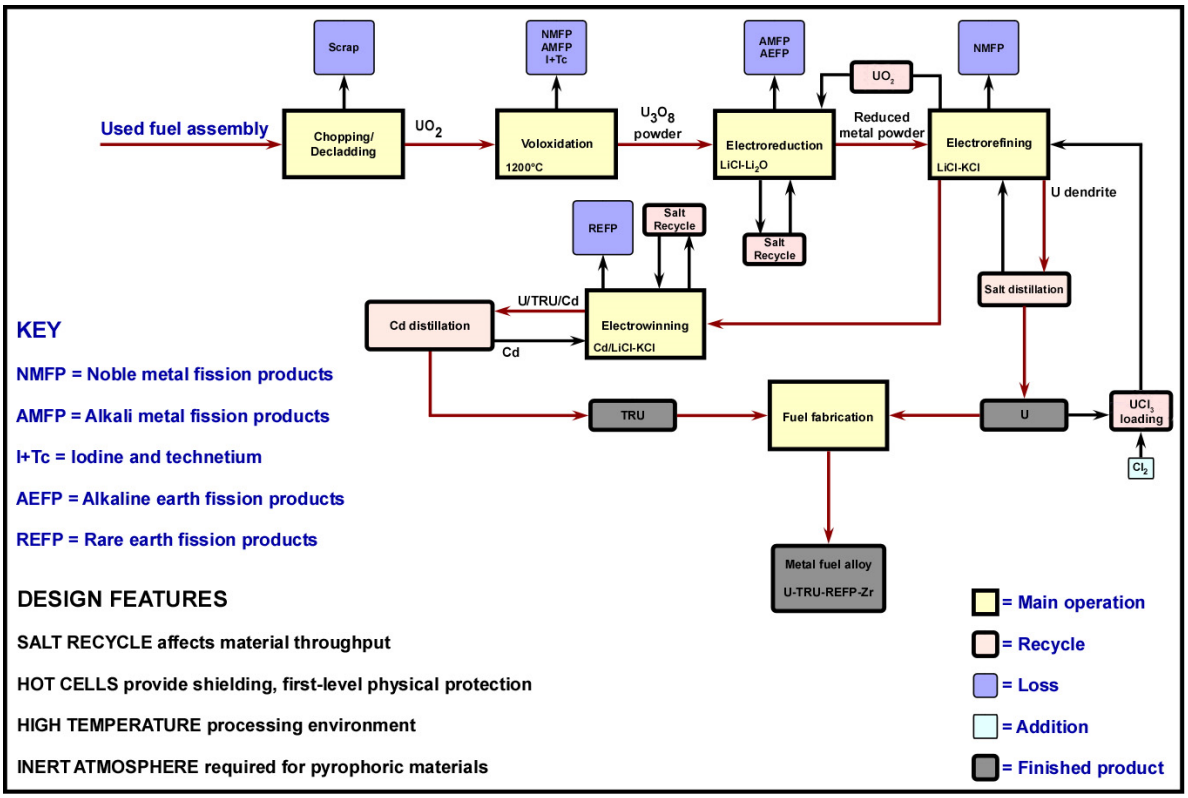

Figure 1.1: Pyroprocessing flowsheet. Pyroprocessing converts used uranium oxide fuel to a metal alloy. The main subsystems in a pyroprocessing facility are voloxidation, electroreduction, electrorefining, electrowinning/cadmium distillation, and metal fuel fabrication, as indicated by the yellow boxes. The primary material flow is shown by the red arrows. Material losses are shown for each subsystem. Treatment and recycle of salts from the electroreduction and electrorefining processes are a major design consideration.

Injection casting is currently assumed for the fuel fabrication process due to cost efficiency, capacity to mass produce metal slugs, and remote operability [19], [20], [21]. It is shown in Fig 1.2. Injection casting was used in the past for the Integral Fast Reactor (IFR) program for EBR-II [22], [23] and is being considered as the fuel fabrication method for some Generation IV systems [21], [24]. However, when scaling up to the commercial level, process losses potentially could be prohibitively high. Materials are first melted in a graphite crucible. Quartz molds are inserted into the molten alloy, and a vacuum is induced. This results in the injection of alloy into the molds. Some of the metal will remain in the crucible. This is called the 'heel' and can be recycled. The molds are removed and sheared. Because they have to be broken to obtain the slugs, they are a waste stream. The crucible will also be a waste stream as it will suffer from eventual wear. Safeguardability in fuel fabrication is important because the

process includes a large amount of SNM, approximately 4 kg of transuranic elements, half of which is ^{239}Pu [7]. A full technical discussion and literature review for the pyroprocessing system applied in this study is contained in Borrelli [5].

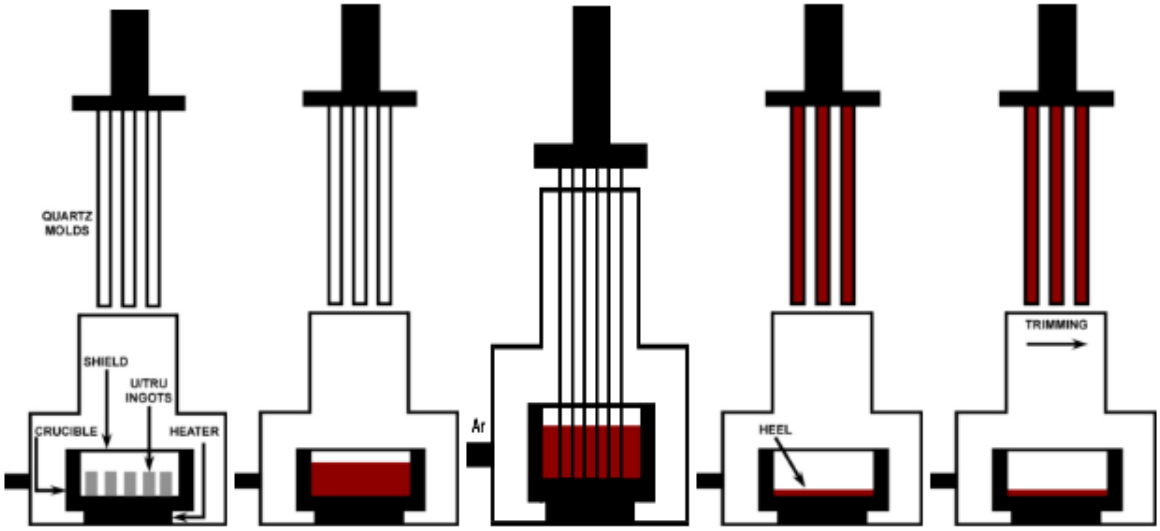

Figure 1.2: Injection casting process to fabricate metal fuel slugs. U and TRU are melted with zirconium to form metal feedstock for slug fabrication by injection casting and eventual fuel element assembly. The metal feedstock is first melted in a graphite crucible, and a vacuum is induced to inject the molten alloy into quartz molds. The 'heel' is a coating of metal that will remain on the crucible. The molds are then sheared and broken to obtain slugs. The sheared casting ends are called the 'scrap.' The crucible will suffer from eventual wear and is a waste stream, along with the quartz molds. The scrap, as well as the heel, will have to be recovered and accounted for prior to disposal.

1.3.2 Prior Use of DES for Pyroprocessing

There has been scant use of DES modeling for pyroprocessing. Previously, DES has been applied to nuclear facilities to study performance measures of used fuel handling [25], [26], [27]. DES also has been used to model the receipt of used fuel assemblies and separation of individual fuel pins [28]. DES modeling has shown that for batch processing, storage buffer capacity will be a key feature governing bottlenecks [29], [30]. Material congestion will occur if the buffer is too small. However, increasing buffer size is dependent on practical design considerations, such as cost and physical space. The challenge in developing a realistic model is that each subsystem requires a different batch size and processing time. For pyroprocessing, large quantities of salt are required for electroreduction, electrorefining, and electrowinning. To avoid lengthy process idleness,

fresh salt must be available to load into these subsystems when needed. Operational scheduling is therefore, vital [29], [30]. Most recently, DES has been used to develop a nuclear materials accounting model to identify potential diversion using a high-level MATLAB model [31]. The head-end processes were modeled, but fuel fabrication was not. Similarly, Garcia et al. [32], [33] used DES for process monitoring to detect anomalies using multiple sensor data for the head-end subsystems in pyroprocessing.

1.3.3 Safeguardability Assessment

A quantitative assessment for safeguardable facility designs has not been developed. Much of the research into safeguardability over the short history of the field has been qualitative. Initially, the Proliferation Resistance and Physical Protection Evaluation Methodology Working Group of the Generation IV International Forum (PRPPWG) promulgated high-level principles for establishing safeguardability [34]. A case study was developed for an Example Sodium Fast Reactor full system [35]. Four sodium fast reactors co-located with various storage facilities and a pyroprocessing facility were analyzed for several diversion and physical protection scenarios. Other studies addressed different components of the Example Sodium Fast Reactor full system based on a pathway analysis for additional scenarios [36], [37], [38], [39], [40], [41], [42], [43]. From a conceptual design analysis perspective within the context of safeguardability, several other studies outside of the PRPPWG are summarized in Borrelli [5]. These studies discuss safeguardability from a high-level, qualitative point of view. However, facility design as a process is not addressed in these studies. Engineering design approaches for a safeguardable facility are now needed. Therefore, because there are not yet any widely accepted metrics for safegurdability assessment, there is considerable latitude to develop one within this context.

1.4 Conceptual Model and Context

1.4.1 Relevance of Materials Accounting and Facility Design to Safeguardability Assessment

There is not yet a full system model that can enhance safety, security, and safeguards from a design-driven perspective. This preliminary process model presented here is not site specific and will be flexible and adaptable to varying facility designs. It can offer user-directed conceptual facility designs with a safeguardability assessment metric for

each. It is design-driven in that proliferation risk reduction is part of the design strategy. A top-down approach to pyroprocessing is applied here for facility design. That is, the whole system is considered as a 'big picture' first. The system is decomposed into first level elements called subsystems. It is described in Figure 1.1. Each system is refined to its 'base elements.' Then, these are studied as to how they interact with one another in order to produce the system output. This is further explained in Section 1.5.1. The model for fuel fabrication is built in this way, and eventually, this design approach will be applied to the full pyroprocessing system.

There are pyroprocessing models with similar goals in terms of process modeling [44], [45]. These are developed from a bottom-up perspective, where the chemistry and physics that govern processes in the base elements are applied in the model first, and then the full system is assembled from there. These research efforts apply different flowsheets from Figure 1.1. This approach is considered to be complementary to these models in that the first focus is on the facility design aspect inherent in the initial formulation of the safeguards- and security-by-design concept [3], [4]. Eventually, for a truly realistic process model that can be used to evaluate safeguardability, these approaches should be integrated. This is a long term goal as part of HRS.

The main focus of this study is to determine if the false alarm probability can be applied as a quantitative metric for safeguardability assessment. There are no current formalized International Atomic Energy Agency (IAEA) goals for the Type I error probability for an advanced fuel cycle concept. Therefore, there is considerable latitude in studying this metric within the context of safeguardability [5], [6]. The occurrence of a false alarm during facility operation would indicate a diversion has occurred, when in actuality it did not. For the model presented here, this could happen due to equipment failures. Equipment failures require repair and cleaning to remove SNM, and these are potential diversion risks. False alarms would have to be resolved by a facility inspection and subsequent inventory accounting. Facility operations would cease in the meantime. This would be costly for the facility operator, both in terms of operation throughput goals and possible compensatory penalties.

1.4.2 The Role of Nuclear Materials Accounting

Quantitative assessment of safeguardability is ultimately based on NMA. Poor accounting could fail to detect an actual diversion event. In order to establish an accurate mass balance for SNM in the facility, material balance areas (MBAs); i.e., the config-

uration of hot cells in the facility, have to be established appropriately. NMA would be performed at designated key measurement points (KMPs) at the interface of the MBAs. For pyroprocessing, two main challenges to safeguardability are: (1) lack of an accountability tank in order to determine SNM concentration and (2) inability to flush out the entire system and entirely clear the inventory. For NMA, the following well-known relationship is used [11]:

$$\Phi^{-1}(1-\alpha) + \Phi^{-1}(1-\beta) = \frac{SQ}{\sigma}, \tag{1.1}$$

where α is the false alarm probability, 1 - β is the detection probability, SQ is the significant quantity of SNM, σ is the standard error of the inventory difference (SEID), and Φ^{-1} is the inverse Gaussian function. An instructive example is commonly used [12]: for $\alpha = 0.05$ and 1 - $\beta = 0.95$, a SQ of 8 kg of Pu allows for an uncertainty in measurement of 2.4 kg in order to detect a diversion.

In the interval t = (t0, t1), over a material balance area, the inventory difference (ID) is formally defined as [11]:

$$ID = I_0 + D - I_1, \tag{1.2}$$

where I_0 = initial physical inventory, I_1 = final physical inventory or the inventory at t = t1, and D = material throughput over the time interval across the material balance area. Ideally, ID = 0 over any time interval, but in reality ID $\neq$ 0 due to material hold up and process losses. Typically, in materials accounting, the three quantities defined in Equation 1.2 are treated as random variables. Therefore, measurements are obtained in terms of the expected value of the ID with associated deviation due to persistent systematic errors; i.e., SEID [11].

A possible pyroprocessing facility conceptual design is depicted by the flow diagram shown in Figure 1.1. For large MBAs containing many of the subsystems, based on standard NMA techniques, the SEID could exceed detection limits for a possible diversion attempt. With small MBAs, the SEID may be low due to more KMPs. There could be frequent Type I errors. Additionally, with more KMPs, more time is needed for accounting, and operation time would be affected. The formation of MBAs and resulting NMA are clearly interrelated with material throughput and operational goals. Both are a function of the facility design. Safeguardability, therefore, is invariably a function of facility mass balance. These considerations should be optimized as part of the conceptual design strategy and safeguardability assessment.

1.4.3 Fuel Fabrication Intracellular Activity

Here, a systematic method that has been established to consider the activities included in each subsystem is described, and it provides a framework for conceptual facility design. This framework informed how the DES modeling architecture was constructed for the fuel fabrication system. This conceptual modeling framework was established for overall hot cell and facility design, and material throughput [5]. It is shown in Figure 1.3a. Five activities will occur during normal operation of any process in the system: (1) process activity, (2) byproduct, (3) in-situ recycling, (4) final product, and (5) ancillary activity. Not all of these activities will be performed in a single cell, however, the prior study has determined that these five are essential.

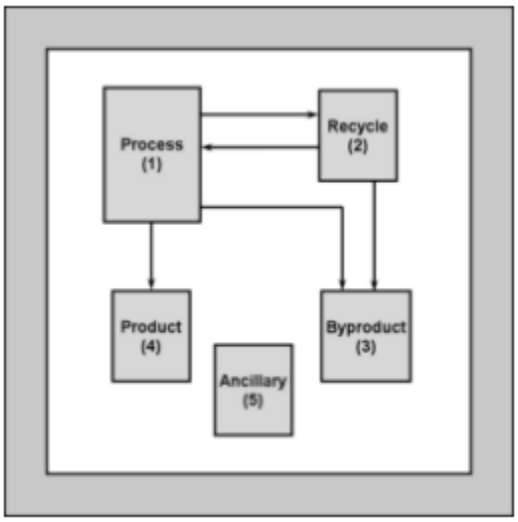

Figure 1.3a

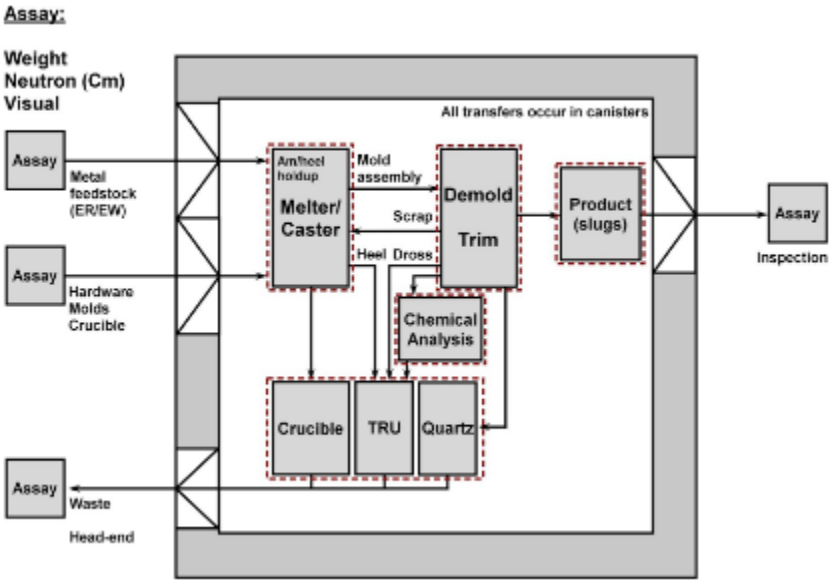

Figure 1.3b

Figure 1.3: Overall hot cell and facility design. A minimum of five activities are assumed to occur in order to complete a process. These are shown notionally in Figure 1.3a and applied to the injection and casting of metal alloy fuel slug in Figure 1.3b. The five activities defined in Figure 1.3a are contained each within the red dotted box in Figure 1.3b. Material arrives from the electrorefining (ER) and electrowinning (EW) processes. The process activity (1) is the injection casting system in which U and TRU metal, rare earth fission products, and Zr are melted into an alloy and injected into quartz molds to form fuel slugs and then trimmed. Material, such as americium, may be held up in the equipment. The recycled (2) material (scrap) is the leftover alloy from the mold trimming process. The heel could be recycled with the scrap. The byproducts (3) are the graphite crucibles. This is treated as waste. The heel also may be collected and returned to head-end processes for recycle or stored in a buffer. The quartz molds, after being trimmed and broken to obtain the alloy, cannot be recycled and are treated as waste. The alloy products are fuel slugs (4). Additional analysis may be necessary as an ancillary activity (5) for in-situ quality control; e.g., slug straightness. Assay both upon entry and exit is critical because U and TRU enter as separate batches, but after fabrication the single alloy will exit the cell. These materials could be assayed by visual inspection, neutron detection, weight, or potentially other destructive means. These activities do not necessarily have to occur in a single cell.

Figure 1.3b shows how these activities apply to fuel slug fabrication. Injection casting will process the largest amount of SNM in the pyroprocessing facility, and material is always left in the crucible; i.e., heel [7]. The heel will contribute to the

SEID and could pose a diversion risk upon equipment failure. The process activity (1) includes the injection casting and trimming processes. Byproducts (2) are the graphite crucible, the heel, and the quartz molds after trimming. The crucible and molds will be disposed as waste. The heel could remain in the crucible until the operator decides to remove it. Or, the heel may be removed after a campaign and stored in a buffer until it is recycled into the injection casting equipment. During the normal operation, scrap (or the leftover alloy from the mold trimming process) is recycled back into the melting and casting equipment (3). The final products (4) are the metal fuel slugs. These would be transferred from the cell to subsequent processing for full fuel element assembly. Finally, some quality control analysis could serve as an ancillary activity (5). This activity may be necessary in order to determine if the product satisfies other physical requirements, such as straightness and diameter. Some destructive assay (DA) may also be required. DA would likely be performed on the fabricated slugs in order to test SNM content. Ideally, the ingots of U and TRU (with Zr added) would form a homogenous metal solution in the melter. Therefore, the slugs would be expected to have a consistent SNM composition, and DA would test for this. Considering only these minimum five activities, modeling any process in the system can become exceedingly complex.

1.5 DES Model

This is the first build for a full system pyroprocessing model intended to quantify safeguardability for different facility designs and material throughput goals. The model is developed with Python. It offers a modular environment which is conducive to the use of discrete event simulation and the batch nature of pyroprocessing. The basic code architecture allows an efficient model platform for the full pyroprocessing facility. This Python code can perform many processes and operate systems simultaneously. Additionally, this model is open source, with the eventual intent that other users can design and model safeguardability of other nuclear handling facilities.[1]

1.5.1 Model Space

The design of the fuel fabrication system is shown in Figure 1.4. It is currently assumed that metal fuel slugs are manufactured by an injection casting system based

[1] https://github.com/lee7632/Fuel-fabrication-process-code-development

on the history and expected future use of this technology as discussed in Section 1.3.1. The 'baseline design' is shown in Figure 1.4a, Design A, and the 'equipment design' is shown in Figure 1.4b, Design B. These designs align with the discussion of the minimum activities needed to complete the task shown in Figure 1.3. Material flows are indicated by the arrows. Maintenance is also included. Chemical analysis and waste streams are currently neglected. The vertices are: (1) storage buffer, (2) melter, (3) trimmer, (4) product storage, and (5) recycle storage. These would be 'base elements' of the fuel fabrication subsystem, as discussed in Section 1.4.1. State changes occur at these vertices. The solid lines indicate the path of the state variable; i.e., these are the edges through which the state variable transitions from vertex to vertex. There are no changes to the state variable on the edges. The KMPs are numbered 0, 1, 2, and 3. Maintenance is not a vertex because there is no state variable transition. The dotted line indicates equipment transfer. Based on Figure 1.4, and the discussion in Section 1.4.3, DA would not be performed until after the product storage vertex. Therefore, DA is neglected at this phase of the model build.

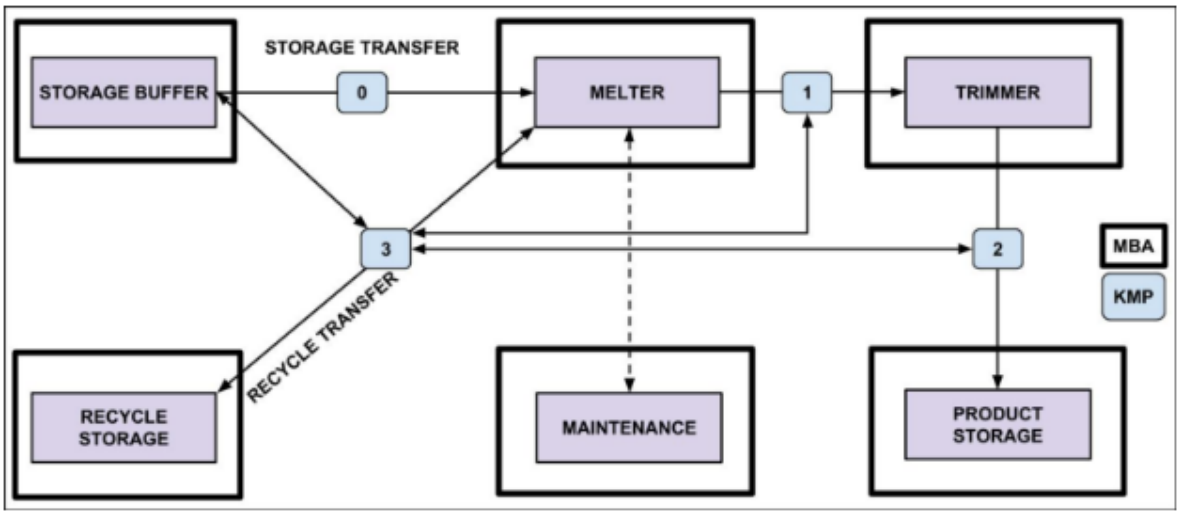

Figure 1.4a

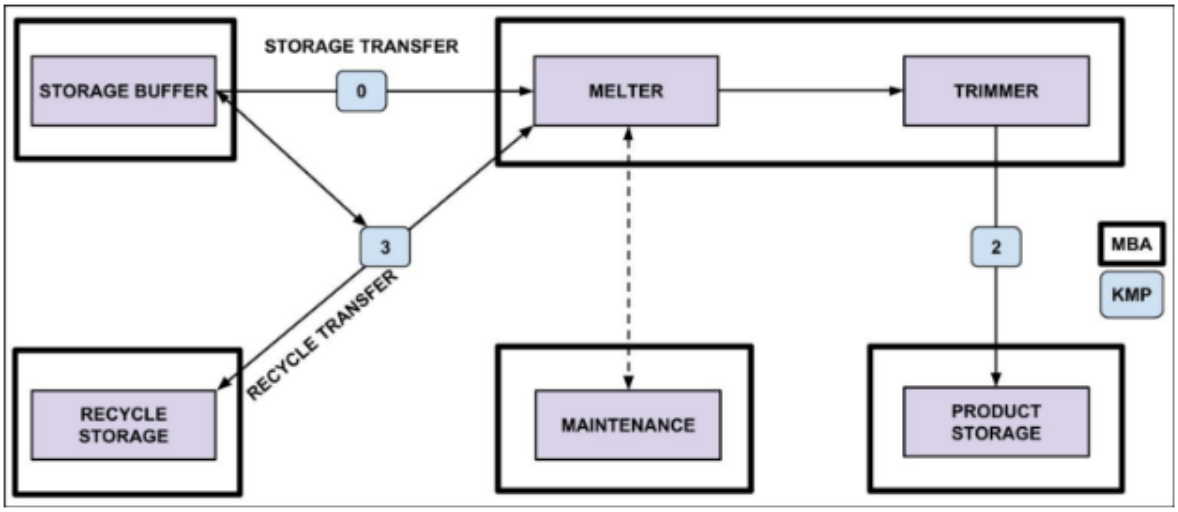

Figure 1.4b

Figure 1.4: DES modeling framework for fuel fabrication. The 'baseline design' is shown in Figure 1.4a, and the 'equipment design' is shown in Figure 1.4b. The state variable is the 'true weight' of the material that will be processed in the system. As metioned above, the vertices are: (1) storage buffer, (2) melter, (3) trimmer, (4) product storage, and (5) recycle storage. The path of the state variable is indicated by the solid lines, and state variables do not change at the edges. There are key measurement points numbered 0, 1, 2, and 3, and the edges represent state transitions from vertex to vertex. Maintenance is not defined as a vertex, and equipment transfer to it is indicated by a dotted line. In this configuration, each vertex is a material balance area.

1.5.2 Assumptions

Without a commercial pyroprocessing facility built yet and the proprietary issues surrounding engineering-scale facilities, as well as the widely known difficulties with regards to scaling from laboratory experiments, obtaining input parameters has been difficult over the years of this model development. Citations have been provided in this section for some of the input parameters, and reasonable assumptions have been made for the rest. This has been based on prior experience from the research collaboration between the Korean Atomic Energy Research Institute and UC-Berkeley, Department of Nuclear Engineering, where the HRS methodology was initially formulated. Further discussion of this collaboration is contained in Borrelli [5], [6].

KAERI was constructing the Pyroprocess Integrated Inactive Demonstration (PRIDE) facility, a cold-test, engineering-scale, mock-up facility designed and operated by KAERI

to support pyroprocessing subsystems demonstration and equipment development [46], [47], [48], [49]. Therefore, modeling the PRIDE system also required a similar approach. There were many discussions and much preliminary work on how a facility could be constructed while also maintaining strong safeguards; i.e., safeguardability, as part of this collaboration, which partially led to the development of this model and the approach applied here [50], [51], [52], [53], [54]. These assumptions for input parameters are reasonable because actual operational targets, such as designing a safeguardable facility that will process a specific amount; e.g., 800 MTHM per year, are not needed currently. The main focus and motivation is to test the safeguardability of different designs while observing how much material can be processed per operational period. This discussion is continued in Section 1.7.2 following the presentation of the results and subsequent discussion.

1.5.3 Safeguardability Criteria

The reasoning in studying the Type I error as a safeguardability metric is that when there is some event, whether it arises from safeguards, safety, or security, there will be a mass balance conducted at least on some subsystems in the facility, if not the entire facility. Therefore, the associated statistical measures are common across all regimes, which is part of the synergistic approach initially conceptualized for safeguardability. However, a mass balance is not only performed due to anomalies in safety, safeguards, or security. It can also be performed after routine maintenance. For example, the crucible in the injection casting machine may be replaced regularly after a set number of campaigns. A facility mass balance may be conducted after a full campaign, or at regularly scheduled intervals in the operational period. These are mass balances over normal operating conditions and would be established most likely by the operator as part of the licensing process, and, presumably, based on IAEA guidelines. This optimization of designing the facility to maximize throughput, while also integrating safeguards, safety, and security measures appropriately into the design is the essential basis for safeguardability.

If an alarm arises, the subsystem will have to cease operations, if not the entire facility. The alarm is an indication of a potential diversion event. It is not known ahead of time whether the alarm is indicative of a statistical anomaly, which can be resolved upon further inspection; i.e., a false alarm. If it is assumed that an inspection would ensue to resolve a potential diversion and that some part of the facility is shut

down, this will cost time and resources, as well as affect the operational goals of the facility. Therefore, if a particular facility design elicited a high number of false alarms, this would be detrimental to all stakeholders involved. This will carry a high cost in terms of resources needed for inspections and materials accounting, as well as the loss of productivity. There will also be an intangible detriment in that a high number of potential diversion events could raise concerns that the State may have malicious intent in terms of the use of this facility. This could cause concern in the international community and perhaps result in political reprisal, such as imposed sanctions. Therefore, a primary criterion for this proposed safeguardability metric would be that the more safeguardable facility design elicits the lowest number of false alarms while maintaining a reasonably high detection probability.

1.5.4 Systems Operation

One campaign is defined as the processing of one batch. That is, the transition of the state variable from the storage buffer to the product storage. Material flow is sequential. Because there are no experimental studies on the commercial scale, some values were assumed, and others were based on prior study. Material flow is simulated for a prescribed 250-day facility operation period, which is about a 0.70 capacity factor [55]. Facility operation is continuous for the operational period except for equipment failure and maintenance, or facility inspection and mass balance. The edge transfer time refers to transition of the state variable from the storage buffer to KMP0, from KMP0 to the melter, etc., as shown in Figure 1.4. Inspection times for both, the end of campaign and after equipment failure, are assumed to be 4 h. Additional operational data is contained in Table 1.1.

Table 1.1: Input values for the simulations

Input variable	Value
Batch size	20 kg
Operational time	250 days
Melter failure rate	$1/30\ \text{day}^{-1}$
Expected material left in the crucible	250 grams
True material left in the crucible	0–500 grams, randomly distributed
Measurement time at a KMP	30 min
KMP transfer time	30 min
Storage buffer batch preparation time	1 h
Melter operation time	8 h
Trimming operation time	3 h
Product storage preparation time	2 h
Maintenance time	4 h
Recycle storage time	1 h
Maintenance transfer time	1 h
Melter cleaning time	2 h
End of campaign inspection	4 h
Failure inspection	4 h

1.5.5 Inventory Difference

The inventory difference for this system is due to the heel in the crucible. There are variables for true ID, expected ID, and measured ID. In this study, the actual values of the three variables are used, although a measurement error is included. During operation, the heel is not removed at the end of each campaign because this causes frequent stoppages. Developing an accurate system of materials control and accountability is perhaps the fundamental tenet of a safeguardable nuclear materials handling facility. For a non-nuclear weapons State, materials accounting is required for IAEA design information verification and related treaty obligations.

A mass balance (inspection) is conducted at the end of each campaign. This takes 4 h. A false alarm is triggered when the measured ID is greater than 2 kg. This threshold is selected as a nominal value below the typical IAEA goal of 2.4 kg due to a lack of any safeguards goals for pyroprocessing facilities.

1.5.6 State Variables

From the DES perspective, the state variable is defined as the 'true weight' of the material that will be processed in the system. In reality, the true weight is never known in the facility. In general, data recorded at KMPs; e.g., weight, neutron count, etc., are compared to expected results based on historical data cohorts. In addition to the state variable of the true weight, for this model, there are also 'expected weight' and 'measured weight' variables.[2] These are the means for estimating the true weight. The 'expected weight' is defined as the batch quantity expected to transition through each vertex. This is based on historical data cohorts, experimental studies, pilot studies, etc. Determination of 'measured weight' at each KMP is the true weight ± measurement error. In Equation 1.2, each of the quantities that comprise the ID has a 'random error of the measurement' associated with it, and these errors are assumed to be independently and normally distributed [11]. Therefore, the uncertainty in measurement is sampled from a normal distribution about a user prescribed value of 0.10 kg. Measurement time is 30 min. In reality, this is the only known value of the batch in the system.

1.5.7 Vertices

1.5.7.1 Storage Buffer

The fuel composition is prescribed by weight percent. It is 65U-20TRU-5REFP-10Zr, REFP = rare earth fission products [7]. Based on the flowsheet in Figure 1.1, prior to fuel fabrication, U is obtained from electrorefining, where U metal is collected on a solid cathode, typically graphite, and TRU is obtained from electrowinning and is collected on a liquid cadmium cathode. Then, these materials will be processed further into metal ingots and stored separately in buffers. The ingots would be subsequently transferred to the fuel fabrication system. Currently, the model assumes a storage buffer vertex that already contains the ingots of U and TRU metal. It is assumed that when the ingots are placed into the crucible and heated, sufficient time has elapsed such that the composition is homogeneously distributed. The batch size is 20 kg [7], [52], where the subcriticality limit is 25 kg [46], [56]. The expected weight at this vertex is then 20 kg. Because no processing occurs, the true weight is also 20 kg. There is a 1 h 'batch preparation time.' The correct amount of material for a 20 kg batch is then assumed

[2]Here, an 'expected quantity' is defined as a amount of material that is anticipated to exist at a KMP in the model.

to be transferred from the storage buffer to the melter in this current model.

1.5.7.2 Melter

Operation time for the melter is 8 h [22]. For this stage of the model development, the true amount of material held up in the crucible per campaign; i.e., the heel, is assumed to be a random variable. The injection casting equipment melts the metal ingots, then the quartz molds are inserted, and the resulting vacuum induces injection of the melt into the molds. Upon removal, some of the melt remains as the heel. This could be due to the melt dripping off the outside of the molds, or perhaps one or more of the molds were not completely filled. Either of these events, however, is of a random nature. When the next campaign starts, the heel is melted along with the new ingots that have been placed into the crucible. The amount of material that remains as the heel is overall more than that from the prior campaign, but the amount that is left from the current campaign is again random and could be more or less than the prior campaign. Therefore, the material left in the crucible per campaign is sampled from a continuous uniform distribution. This is used for many problems where there is a lack of data describing the phenomenon of interest. Typically, laboratory experiments would be performed to quantify the heel, and these data would be fit to a known distribution. Then, the mean and variance could be used in the model. Since these data are not currently available, the true amount of material left in the crucible is conservatively assumed to be a continuous uniform distribution between 0 g and 500 g, based on prior study [7]. The expected process loss is prescribed at 250 g. Scrap is currently neglected. Therefore, the expected weight is 19.75 kg. Failure testing occurs halfway into operation. This is discussed at length subsequently.

1.5.7.3 Trimmer

Operation time for the trimmer is 3 h. There are currently no failures or process losses. Therefore, the expected weight is also 19.75 kg, and the true weight is the same as determined in the melting process.

1.5.7.4 Product Storage

No processing occurs here. The weights are the same. There is a 2 h ‘product storage time.’

1.5.8 Melter Failure

Any piece of equipment in an industrial facility will have several failure modes associated with it, depending on the complexity of the equipment. Analysis of these failure modes is essential for preparing a probabilistic risk assessment for the entire facility. A pyroprocessing facility exhibits additional complexity because proliferation risk must be characterized as well. While fully assessing equipment risk is beyond the scope of the current paper, equipment failure can be nominally modeled for this system.

There are numerous failure modes in the injection casting system, in both the melter and the trimmer. Failures of the trimming equipment are neglected. For the melter, frequent and expected failure modes include crucible or quartz mold cracking. The alloy may not be completely melted due to a heater failure. There may be a failure with the injection system where the alloy may not completely fill the molds. The loss of the inert atmosphere could result in a fire. It can be reasonably assumed that any of these failures results in a complete shutdown of the injection casting equipment. Therefore, a single, general failure of the melter is assumed, and this results in a system shutdown and necessitates removal of the failed equipment and installation of a new melter.

Upon a melter failure, after the batch is measured at KMP3 and transferred to the recycle storage, the facility inspection is conducted to calculate ID. This is where a false alarm could occur. If a failure occurs during the first processing campaign, the ID is due to the random amount of heel present in the crucible. For subsequent campaigns, the ID is due to the random amount left due to the current campaign and the quantity accumulated from prior campaigns.

The cumulative distribution function based on the Weibull distribution is used to model the stochastic failure of the melter [57]. The Weibull distribution is a widely accepted and applied model for failure analysis, especially in cases where information about failures or related failure modes is largely unknown. The 'unreliability' of a system element can be defined under Weibull as:

$$Q(t) = 1 - e^{-\frac{t}{\eta}^{\beta}}, \tag{1.3}$$

where: t = facility operation time, η = mean time to failure, and β = shape parameter. In the facility, as operation time increases, the probability of melter failure will increase. By definition, Equation 1.3 then gives the probability of failure over the operation time in the facility. The unreliability function based on Weibull is useful because it is rather generalized and can be applied to a wide variety of problems. Typically, the shape

parameter is determined based on historical operational data. From a mathematical perspective, it should be relatively intuitive that variation of the shape parameter will significantly affect the character of the distribution. This is the strength of the Weibull distribution; fitting failure data by adjusting the shape parameter will yield information about the nature of failure. For example, with $\beta < 1$, this implies failure rate that decreases with time. Therefore, this equipment is still in the early life stage. However, here, with the lack of operational expertise, it is assumed that $\beta = 1$; i.e., 'general failures. Any of the failures described above cease activity and require maintenance within the system. Therefore, Equation 1.3 reduces to the exponential distribution, and the reciprocal of the mean time to failure (η^{-1}) equals the constant failure rate (λ). A melter failure rate of once per month is assumed.

A Monte Carlo routine based on Q(t) was then developed to this end to model the failure of the melter. Upon failure, the batch is moved to recycle storage from the melter. The equipment is then 'cleaned;' i.e., the heel is moved to recycle storage with a 2 h cleaning time. During maintenance, the defective equipment is removed, and a new equipment is installed. The total amount of material is then transferred from recycle storage to the melter, and operation resumes.

1.5.9 Features of the Code

The code focuses on maintaining a hierarchical decomposition of the facility components. This design logic goes well with batch processes since only the state variable is passed from vertex to vertex. In this regard, each node in Figure 1.4 is represented by its own class in Python. Each of these objects accepts the batch (which is its own object), acts on it accordingly, and then passes it to the next vertex class.

The vertices in the system model act as the bottom-most children of the hierarchy. They are grouped together according to proximity as shown in Figure 1.4, and each group is assigned a managing object that can call on any of its children at any given moment for pertinent information; i.e., the measured weight, the expected weight, etc. That information is then passed on to the supervisor who uses the information to make facility-wide calculations and decisions such as when an alarm should be triggered. However, the supervisor does not call on the managers to collect this information until it is needed, minimizing the computation time by avoiding unnecessarily frequent updates.

Although many programming languages are robust enough, Python is favored for its flexibility in importing objects and accessing components. An entire object can be

imported to a different object, or one can bring in only a few variables or methods from that object. These objects are passed internally by reference, minimizing overhead costs when manager and supervisor nodes call their children nodes. This structure can be readily expanded in order to model the full system shown in Figure 1.1 in a similar manner.

1.5.10 Simulations

First, the input/output directories of the full system were created. The system input parameters in these directories included relevant operational data. Then, the simulation was run for the operational period of 250 days. At the end of each campaign, the full material balance over the facility was performed, and in each case, the measured inventory difference was checked against the expected inventory difference as a semi-empirical Shewhart's test [58]. If this difference was above the prescribed threshold, an alarm was raised. The system output data obtained from the simulation were recorded in the output directories. Execution scripts were built to automate simulation for a user prescribed number of times. The simulated false alarm probability was computed based on actual false alarms over potential opportunities for a false alarm. Simulated melter failure probability was calculated by dividing the number of failures by operation time.

To assess safeguardability on a pyroprocessing facility, it is imperative to test various facility designs. Material throughput for two different facility designs were simulated based on Figure 1.4: the 'baseline design (Design A)' and the 'equipment design (Design B).' Design B was with KMP1 removal. From a qualitative perspective, Design A was intended to exhibit stronger safeguardability because each vertex is its own MBA, while for Design B, the removal of KMP1 was intended to maximize material throughput. Optimization of each is the basis for a highly safeguardable facility. Operation periods were simulated for 1000 times, 2000 times, and 3000 times, and the average output values with standard deviations were calculated for both designs.

1.6 Results and Discussion

1.6.1 System Output

It was determined that 1000 simulations were large enough to achieve convergence in the output data. Results are presented as the average values with standard deviations over the 1000 simulations. Figure 1.5 shows the melter failure probabilities for both

designs. The simulated melter failure probabilities shown in Figure 1.5 for Design A and Design B are essentially equal at 0.150 ± 0.013. This shows that the subsequent results are not a function of melter failure, and therefore, safeguardability is not a function of the choice of equipment and only based on material flow and design. Therefore, from this result, the code is producing results consistent with the physical conditions established in this study.

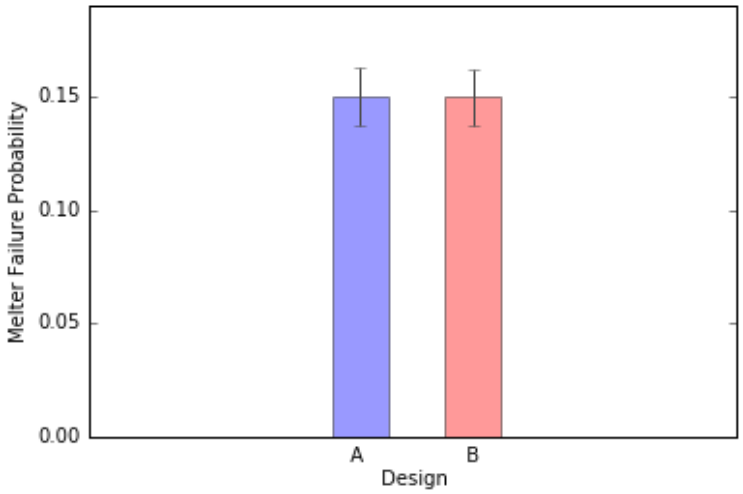

Figure 1.5: Simulated melter failure probability. The simulated melter failure probabilities for Design A and Design B are equal at 0.150 ± 0.013. This shows that the subsequent results are not a function of melter failure.

The average completed fuel fabrication campaigns are shown in Figure 1.6. The average number of campaigns of Design A is calculated as 229 ± 4.2, and that of Design B is 229 ± 4.1. This indicates that the proposed designs do not affect operational goals. The false alarm probability of Design A and that of Design B are also effectively similar, as shown in Figure 1.7. The false alarm probability of Design A is given as 0.019 ± 0.007 and that of Design B is 0.019 ± 0.008. This is considerably less than the typical IAEA recommended goal of 0.05. After the 250 day operations, the average amounts of processed material for Design A and Design B are 4568 ± 84.2 kg and 4570 ± 83.0 kg, respectively, shown in Figure 1.8.

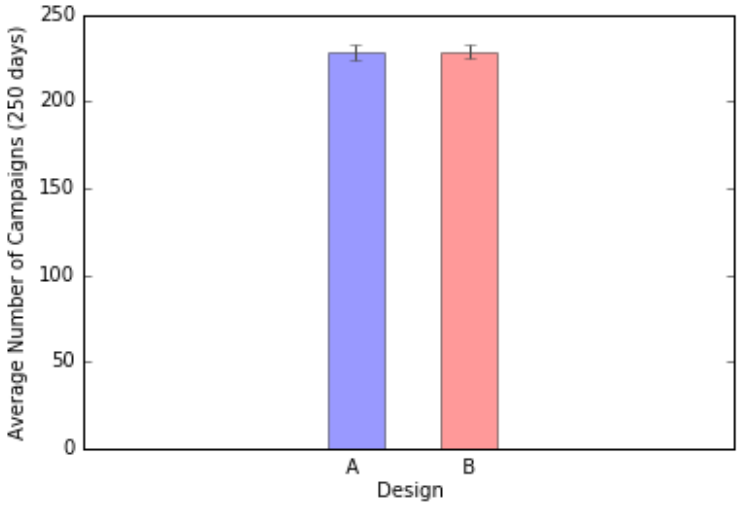

Figure 1.6: Simulated number of completed campaigns. The average number of campaigns of Design A is 229 ± 4.2, and that of Design B is 229 ± 4.1. These proposed designs do not affect operational goals, but these results also indicate that the designs are essentially equivalent.

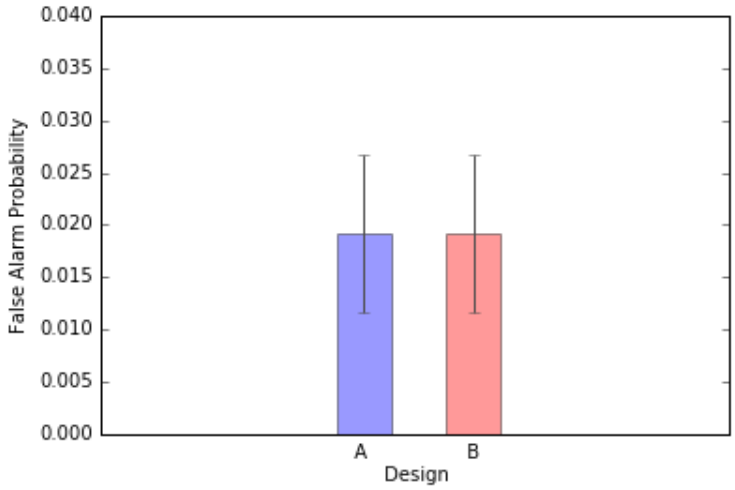

Figure 1.7: Simulated false alarm probability. The false alarm probability of Design A is 0.019 ± 0.007, and that of Design B is 0.019 ± 0.008. Again, these values are less than the typical IAEA recommended goal of 0.05. A low false alarm probability with a reasonably high detection probability is a proposed criteria for safeguardability assessment and indicative of a strong, safeguardable design.

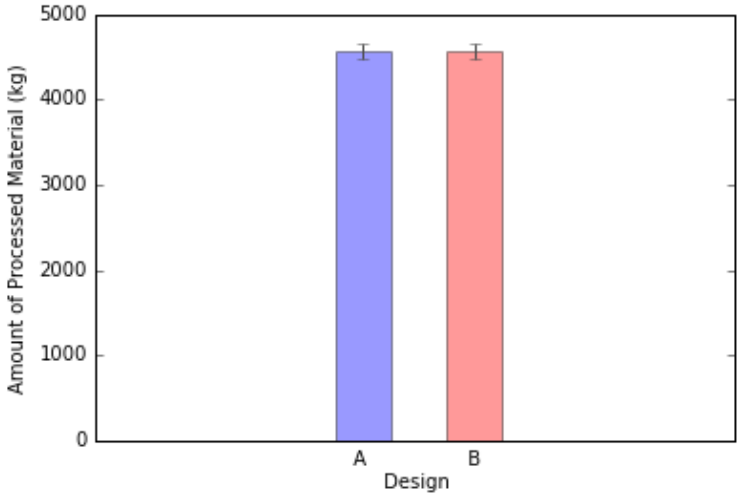

Figure 1.8: Simulated amount of processed material at the end of the operational period. The amount of processed material for Design A is 4568 ± 84.2 kg and for Design B, it is 4570 ± 83.0 kg. There are currently no operational goals for the pyroprocessing facility, but this will have to be optimized with safeguardability.

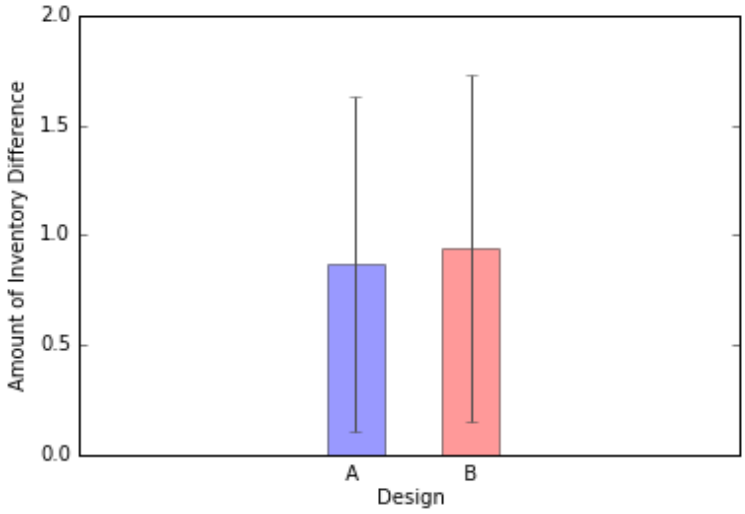

Figure 1.9: Simulated inventory difference. The inventory difference for Design A is 0.868 ± 1.152 kg, and for Design B, it is 0.940 ± 1.189 kg. Both of these designs offer strong safeguardability. The ID is well below the 8 kg for a significant quantity for plutonium for both, and the SEIDs for both are below the 2.4 kg based on suggested IAEA goals.

1.6.2 Inventory Difference

The inventory differences for Design A and Design B are shown in Figure 1.9. The simulated ID of Design A is 0.868 ± 1.152 kg, and that of Design B is 0.940 ± 1.189 kg. This indicates that both Design A and Design B are relatively safeguardable designs. The ID for each design is well below 1 SQ of 8 kg for plutonium, and the simulated SEIDs are below the 2.4 kg limit previously discussed.

To further examine the implications of SEID on safeguardability, Equation 1.1 is applied. Here, for α, the simulated false alarm probability of 0.019 ± 0.008 is substituted. Because it is essentially equal for both designs, the simulated false alarm probability with the higher standard deviation is used as a conservative estimate. Detection probabilities (1 - β) of 0.90 and 0.95 were selected. Appropriate design approaches can render decisions by the State to initiate a diversion attempt to be strategically poor because the detection probability is reflective of a State decision. A detection probability of 0.90 is considered a reasonable lower bound for study of this system. The SQ is 8 kg for plutonium. Therefore, the SEID in Equation 1.1 (σ) can be obtained directly. These calculations are contained in Table 1.2, where the IAEA goal of SEID = 2.4 kg is included for reference, as well as the SEID of 2.7 kg for α = 0.05 and 1 - β = 0.90. Clearly, for the simulated false alarm probability range, the calculated SEIDs shown in Table 1.2 ranging from 2.03 kg to 2.38 kg fall below the IAEA goal of SEID = 2.4 kg, except in the one instance of 2.49 kg. However, the value of 2.49 kg falls below the calculated limit of 2.7 kg. Even though there are no current IAEA goals on safeguards for the advanced fuel cycle, the simulations and related calculations are on par with the suggested IAEA goals previously discussed. This shows that the use of the false alarm probability offers merit as a safegurdability assessment metric.

Table 1.2: Calculated standard errors of inventory difference using Equation 1.1

False alarm probability (α)	Detection probability (1 − β)	SEID (kg)
0.05	0.95	2.4
0.05	0.90	2.7
0.011	0.95	2.03
0.019	0.95	2.15
0.027	0.95	2.24
0.011	0.90	2.24
0.019	0.90	2.38
0.027	0.90	2.49

More importantly, the simulated SEIDs of 1.152 kg and 1.189 kg for Design A and Design B respectively, are far below the calculated SEIDs. Both designs are highly safeguardable and therefore could be prohibitive for State-driven attempts at material diversion even at a detection probability of 0.90. Yet at the same time, these facility designs showed that approximately 4500 kg of material could be processed. This model can offer the capabilities of optimizing operational goals with an assessment of design in terms of safeguardability. This is a significant result for safeguardability assessment. Applying the false alarm probability to safeguardability assessment in this way is a valuable, preliminary effort into developing a safeguards- and security-by-design approach for a commercial pyroprocessing facility.

1.6.3 Functional Design Components and Preliminary Safeguardability Assessment

Ultimately, the intent is to use this model in order to assess proposed facility designs and offer functional design components to enhance safeguardability. To this end, Design A was expected to be a highly safeguardable design, due to a key measurement point after each vertex and a material balance after the product was stored in the final vertex. Design B was expected to exhibit a higher throughput with the removal of KMP1 but potentially be less safeguardable.

Essentially, Design A and Design B processed about the same amount of material over the operational period. In Design A, a MBA was established for each process step, and for Design B, the melting and trimming processes were included in a single MBA. Ideally, maximizing material balance calculations will produce a strong, safeguardable facility. With no appreciable changes in the false alarm probability and the quantity of processed material, both Design A and Design B can be applied to this system without sacrificing operational goals. Therefore, these results show that there is almost no difference in terms of safeguardability between Design A and Design B; i.e., these are equivalent designs based on the conditions established for this proposed facility. This is still a meaningful result and a good application of this model. In reality, two proposed designs might look different where one carries a much higher cost. The model can show that the designs are in actuality equivalent and provide a nominal economic tool.

The simulated SEIDs for both designs fell well below the calculated SEIDs, even for the lower bound detection probability of 0.90. When instituting safeguards measures in a new facility, the use of the lower detection probability may result in less overall

cost. IAEA does not currently have safeguards goals for advanced nuclear fuel handling facilities, and this result could be the basis for new evaluations of safeguards between IAEA and the host State. In essence, this could be similar conceptually to ALARA, where an economic limitation is placed on the quantitative reduction in radiation exposure. Increasing the detection probability in the safeguards system from 0.90 to 0.95 may be cost prohibitive and potentially not necessary if SEID simulations can be shown to fall below projections obtained from Equation 1.1. Clearly, this is also based on a simulated low false alarm probability as was the case in this study.

1.7 Future Work

The results in this study lead to substantial upcoming work. Near term activities will focus on three overall features: (1) measurement and accounting, (2) building in practicality, and (3) integrating the chemistry and physics that govern these processes through mathematical modeling. Currently, the model has not been developed to the point of being usable as a tool for major design approaches for the full pyroprocessing facility. However, these results are promising in the development of a robust manner in which safeguardability can be assessed within the context of facility design in its current form. Upgrades to the model will focus on a more accurate simulation of the safeguards system and NMA, as well as operational considerations, which affect safeguardability assessment.

1.7.1 Measurement and Accounting

Activities at the KMPs require further development. This includes the removal of different KMPs, investigating changes in parameters (such as the uncertainty of the KMP measurement), the ID inspection at each KMP, and changes in the weight threshold on operational goals. Currently, only a weight measurement is simulated at the KMP. If the U and TRU ingots could be melted to produce a homogenous mixture, then it may be possible to use neutron counting after the melting process. This could be upon transfer of the injected molds to the trimmer or after slug trimming. This would be at KMP1 and KMP2 in Figure 1.4. In terms of configuration of KMPs in the system; i.e., examining the possible formations of MBAs, observing how system parameters are affected will yield further insight into safeguardability. Whether it is more prudent to minimize the number of KMPs, but not necessarily the number of material balance calculations will also be considered. There may be centrally located

assay station(s) in order to conduct the measurements. Therefore, it may be possible to enhance operational goals while maintaining strong safeguards.

As part of an NMA system, DA should also be considered. For fuel fabrication, if there is a storage buffer of fabricated slugs, as presented in the current model, in which the next stage would be assembling the fuel rods, it is reasonable that DA could be performed at this point in the system, where slugs would be presumably chosen at random for assay. DA would be needed to address inhomogeneity of processed materials. Therefore, DA would not cause an operational disruption because the slugs are already stored in the buffer. Additional analysis is needed to determine if the destroyed material is a diversion risk, or how much of a risk it is in comparison to other potential diversion pathways in the facility. The NMA system will also have to include accounting for the SNM content in tested material. The final state of the tested material would need to be considered. An operator would want to process as much material as possible and might want to recycle the material back into the melter, rather than outright disposal, but the composition of the melt is prescribed. New procedures would then be needed to address recycle in this manner. The material could still be stored and monitored relatively long-term in a separate, dedicated buffer.

1.7.2 Practical Use of the Model

Every effort was made to build a practical model, compiled over several years of study, but there could be more robust input data. Currently, assumed parameters were used, as previously discussed in Section 1.5, in order to test the model, analyze its performance, and determine directions for the next phase of development. It was established that the model described the physical conditions established for this study, which is important, and, that the results showed the proposed designs under these conditions were equivalent, which partially supports the hypothesis set at the start of this study. Process loss in the trimmer was neglected. The physical material in this process will be fine particulates of metal. Quantifying the amount of this material as well as determining how much material can be cleaned will be challenging. If a suitable model can be developed, or more reliable data can be obtained to include process loss in the trimmer, then the model should again be applied to assess Design A and Design B in terms of safeguardability.

Historical operational data is currently lacking. However, injecting casting, as an industrial process, has been used for decades. Applying operational data from an anal-

ogous process to the injection casting process of the U and TRU metal to this pyroprocessing system model would be fairly useful, from a risk assessment perspective, in terms of failure modes and associated failure rates. Recent dissemination of this work for the first time [59] has generated interest in further discussions on this work and could help address this issue. Engaging with other experts in this field has been an ongoing process, and additional solicitation of expert judgement would be beneficial. Failure rates for both the melter and the trimmer are needed, as well as processing times and determination of held up material for both. More accurate processing times will elicit a clearer conclusion in terms of operational goals. In reality, there are multiple failure modes for the equipment, and an envelope of the most common modes should be developed. A parallel study is focused on developing a high-level hazard and operability (HAZOP) analysis for the pyroprocessing facility in order to better understand operational considerations and equipment failure modes. Therefore, with more robust input data and improved engineering design, as discussed in Section 1.7.3, the safeguardability of a facility design with operational goals can be optimized, and the outcomes put forth under HRS can be achieved.

1.7.3 Engineering Design

Results from this study were not exactly as expected. Our hypothesis asked whether the false alarm probability can be used as a metric to evaluate system designs in terms of safeguardability. Because no studies have been formulated in this way, there is not really any additional guidance on how to proceed. The results show that the proposed designs themselves are equivalent, but there needs to be more insight into actually quantifying safeguardability in a meaningful way that is readily acceptable. The engineering design aspect of this study needed to be stronger, and in the next build of the code, more demonstrably different designs will be considered.

1.7.4 Complementary Approaches

The next phase of model development beyond bulk material flow, as presented here, will be to integrate the chemical and physical processes governing the fuel fabrication subsystems; i.e., applying the bottom-up approach to the system model. DES is a useful modeling structure to this end because mathematical models that describe these processes can be built into the appropriate vertices. For example, with injection casting, the melting process is modeled as the classical Stefan problem found in heat trans-

fer. With these upcoming accomplishments, the model can be expanded for the full pyroprocessing system.

Finally, when this model achieves a reasonable level of maturity, it can be validated against similar models in the literature; e.g., most notably, the model developed by Cipiti et al. [44], but other published work as well. Validation will aid in expanding this DES model significantly and provide meaningful insight into safeguardability assessment.

1.8 Summary Remarks

The design of a safeguardable facility in the advanced fuel cycle will involve optimization of operational goals with accurate NMA. This paper presented the first built material throughput model for the fuel fabrication in a commercial pyroprocessing facility by applying discrete event simulation principles. The goal was to determine how established safeguards metrics, namely, the false alarm probability, can be used for quantitative safeguardability assessment. An initial criterion was proposed that a safeguardable facility would elicit a lower number probability of false alarms while maintaining a reasonably high detection probability when comparing different facility designs. False alarms in the facility occur due to safeguards, safety, and security events. Therefore, a quantitative safeguardability assessment can yield important design information.

The material throughput model simulated fuel fabrication campaigns over a 250 day operational period for two different designs, one to maximize safeguards, the other to maximize material throughput. The main implications from the simulations are:

- Results described the physical conditions established for this study, and the model is performing as expected.
- Major system output parameters are not demonstrably different over each design. Therefore, operational goals are not affected, and the designs are essentially equivalent in terms of safeguardability.
- The simulated standard error of the inventory difference obtained for each design fell well below that calculated from the standard, mathematical relationship used for safeguards. This suggests the system could detect a diversion attempt reliably.
- The simulated standard error of the inventory difference is sufficiently low as to potentially lower the current IAEA goal for detection probability, thus offering a

less costly approach to establishing the safeguards system in the facility. It would not be prudent at this time to establish a criteria for safeguardability assessment based on the SEID because there are no current IAEA goals for the advanced fuel cycle. As this model matures, new criteria may come to light within this context.

Near-term work will focus on addressing modeling limitations, such as obtaining input data, studying failure modes for the equipment, and integrating the chemical and physical processes into the model. Further DES modeling in this way is applicable to a pyroprocessing facility due to the batch nature of subsystems processing, including transfers between subsystems, and salt recycle. Additionally, once facility data can be obtained; e.g., equipment reliability, maintenance times, etc., DES can be used to identify locations where bottlenecks will occur and material throughput is held up. This will further inform facility design by suggesting hot cell configurations where bottlenecks can be minimized, while enhancing safeguardability. With no current goals for the Type I error probability, there is wide latitude in the development of possible design strategies for a design-driven, safeguardable model for a pyroprocessing facility.

Chapter 2: Sensitivity analysis and application of advanced nuclear accounting methodologies on the high reliability safeguards model: use of discrete event simulation for material throughput in fuel fabrication

Submitted to *Nuclear Engineering and Design* and under review

2.1 Abstract

Our overall research objective has been to develop a high reliability safeguards model for a full, commercial-scale pyroprocessing facility based on the fundamental principle of safeguards-by-design. To this end, a quantitative safeguards model with the metric of false alarm probability has successfully been developed for the fuel fabrication process to the point of being useful and flexible in practical nuclear material accounting, particularly with weight measurements. Fuel fabrication was selected for study because a large amount of special nuclear material is included in this process. The current model allows for adding key measurement points (KMPs) or sub-processes, and it updates an inventory difference calculation at each KMP. A facility design (the baseline design) including a KMP between the melting and trimming processes produced much less products than the equipment design without the same KMP given the same desired false alarm probability of 0.05, which is the IAEA recommended goal. Therefore, the operator will prefer to have the equipment design to process more material while the baseline design can tell the exact location at which a diversion has attempted. In this paper, a sensitivity analysis has been developed for various facility parameters, such as false alarm probability, melter failure rate, alarm threshold at each KMP, etc., to observe how they result in the productivity of operation. With a larger false alarm probability compared to 0.05, much less material had been processed. In addition, if the melter failed more often than once per month, less material was processed. Changes related to the heel amount accumulated in the melter did not affect the number of campaigns because the model correspondingly calculates the alarm thresholds to achieve the same desired false alarm probabilities. If different false alarm probabilities were set up for the installed KMPs, then safeguards on each sub-process unit in a pyroprocessing facility would effectively be applied. In addition, the functionality of random sampling for physical or interim inventory verification was tested.

2.2 Introduction

2.2.1 Need for a New Safeguards Approach

Pyroprocessing is a promising alternative to aqueous nuclear reprocessing technologies. It extracts actinides and other fission products to reduce the toxicity of spent nuclear fuel, or recovers U/TRU for further fuel production for an advanced nuclear system. This method is a 'dry' process and adds an additional barrier to nuclear proliferation since there exists no separation of pure Pu stream [60]. Use of safeguards applied for traditional aqueous reprocessing facilities to pyroprocessing is questionable due to the following reasons: (1) The aqueous reprocessing technologies, such as the PUREX process, have the advantage of using the accountability tanks, where inventories can be recorded by sampling of homogeneous solutions by either destructive analysis (DA) or non-destructive assay (NDA). However, for pyroprocessing, special nuclear fuel is dissolved in electrolytes, and sampling the salts may not provide accurate inventory measures due to dynamic chemical processes involved and the heterogeneity of processing materials. (2) Resetting inventory is not feasible for pyroprocessing because flushing out the electrolytes containing actinides is not achievable. Therefore, implementation of distinctive, strong safeguards is imperative to detect diversion of significant quantities (SQ) of nuclear material [12] in the pyroprocessing facility. If a State attempts to divert nuclear material to create nuclear weapons, the installed safeguards regime is expected to deter this action. The following is a new approach introduced to assure robust safeguards because the previously established safeguards for aqueous reprocessing facilities, considering traditional fuel types, are not suitable anymore.

2.2.2 Safeguards-by-design Modeling Approach

One such approach to the pyroprocessing facility is to apply the principles of safeguards-by-design, also often referred to as safeguardability. We use these terms interchangeably in this paper. Safeguards-by-design seeks to integrate safeguards, safety, and security as a facility design strategy. A safeguards-by-design approach is practical to apply safeguards features into the nuclear facilities at the early stage of process design [61]. It helps to determine where proper safeguards activities must be performed relevant to potential plant designs, brings economic incentives reducing the capital costs of design features and safeguards implementation, and facilitates effective international safeguards implementation [62]. In fact, the Korea Atomic Energy Research Institute

(KAERI) has addressed the application of the safeguards-by-design concept to a pyroprocessing facility [46]. The safeguards-by-design approach is readily applicable to a commercial pyroprocessing facility because one has not yet been built, nor are there any formalized International Atomic Energy Agency (IAEA) goals for its safeguards. This allows for a broad latitude in formulating design approaches to model a safeguardable facility. To this end, the High Reliability Safeguards (HRS) methodology addresses the safeguardability of advanced fuel cycle concepts, in this case, for a pyroprocessing facility [5], [6]. HRS focuses on approaches to safeguardability that are design-driven. The fundamental principle is to offer design approaches to pyroprocessing facilities that can readily accommodate the application of IAEA safeguards.

Since there is no experience operating a commercial-scale pyroprocessing facility, applying the principles of safeguardability is pragmatic to optimize system designs. Therefore, Lee et al. [63] presented the first-build of a model based on the safeguards-by-design concept that includes material throughput and is flexible in terms of accommodating multiple facility designs, where each can be tested in terms of safeguardability. The fuel fabrication process was modeled because this contains the highest content of special nuclear material (SNM) in the system. The Type I error [11] is used as a preliminary means of safeguardability quantification. Currently, the model focuses on application of traditional nuclear material accounting (NMA) concepts, but the long-term vision is to model a full pyroprocessing system and add corresponding NDA and DA methods for individual sub-processes. These techniques will be developed into the model as it progresses.

2.3 Background

2.3.1 Traditional NMA Methodologies used for Reference Safeguards

The international safeguards placed on the Rokkasho reprocessing plant, under the Nuclear Non-Proliferation Treaty and Additional Protocol, can be a reference for safeguarding future reprocessing plants [64]. Its accountancy structure has been implemented by dividing the facility into several different material balance areas (MBAs) [65]. The monthly interim inventory verification (IIV) and the physical inventory verification (PIV) apply a statistical random sampling of vessels containing SNM. Besides, based on the conceptual design of the Advanced Fuel Cycle Facility (AFCF), Durst et al. [64] suggests that PIV is planned to randomly verify fuel defects for the spent fuel storage,

and mass balance monitors SNM movement throughout the facility operation.

2.3.2 Non-destructive Assay, Destructive Assay, and Advanced NMA Methods

Although implementation of NDA or DA is not applied to the current model yet, we have suggested its conceptual approaches in advance, which will be useful for further developing the safeguards model for the full-scale pyroprocessing facility. We have determined DAs for the completely processed fuel rods in the product storage, part of fuel fabrication [63], and specific KMP locations for NMA using $^{244}Cm/Pu$ ratio and neutron coincidence counting, weight measurement, etc. We concluded that some DAs may be necessary given the operational deviations derived by the hazard and operability (HAZOP) analysis for head-end processes [66]. However, frequent DA of nuclear material may affect the facility operation goal by adding time lags, which may affect the overall process efficiency [67]. In addition, NDA of neutron coincidence counting might not fit for electrorefining due to the heterogeneity of materials, and different Pu/Cm ratios in the salt and cathode deposit [45] although experimental verification is needed. While neutron coincidence counting might still be useful [64], [68], some advanced NMA methods such as process monitoring, near-real-time accounting (NRTA), or signature based safeguards [67], [69] can also compensate drawbacks of traditional NMA. For instance, real-time process monitoring considers process data, such as cell current and cathode potential, to monitor cathode deposition and Pu in the salt [70].

2.3.3 Application of Various NMA Methods for Safeguardability in Fuel Fabrication

Here, we turn to the fuel fabrication process. Our current model includes KMPs, which can physically measure material weights. Other traditional NMA methods introduced as the reference safeguards approach in Section 2.3.1 are also built into the model. In addition, NDA might be possible for the homogeneous U/TRU metal, and DA may be useful with the processed fuel pellets (details about these are shown in Section 2.3.2). Since only physical changes of nuclear material are expected in the fuel fabrication process (unlike head-end processes, which involve complex chemical changes), traditional NMA methods were applied to develop the first framework of the safeguards model. NRTA was also used to reduce extensive reporting of inventory changes [71]; a frequent,

sequential evaluation of ID is calculated upon KMP locations.

2.3.4 Advantages of a New, Particular Safeguards Model designed for Fuel Fabrication

There have been substantial pyroprocessing process modeling studies on head-end processes, particularly for electrorefining [44], [45], [60], [67], [72], [73], [74], [75], [76], which tend to be proprietary and not accessible to the research community at large. While the bottom-up perspective models are to estimate material amount in a specific unit, our model provides NRTA of material transfer throughout the operation, incorporating fundamental concepts of safeguardability with a risk-informed approach. Quantification of risk within the context of safeguardability is a unique feature, and it will facilitate the eventual licensing process and the facility safety analysis. The importance and relevance of our model to the field is in terms of supplementing traditional nuclear material control and accounting measures to improve performance of the safeguards system.

2.4 Theoretical Concepts applied to the Model

2.4.1 Nuclear Material Accountancy

NMA is a conventional safeguards method for tracing nuclear material flow in facilities. With defined MBAs in the facility, changes in the nuclear material quantities within specific periods are recorded [12]. Herein, multiple MBAs are useful to organize separate activities in a bulk handling facility, and KMPs are at which nuclear material can be measured to determine material flow or inventory. Figure 2.1 and Figure 2.2 show the general overview of implementation of MBAs, and our model applies fundamental NMA principles using different facility designs shown in Figure 2.3.

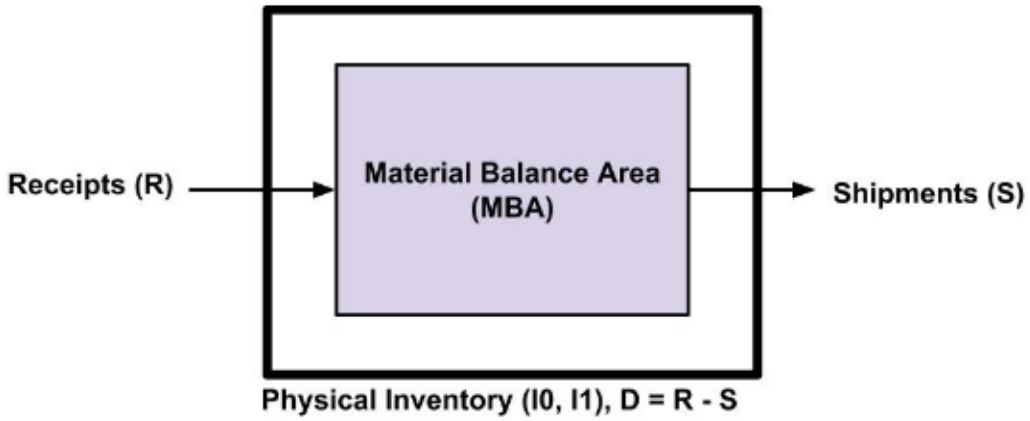

Figure 2.1: The material balance concept. A material balance area can be defined around one or multiple subprocesses. The material throughput (D) is calculated by subtracting the receipts (R) by the shipments (S). The initial inventory (I_o) and the final inventory (I_1) are used to calculate ID for a MBA containing inventories.

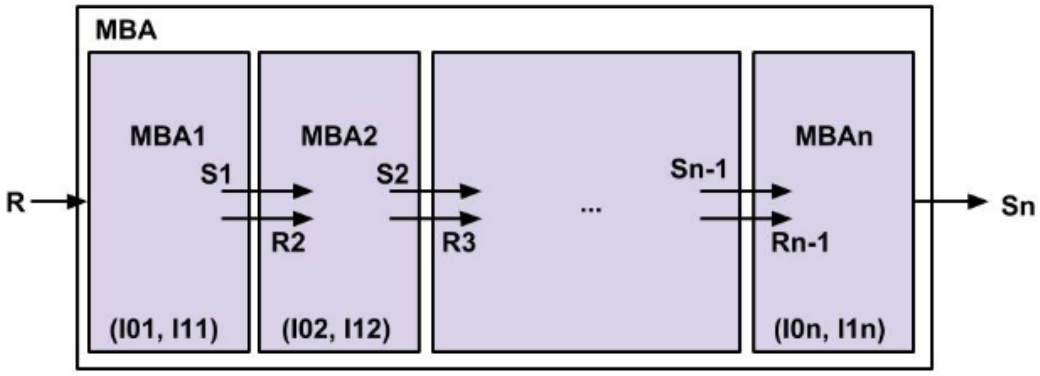

Figure 2.2: Subdivision of material balance areas. Accumulated sequential IDs get compared with the alarm threshold of 2.4 kg every campaign. If the accumulated data is above the threshold, an alarm is raised, and the operation stops. The current model does not involve material transfer yet after the alarm rise, but it stops the facility operation. MBAs storing inventories are excluded for this calculation, and only mid-processes get accounted for.

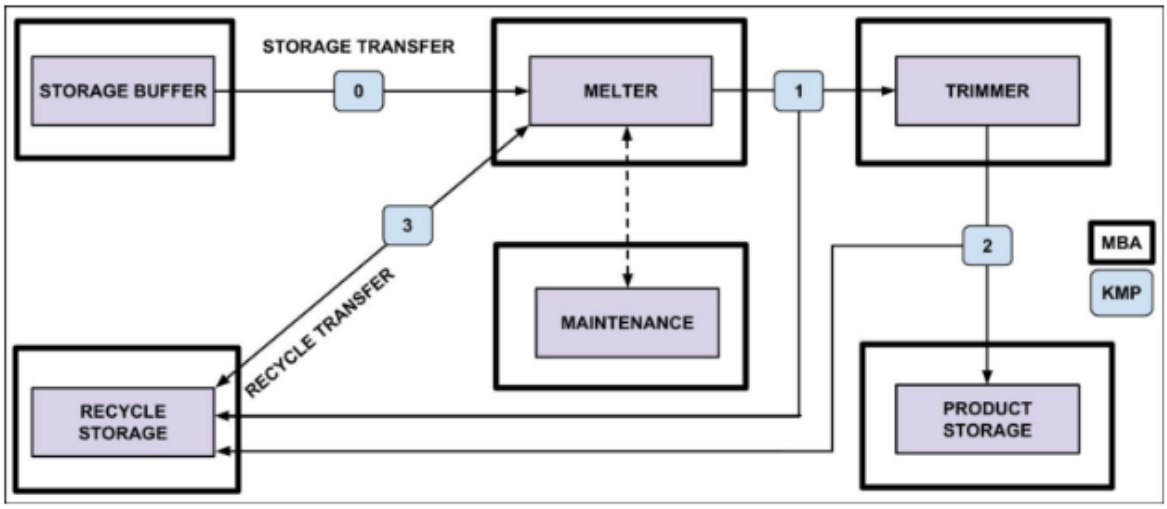

Figure 2.3a

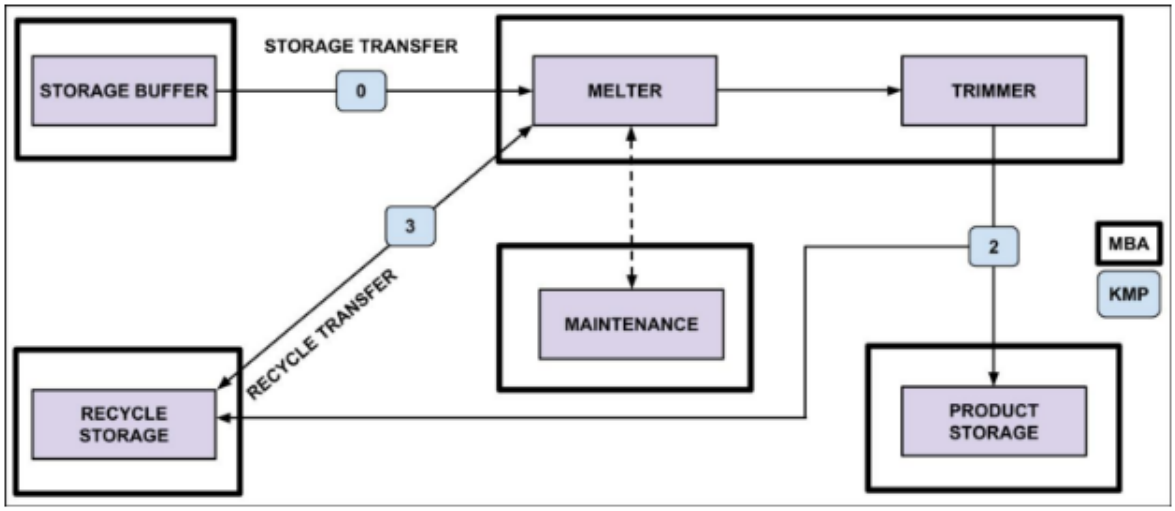

Figure 2.3b

Figure 2.3: DES modeling framework for fuel fabrication.

Baseline Design: A MBA is installed for each sub-process, and a KMP is located right after every process. Only weight measurement is performed at KMPs, and ID can be calculated by subtracting the measured batch weight at the previous KMP by the measured batch weight at a current KMP. The solid arrows represent material flows while the dashed arrow is for handling material in the planning phase. Now, no material gets moved to the MBA installed around maintenance. If the melter fails, both the batch and the heel are moved to the recycle storage. At KMP3, ID can be calculated in two different ways since the material might be going towards the recycle storage, or it may be heading back to the melter. Additionally, if ID at each KMP is above a threshold, the material is moved to the recycle storage for further testings.

Equipement Design: Only one MBA is installed around both the melter and the trimmer. KMP1 previously installed between the melter and the trimmer is removed, and other conditions follow the same as ones that are for the baseline design.

2.4.2 Inventory Difference and False Alarm Probability

Material balance evaluation is imperative to assure if there exists a possible missing material, and this works only with bulk material handling processes [12]. If the beginning inventory and the material throughput during a period are equal to the ending inventory, which is an ideal case, ID must be zero. However, due to uncertainties in measurements or material losses, actual ID values would seldomly be zero in reality [77]. ID is defined as Equation 2.1 below [11], [12], [78], [79].

$$ID = I_0 + D - I_1, \tag{2.1}$$

where I_0 = beginning physical inventory at $t = t_0$, I_1 = ending physical inventory at $t = t_1$, D = material throughput across the material balance area over a given time period. This is depicted in Figure 2.1. Herein, we apply statistical concepts to prove if the concept of a false alarm probability can be used as a quantitative metric for implementation of safeguards on a metallic fuel fabrication facility. ID can be compared with an alarm threshold to raise a false alarm [79]. The alarm limit can be $n\bar{\sigma_{ID}}$, where n is the desired false alarm rate, and $\bar{\sigma_{ID}}$ is a good estimate of σ_{ID} [78], [80]. The false alarm rate can be obtained from z-values listed in the z-table constructed for a normal distribution [81]. We assume a Gaussian distribution of ID values, and without a material loss, $ID \sim N(0, \sigma_{ID})$, which represents the normal distribution of ID values

with mean of '0' and standard deviation of σ_{ID}.

The concept of 'propagation of error (variance)' is applied to determine the expected ID uncertainties [79]. Our model covers two cases for the expected ID uncertainty calculation; a MBA with a random material loss or without random losses. Before the calculation of 'propagation of error,' both 'random' and 'systematic' errors must be considered to bring precise combined standard uncertainties for weight measurements. Since these two input values do not affect each other, their covariance becomes zero. Therefore, the combined standard deviation can be calculated by Equation 2.2 [82], [83], [84], [85].

$$\begin{aligned} {\sigma_c}^2 &= {\sigma_r}^2 + {\sigma_s}^2 \\ \sigma_c &= \sqrt{{\sigma_r}^2 + {\sigma_s}^2}, \end{aligned} \tag{2.2}$$

where σ_r = random error, and σ_s = systematic error. Here, Zhao et al. [85] proposes the relative random and systematic uncertainties in the unit of percentage for bulk mass measurement. They are given as 0.05% using an electronic balance or a load-cell based weighing system. Thus, a combined uncertainty for the weight measurement performed at a specific KMP can be calculated and applied to the model given an unique batch weight.

Assuming that a batch is passed through the MBAs determined for the melter and the trimmer, and no materials get stored in them (in other words, there are no inventories at the beginnings and the ends of time intervals), $ID = D$ since I_0 and I_1 are equal to zero. The model calculates ID at the KMPs installed before and after the process in a MBA (Figure 2.1). In other words, ID is calculated by subtracting material receipts by removals. Now, if no material loss is assumed in a MBA, Equation 2.1 can be simplified as below.

$$ID = R\ (receipts) - S\ (shipment) \tag{2.3}$$

Therefore, the error propagation can be calculated by

$$\begin{aligned} {\sigma_T}^2 &= {\sigma_R}^2 + {\sigma_S}^2 - 2\sigma_{RS} \\ \sigma_T &= \sqrt{{\sigma_R}^2 + {\sigma_S}^2 - 2\sigma_{RS}}, \end{aligned} \tag{2.4}$$

where σ_R = measurement error from a batch receipt, σ_S = measurement error from a batch shipment, and σ_{RS} = covariance between two random measurements. Now, σ_{RS} is equal to zero because the receipt and shipment measurements are independent

events. Consequently,

$$\sigma_T = \sqrt{{\sigma_R}^2 + {\sigma_S}^2} \tag{2.5}$$

If there is a material loss due to hold-up materials, ID can be calculated by Equation 2.6.

$$ID = R\ (receipts) - S\ (shipment) - \Delta\ (material\ loss). \tag{2.6}$$

We also treat R, S, and Δ to be independent random variables [11], and a material loss can be estimated from precedent engineering studies. Therefore, the error propagation is shown in Equation 2.7.

$$\sigma_T = \sqrt{{\sigma_R}^2 + {\sigma_S}^2 + {\sigma_\Delta}^2}, \tag{2.7}$$

where σ_Δ = uncertainty associated with a material loss. Therefore, the model calculates the expected uncertainties of ID using Equation 2.5 and Equation 2.7 [78], and different false alarm rates process various amounts of products at the end of one year operation.

'Type I error' states that there exists a missing nuclear material; in fact, no diversion has occurred [11]. In statistical term, the null hypothesis, $H_0 : E(ID) = 0$, is assumed to be true, and its rejection occurs. The probability of this rejection is represented as a false alarm probability (α) shown in Equation 2.8.

$$\alpha := prob\ \{ID > s \mid H_0\}, \tag{2.8}$$

where the significance threshold(s) can be an expected uncertainty ($\bar{\sigma_T}$) or a multiple of it. The significance level (α) is usually set at 0.05 (5%) or less, and the confidence level ($1 - \alpha$), which represents the probability of containing the true value of a statistical parameter, is expected to be 0.95 (95%) or more [12]. In case of 'Type II error', no diversion is indicated while an actual diversion has occurred. A non-detection probability (β) indicates that the alternative hypothesis (H_1) is not true; in fact, it is true. The alternative hypothesis is defined to be $H_1 : E(ID) = M$, where M is the amount assumed to be missing. The non-detection probability is described as

$$\beta := prob\ \{ID \leq s \mid H_1\}, \tag{2.9}$$

Detection probability ($1 - \beta$), false alarm probability, amount (M) assumed to be diverted, and standard error of ID establish a relation derived below (Equation 2.10).

$$\Phi^{-1}(1 - \alpha) + \Phi^{-1}(1 - \beta) = \frac{M}{\sigma_{ID}}, \tag{2.10}$$

where Φ^{-1} is the inverse Gaussian function. The significance threshold (alarm threshold) can also be set up as one significant quantity (SQ) of SNM. One SQ is the amount of nuclear material for which the possibility of fabricating a nuclear weapon can not be disregarded [12]. Particularly, for Pu, one SQ is 8 kg. In this case, with the detection probability of 0.95 and the false alarm probability of 0.05, the standard deviation of inventory difference of 2.4 kg is allowed based on Equation 2.10.

Sequential IDs can also be accumulated throughout the facility (Figure 2.2). A physical count of the vessels containing nuclear material takes a large amount of time to investigate the whole facility. Therefore, for frequent calculation of accumulated sequential IDs, MBAs installed around physical inventories are excluded due to the time constraints. When $E(Si) = E(R_{i+1})$ for $i = 1, \cdots, n-1$, addition of sequential IDs can be represented as

$$\Sigma_{i=1}^{n} ID_i = \Sigma_{i=1}^{n} I_{0i} + R_1 - S_n - \Sigma_{i=1}^{n} I_{1i}, \tag{2.11}$$

where R_1 is the initial receipts of the first MBA, and S_n is the final shipments of the last MBA [11]. For the MBAs across the melter and the trimmer, physical inventories are equal to zero ($I_{02}, I_{12}, I_{03}, I_{13} = 0$). In reality, KMPs must be installed in front of the storage buffer and after the product storage to measure R_1 and S_n. However, as mentioned before, physical inventory terms are not considered for frequent calculation of accumulated sequential IDs. Therefore, individual inventory differences are simply added and compared with the alarm threshold to prevent nuclear diversion attempts.

$$\Sigma ID = ID_1 + ID_2 + ID_3 + \cdots \tag{2.12}$$

2.4.3 Physical Inventory and Interim Inventory Verification

Inventories likely contain large quantities of nuclear material, and the IAEA inspectors might have to select a sample size of the population rather than measuring and counting all the sealed containers in the storages. For PIV and IIV, the sample size, which can represent properties of all items in a population, is determined using Equation 2.13 under the principle of 'random sampling' [12].

$$n = N(1 - \beta^{\frac{x}{M}}) \tag{2.13}$$

where N is the total population, and $\bar{x}$ is the average weight of items. A significant quantity of 8 kg of Pu is used for M, and the detection probability (1-β) is 0.95. The selected samples will be used for further DA or NDA tests.

2.5 Model Description

The model initially developed in Lee et al. [63] is based on a discrete event simulation (DES) framework. The concept of DES was initially applied to the model because sub-processes in the pyroprocessing facility are batch-type, and material transfers are performed in bulk form. A DES model monitors operations as a discrete sequences of processes. NRTA is incorporated through the use of a DES model, which involves nuclear accounting techniques applicable during operation without the facility shutdown and cleanout [86]. Measurements are currently only performed on the KMPs. In this work, the model has undergone more sophisticated upgrades in order to incorporate the design principles inherent in the concept of safeguardability. See Section 2.7 for the upgrades.

2.5.1 Fuel Fabrication Description

Understanding the fuel fabrication sub-processes is necessary to specify KMP locations and MBAs for developing a safeguardability model. This is discussed in detail in Lee et al. [63] and briefly summarized here to provide context. We have assumed that metallic fuel slugs are fabricated by injection casting. Injection casting first melts ingots of nuclear material in a crucible. Next, quartz molds are inserted into the homogeneously mixed molten metal alloy, and a vacuum is induced to draw the molten material into quartz molds. Some material may remain in a crucible, and it is called the 'heel.' Metal slugs are then produced through the trimming process by shearing and breaking the molds. Finally, in our model, the fuel slugs are stored in a product storage buffer. In the full commercial-scale facility, the slugs would be transferred for subsequent processing into fuel rods.

2.5.2 Object-oriented Programming

A major upgrade to the model involves the application of object-oriented programming. Figure 2.4 shows hierarchical inheritance of the safeguards model. Its architecture is described here as part of the current work. Object-oriented principles follow well

with batch-type processes and the DES modeling framework since an object created by a class can accept a batch, act on it accordingly, and pass it to the next object. Multiple subclasses inherit the properties and behaviors from a base class [87], [88], [89]. In our model, a facility command module controls the logic flow of the program run. It creates its own objects and modifies the material flow by accessing other classes' attributes and behaviors. For instance, there exist subclasses defined for sub-processes in a fuel fabrication facility, which correspond to each vertex: storage buffer, melter, trimmer, product storage, and recycle storage. Now, in the current work to upgrade the model, one facility command class controls the full material flow. In this case, any sub-processes or KMPs can simply be implemented or discarded. The base class is called the facility component class, which carries the functions to check if the melter failed or not, to log the material flow and increment the operation time. It also initializes a data output object to record the output data in a certain format. These inclusive functions are inherited by other subclasses.

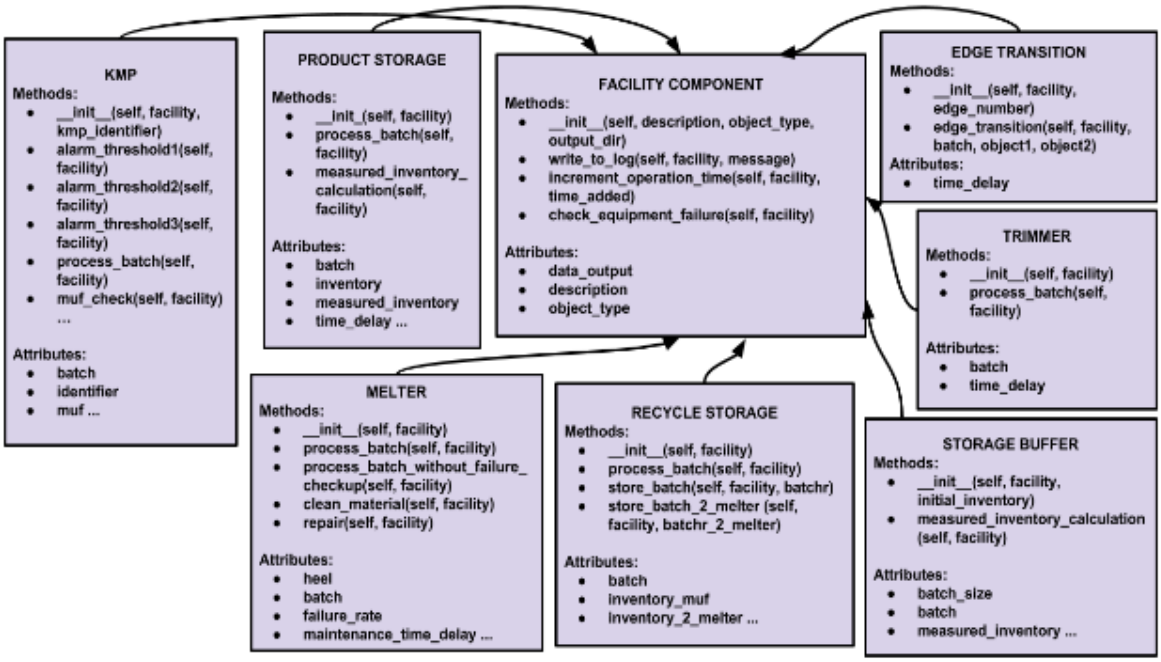

Figure 2.4: Architecture of hierarchical inheritance. Other than subclasses for sub-processes in the fuel fabrication process, the key measurement point class and the edge transition class also inherit functionalities from the facility component class. Major methods and attributes for each class are described above.

2.5.2.1 Key Measurement Point

Several 'alarm threshold' functions are defined in the KMP class because the expected standard deviation is individually calculated at each KMP to adhere the false alarm probability; i.e., changing the physical values for the relative random and systematic errors associated with weight measurements does not influence the desired false alarm probability. We prescribe a false alarm probability of 0.05 in the model, in line with current IAEA safeguards goals [12]. Though, users can easily change the false alarm probability by modifying the false alarm rate. The KMP class also includes functions for ID calculation given different KMP identifiers.

2.5.2.2 Other Major Functions and Variables

Overall 'process batch' functions process a batch corresponding to sub-processes' purposes. The edge transition class moves a batch from vertex to vertex. The trimmer does not include any physical changes of SNM, and only weight measurements are performed before and after this process. 'Store batch' functions defined in the recycle storage class are for storing material. The batch and the heel might move back to the melter after maintenance while some transferred material due to a false alarm must be stored in the recycle storage temporarily for further inspection. Although 'measured_inventory' for the recycle storage does not get updated (only needed for inventory verification in future), its true inventory data is logged when the material comes in. Currently, the functionality of measuring inventories is successfully applied for both the storage buffer and the product storage.

2.5.3 Model Space

In the model space, we assume a single batch of nuclear material. In DES parlance, the model consists of five vertices: (1) storage buffer, (2) melter, (3) trimmer, (4) product storage, and (5) recycle storage. A batch passes through each vertex, and KMPs perform measurements to determine material flow. Hold-up material exists in the melter, and it is treated as a material loss. We currently assume there is no material loss in the trimmer. The false alarm probability is applied using the ID calculation with the mean of '0' given that the amount of heel is accounted for [90].

2.5.4 Baseline Design and Equipement Design

Consequently, our model addresses two conceptual facility designs with different KMP locations and MBA specifications. Figure 2.3a and 2.3b show the 'baseline design' and the 'equipment design,' respectively. The baseline design includes KMP 0, 1, 2, 3 and five different MBAs installed around storage buffer, melter, trimmer, product storage, and recycle storage. In case of the equipment design, KMP1 is removed, which means only one MBA is proposed for both the melter and the trimmer. The current model adds the functionality of ID calculation at each KMP while the previous version only calculates IDs at the ends of campaigns.

2.6 Module Characterization

The model includes the input parameters based on prior study. Due to non-existence of a commercial-scale pyroprocessing facility and a lack of historical engineering-scale experiments, some parameters are assumed reasonably based on engineering judgement. We assume that the facility operates about 250 days per year with a capacity factor of 0.7 [55]. One campaign is completed when a batch is passed from the storage buffer to the product storage or the recycle storage. Table 2.1 shows the input parameters used for the simulations, and they are very similar to the previous values provided by Lee et al. [63].

Table 2.1: Input parameters used for the simulations

Input parameter	Value
Batch size	20 kg
Total operation time	250 days
Melter failure rate	1/30 day^{-1}*
Expected heel weight	250 g*
True heel left in the crucible	250 g $\pm$ σ (standard deviation)*
KMP measurement time	30 min
Batch preparation time (storage buffer)	1 h
Melter operation time	8 h
Trimmer operation time	3 h
Product storage operation time	2 h
Recycle storage operation time	2 h
Maintenance time after every campaign or due to melter failure	4 h
Melter cleaning time	2 h

*These values vary for corresponding sensitivity analyses. Section 2.7 shows different input parameters used to observe different output data trends such as changes in the amount of processed material.

2.6.1 Inventory Difference

A 20 kg batch is prepared in the storage buffer, and is passed to the KMP point to measure its weight before going into the next vertex (sub-process). The current model inspects ID at each KMP. KMP 0 does not calculate ID due to unknown information of how the receipts for the storage buffer will be performed. When a false alarm is raised because an ID is above the alarm threshold, the material is directly transferred to the recycle storage. When the melter fails, the batch and the heel are combined, and moved to the recycle storage. KMP 3 calculates ID whenever the material is passed between the melter and the recycle storage. When its discrepancy is above the alarm threshold, even after the melter is fixed, in this case, a new batch is prepared at the storage buffer, and the previous batch is stored in the recycle storage. Heel is removed from the melter every campaign so that the concept of 'propagation of variance' can be applied. After accumulating sequential IDs in the whole facility, this is compared with the typical IAEA goal of 2.4 kg, and if an alarm is raised, then the operation stops.

2.6.2 State Variables

The state variable is the 'true weight' of material, and in reality, this value is never known. The model accounts for 'expected', 'measured' weights not only the 'true' values. The previous model calculates measured weights by adding uncertainties on the true weights. Now, 'measured' values are calculated by adding uncertainties on the 'expected' weights for application of the ID calculation with the mean of '0' and the standard deviation obtained by propagation of error. True weight of the batch is still updated by true weight loss from heel left in the crucible.

The real data for individual uncertainties from KMP measurements and material losses, is still needed. However, at the present stage, because the false alarm rates are set in order to maintain the desired false alarm probabilities, future changes on uncertainty values given the same facility input parameters shown in Table 1 would not affect the material throughputs.

2.6.3 Melter

Heel stored in the crucible is cleaned out every campaign. The true weight is 250 ± 100 g, and the expected batch weight is 19.75 kg after the melting process. Failure check is performed for this process, and the failure routine is called when the melter fails. Melter failure is nominally modeled assuming that the failure rate is constant with time (in other words, equipment wear is neglected.) The Weibull distribution is a widely known probability density function (pdf) of a Weibull random variable, and its cumulative density function (cdf) provides the cumulative probability of equipment failure before a specific time [57]. Since the shape parameter (k) is assumed to be 1, the pdf is represented as the exponential distribution shown in Equation 2.14.

$$f(t) = \lambda e^{-\lambda t},\ t \geq 0, \tag{2.14}$$

where λ = rate parameter, and t = facility operation time. Herein, the concept of the Monte Carlo method, which repeats random sampling to draw numerical solutions, is applied to check if the melter failed or not. If a randomly generated number between 0 and 1 is less than or equal to the cdf value at a specific operation time, then the melter failed (Equation 2.15).

$$F(t) = 1 - e^{-\lambda t},\ t \geq 0, \tag{2.15}$$

Also, whenever the melter fails, maintenance and the cleaning process are required.

2.7 Results and Discussion

The simulation setup file created the corresponding input/output files in particular directories. Input files in the library directory were adjusted to change facility operation parameters before running the simulations. The execution file has been developed to run total 1000 simulations of a 250-day operation because 1000 simulations are large enough to achieve the convergence in the output data. The model was tested with desired false alarm rates (false alarm probabilities), different KMP locations, measurement error changes, particular melter failure rate parameters, and different heel amounts.

Upgrades on NMA include ease in adjusting KMP locations, ID calculation performed at each KMP, and accumulation of sequential IDs every campaign. The alarm threshold was set as 2.4 kg for total sequential IDs (from every campaign), and the operation stopped when they exceeded the threshold. Two different facility designs were tested to assess safeguardability of each, and they both had different numerical values for alarm thresholds at KMPs to keep the same false alarm probability of 0.05 at each KMP and overall. For instance, KMP 2 from the baseline design did not account for the uncertainties due to material losses since they were neglected for the trimming process. However, with the equipment design, KMP 2 accounted for the material loss from heel since one MBA was installed for both the melter and the trimmer. Using the false alarm rate of 1.645 provided the false alarm probability of 0.05.

2.7.1 Measurement & Inventory Difference Calculation (Unit Testing)

Before actual functions for ID calculation were added to the KMP class, the unit testings were performed to verify if the concept of propagation of error can be successfully applied to bring the desired false alarm probabilities. The weight measurement of a batch includes both the random and systematic errors. Since 0.05% of 20 kg (a batch weight) was assumed to be a random or systematic error (0.01 kg), the combined standard deviation was calculated as 0.014 kg. Figure 2.5 shows how the measured weights varied with the mean of 20 kg and the standard deviation of 0.014 kg. Figure 2.6 shows the heel weight variation with the mean of 0.25 kg and the standard deviation of 0.1 kg. By using Equation 2.5 and 2.7, distribution of IDs at a KMP with a material loss from heel and that without material losses are shown in Figure 2.7. Here, the alarm thresholds were set different for ID calculation to keep the false alarm probability of 0.05 each.

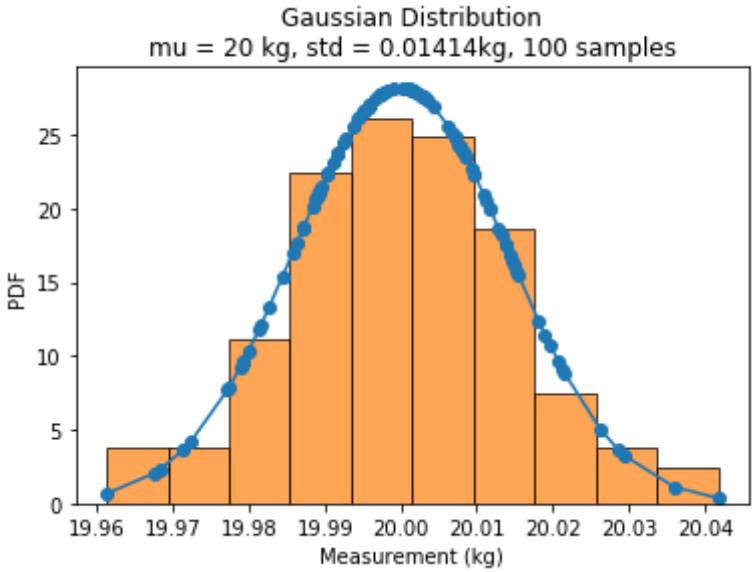

Figure 2.5: Gaussian distribution of weight measurements. A Gaussian distribution was used to generate the randomly measured weights at any KMPs. This graph visualizes how the measured weights varied at KMPs given the mean of 20 kg and the standard deviation of 0.014 kg. The mean weights may be different from 20 kg depending on KMP locations, especially if there is a material loss before the measurement. Also, in reality, the relative random and systematic errors may be much larger than 0.05%.

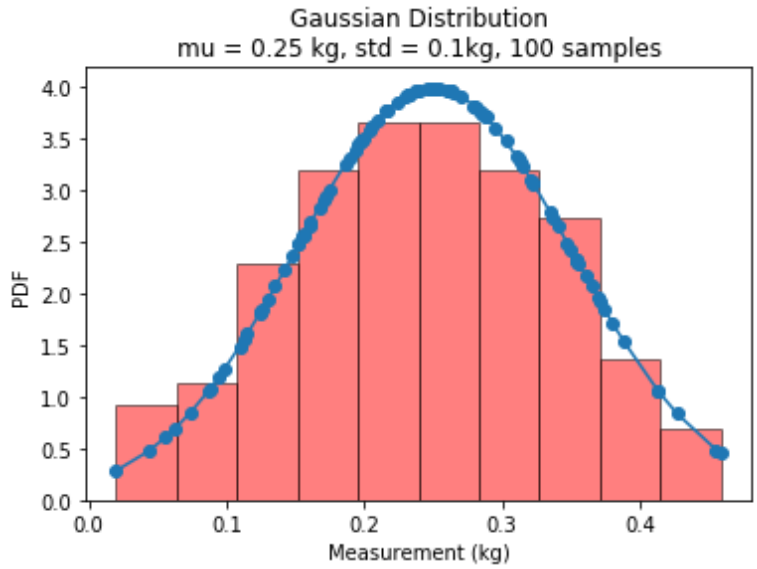

Figure 2.6: Normal distribution of heel amounts. A normal distribution was assumed for a heel left in the crucible. The mean of 0.25 kg and the standard deviation of 0.1 kg were used. The heel amount was modified to verify if the model can maintain the desired false alarm probabilities.

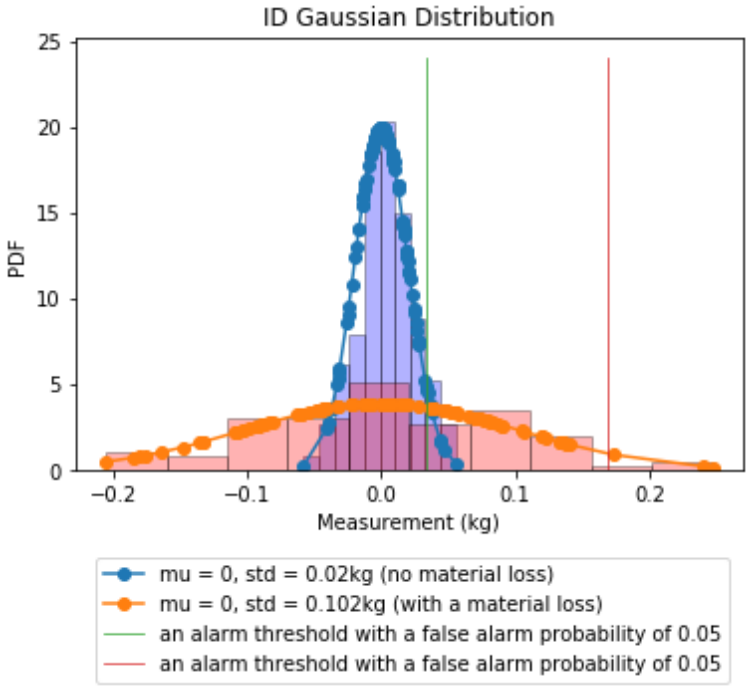

Figure 2.7: Normal distribution of IDs. The mean for ID values is 0, and the standard deviation is 0.02 kg with no material losses, or 0.102 kg if the material loss is accounted for.

2.7.2 Melter Failure

The cumulative density function using the failure rate parameter of 1/30 days for 50 days is shown in Figure 2.8. In the actual model, whenever the melter fails, the old equipment was swapped with a new equipment, which means that the cdf discarded the accumulated failure probability of the old melter and was reset for a new equipment. When the operation time increases, the cumulative probability of melter failure increases as shown by Equation 2.15.

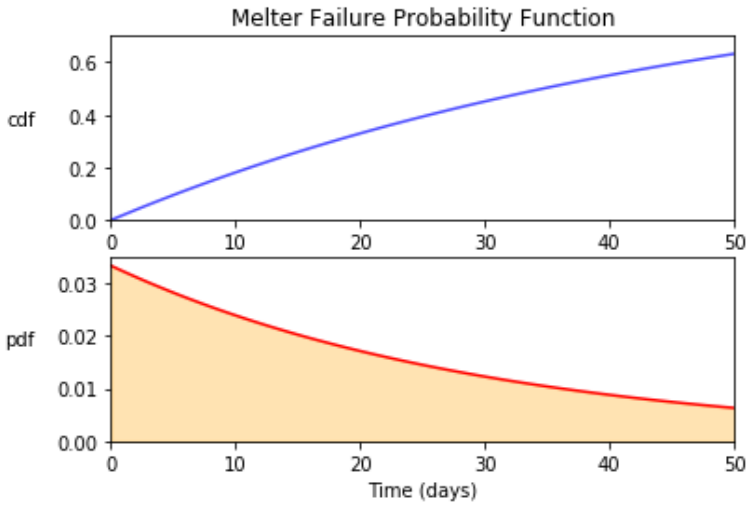

Figure 2.8: The probability density function and the cumulative density function for melter failure. As the operation time increases, the equipment is likely to fail.

2.7.3 Baseline Design vs. Equipment Design

While the previous model calculated ID only at the end of campaign, now it happens at every KMP. The false alarm probability of 0.05 was used for both designs, however, the equipment design processed more material than the baseline design. When KMP 1 was removed, less material was passed to recycle storage, therefore, more products were stored in the product storage (Figure 2.9a).

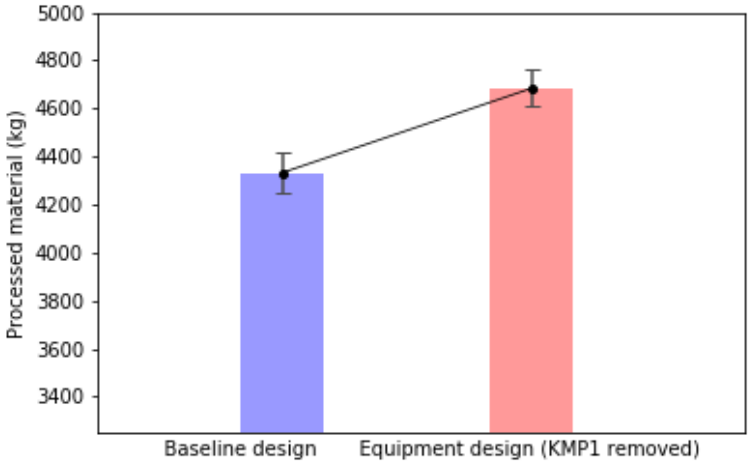

Figure 2.9a: The baseline design processes the product of 4332 ± 81.8 kg while the equipment design processes 4684 ± 75.5 kg. Equipment design can process more of 350 kg compared to the baseline design with the same false alarm probability of 5% at each KMP.

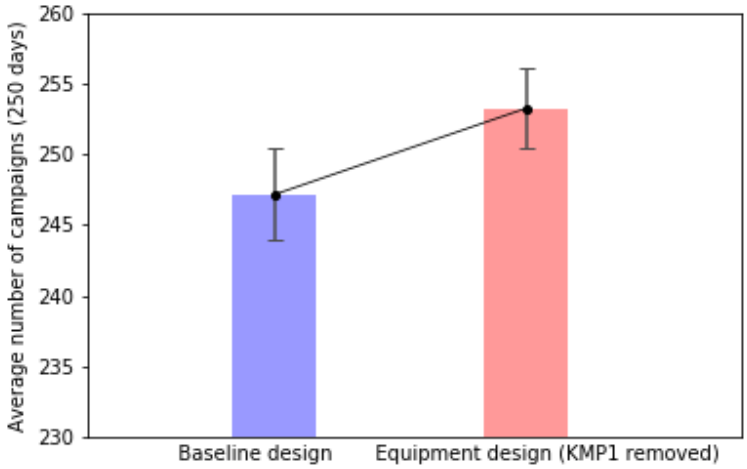

Figure 2.9b: The average number of campaigns is 247 ± 3.2 for the baseline design while that for the equipment design is 253 ± 2.8.

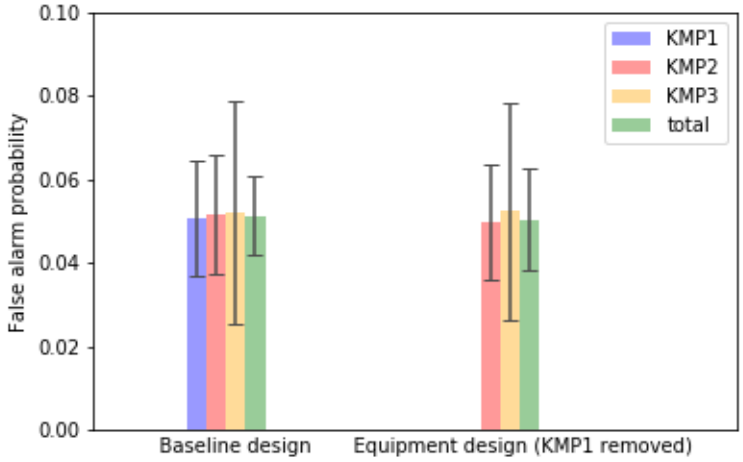

Figure 2.9c: For both the baseline design and the equipment densign, the mean of false alarm probabilities obtained from simulation at each KMP stays around 0.05.

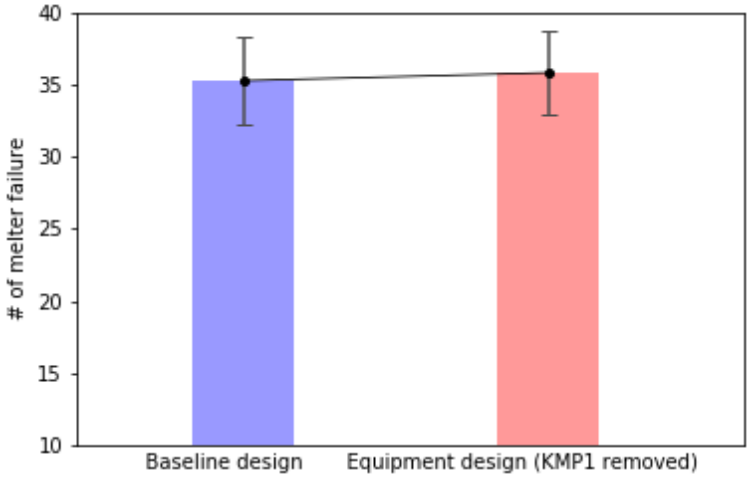

Figure 2.9d: The average total numbers of melter failure during the operation time are 35 and 36, respectively, for the baseline design and the equipment design. Both standard deviations are about 3 times.

Figure 2.9: Baseline design vs. Equipment design

The equipment design processed 350 kg more material. By having the same false alarm probability, which is a fairly strong safeguardable standard that IAEA recommended, more than 17 batches were passed with the equipment design. Therefore, the equipment design would be beneficial to optimize the operational goal, which is to maximize

material throughput, and at the same time, a reasonably safeguardable design can be implemented. Both designs are safeguardable in terms of the false alarm probability, and the operator will prefer to have the equipment design to process more material while the baseline design can exactly tell where a diversion had been attempted. At this point, KMP locations for a commercial-scale fuel fabrication facility will be determined by the negotiation between IAEA and a State. Figure 2.9b shows the average numbers of campaigns for both designs, and the equipment design passed more campaigns since material transfer scenarios without KMP1 introduced less average operation time to complete a campaign. Individual false alarm probabilities and the overall false alarm probabilities are shown in Figure 2.9c. We concluded that functionalities for ID calculation were appropriately incorporated into our safeguards model because all these false alarm probability values were fairly close to 0.05. The uncertainty associated with KMP3 was larger than those at other KMPs, and it may be due to a small sample size. Table 2.2 contains the actual output data. Additionally, the total numbers of melter failure for the baseline design and the equipment design were relatively similar (Figure 2.9d), which represents that facility designs do not interfere melter failure.

Table 2.2: False alarm probability output

Baseline design vs. equipment design

	KMP1	KMP2	KMP3	Total
Baseline design	0.05054 ±0.01367	0.05152 ±0.01438	0.05206 ±0.02660	0.05115 ±0.009341
Equipment design	-	0.04983 ±0.01386	0.05222 ±0.02609	0.05033 ±0.01201

False alarm probability variation

False alarm rate	KMP1	KMP2	KMP3	Total
1.28	0.1004 ±0.01870	0.1035 ±0.01938	0.1058 ±0.03569	0.1024 ±0.01260
1.44	0.07433 ±0.01642	0.07742 ±0.01771	0.07850 ±0.03335	0.07615 ±0.01129
1.645	0.05054 ±0.01367	0.05152 ±0.01438	0.05206 ±0.02660	0.05115± 0.009341
2.05	0.02014 ±0.008886	0.02055 ±0.009321	0.02046 ±0.01687	0.02037 ±0.006063
2.33	0.009891 ±0.006525	0.009757 ±0.006415	0.01001 ±0.01208	0.009844 ±0.004262

Individual false alarm probability at each KMP

Relative measurement error (%)	KMP1	KMP2	KMP3	Total
0.05	0.05054 ±0.01367	0.05152 ±0.01438	0.05206 ±0.02660	0.05115 ±0.009341
0.1	0.05967 ±0.01468	0.2125 ±0.02745	0.2260 ±0.05352	0.1445 ±0.01461

*These values vary for corresponding sensitivity analyses. Section 2.7 shows different input parameters used to observe different output data trends such as changes in the amount of processed material.

2.7.4 False Alarm Probability Variation

By modifying the false alarm rates, the baseline design was used to observe how much material can be processed and stored in the product storage for each case. It was also to verify if the results would match with the desired false alarm probabilities and to check if melter failure probabilities would stay the same. Figure 2.10a shows that less materials were processed when more false alarms were raised given the higher false alarm probabilities.

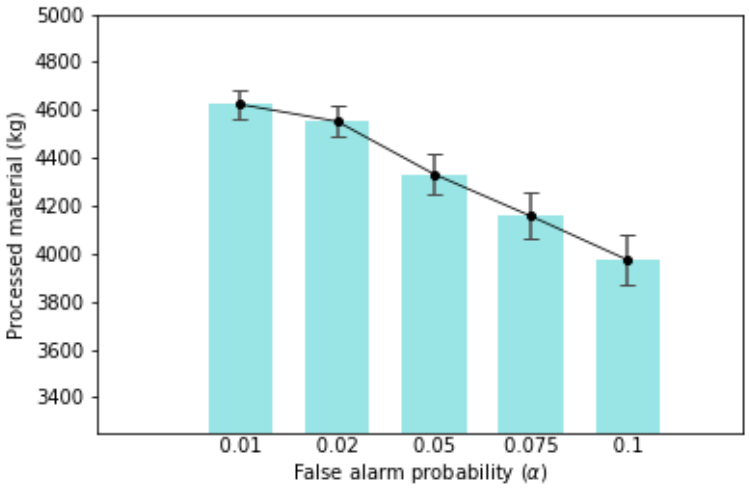

Figure 2.10a: With the false alarm probability of 0.01, the average amount of 4622 ± 58.3 kg is processed. The following average amounts given the false alarm probabilities of 0.02, 0.05, 0.075, and 0.1 are obtained as 4552 ± 64.9 kg, 4332 ± 81.8 kg, 4156 ± 96.0 kg, and 3973 ± 102.0 kg.

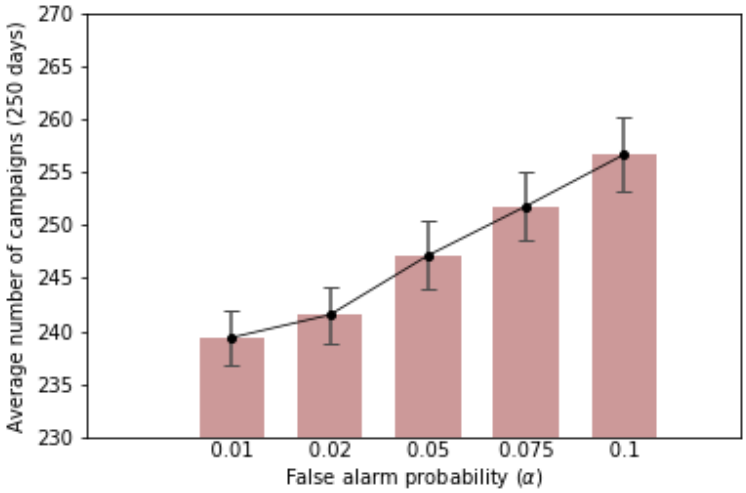

Figure 2.10b: With the false alarm probability of 0.01, the average number of campaigns is 239 ± 2.6. The following average numbers of campaigns given the false alarm probabilities of 0.02, 0.05, 0.075, and 0.1 are 242 ± 2.7, 247 ± 3.2, 252 ± 3.3, and 257 ± 3.5.

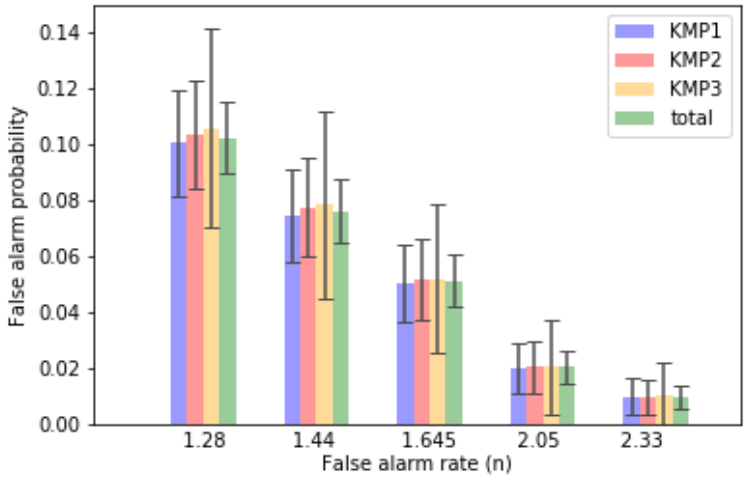

Figure 2.10c: The desired false alarm probabilities matched well with the simulation results calculating the false alarm probabilities by dividing the raised alarms by the total numbers of ID calculation during operation. Not only counting the total alarms, alarms raised at each KMP had been monitored. The detailed numerical data is shown in Table 2.2.

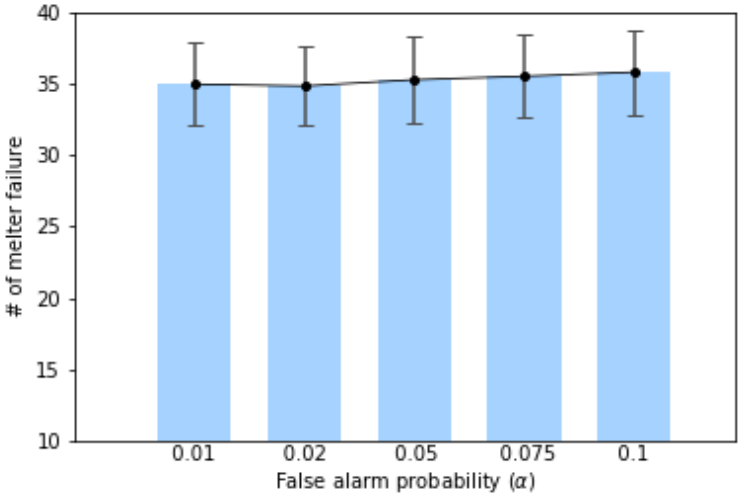

Figure 2.10d: The melter failed 35 times given the false alarm probabilities of 0.01, 0.02, 0.05, and 0.075. The melter failed 36 times with the false alarm probability of 0.1. Their standard errors stayed about 3 melter failures.

Figure 2.10: False alarm probability variation

Figure 2.10b shows when we set a desired false alarm rate to be lower, the number of campaigns increases. The current model increments the number of campaigns whenever the material is stored either in the recycle storage or the product storage. Therefore, with higher false alarm probabilities, a relatively large amount of material was stored in recycle storage, and it saved some time to complete a campaign by moving a batch directly to recycle storage not going through the trimming process. Figure 2.10c and Table 2.2 verify that the desired false alarm probabilities matched with the simulated false alarm probabilities given different false alarm rates. With a higher false alarm rate, the false alarm probability decreases. In other words, the area under the ID Gaussian distribution and above the alarm threshold is equal to the false alarm probability (Figure 2.7), therefore, a higher false alarm rate set an alarm threshold higher, which represents that the false alarm probability would be smaller. Finally, the average numbers of melter failure stayed around 35 because different false alarm probabilities did not affect melter failure (2.10d).

2.7.5 Failure Rate Variation

By increasing the failure rate parameter, less material was processed (Figure 2.11a), and also less number of campaigns was passed (Figure 2.11b). In this case, time needed to pass the material through KMP 3 was much longer than time to pass the material directly to the product storage without melter failure. The average false alarm probabilities were the same, around 0.05, and it is not shown in Figure 2.11c due to redundancy of previous graphs. Particularly, the standard deviation of false alarm probabilities at KMP 3 decreased since a higher failure rate parameter might have provided a larger sample size (2.11c). In other words, melter failed more often so that the material passed through KMP 3 more, and ID calculation happened many times compared to the previous model with a lower failure rate parameter. Herein, the number of melter failure indeed increased because the failure rate parameter increased (2.11d).

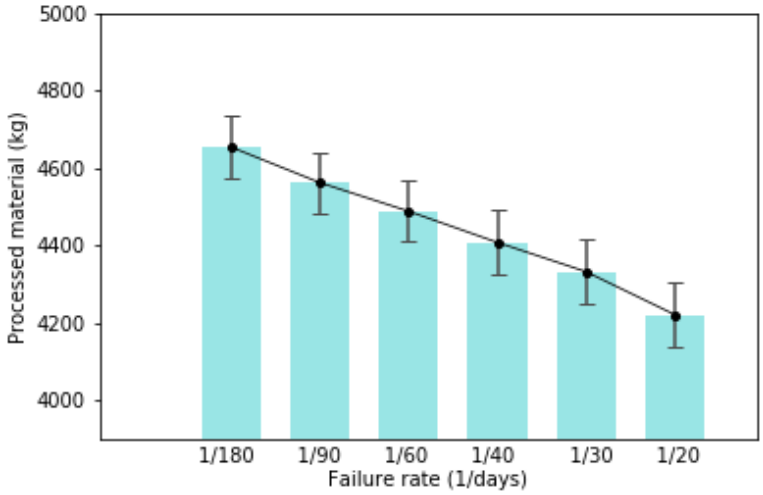

Figure 2.11a: With the failure rate parameter of 1/180 days, the average amount of 4653 ± 80.8 kg is processed. The following average amounts given the failure rate parameters of 1/90 days, 1/60 days, 1/40 days, 1/30 days, and 1/20 days are obtained as 4561 ± 77.1 kg, 4488 ± 78.9 kg, 4407 ± 82.1 kg, 4332 ± 81.8 kg, and 4221 ± 85.2 kg.

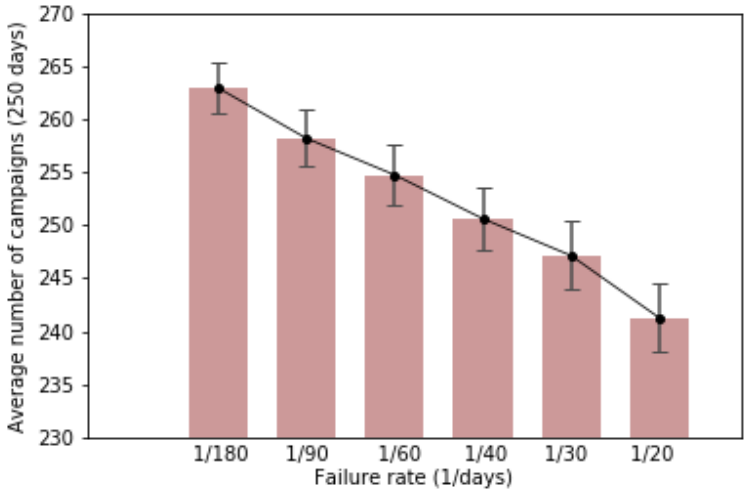

Figure 2.11b: With the failure rate parameter of 1/180 days, the average number of campaigns is 263 ± 2.4. The following average numbers of campaigns given the failure rate parameters of 1/90 days, 1/60 days, 1/40 days, 1/30 days, and 1/20 days are obtained as 258 ± 2.7, 255 ± 2.8, 251 ± 2.9, 247 ± 3.2, and 241 ± 3.2.

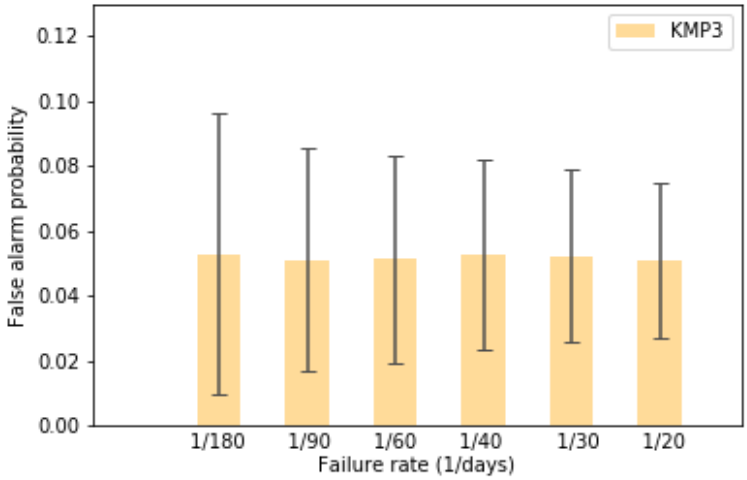

Figure 2.11c: Given the false alarm probability of 0.05, different failure rate parameters bring different standard errors. While all the means of false alarm probabilities at KMP 1, KMP 2, and KMP 3 are close to 0.05, the standard deviation of false alarm probabilities at KMP 3 decreases as the failure rate parameter increases.

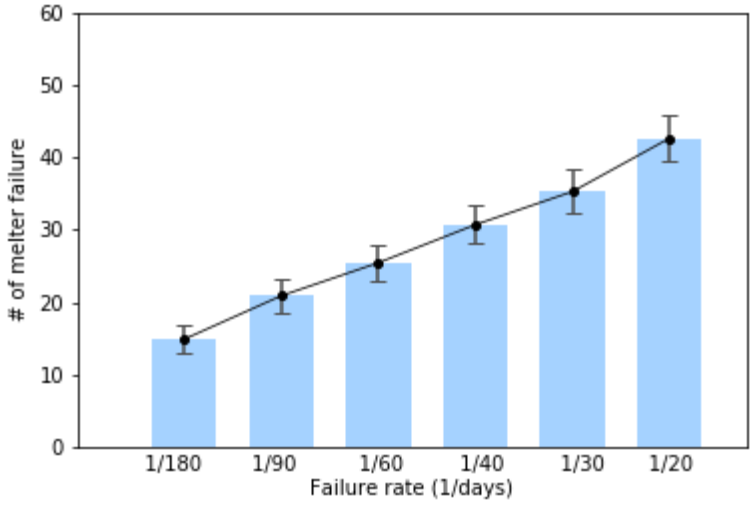

Figure 2.11d: With the failure rate parameter of 1/180 days, the average number of melter failure is 15 ± 2.0. The following average numbers of melter failure given the failure rate parameters of 1/90 days, 1/60 days, 1/40 days, 1/30 days, and 1/20 days are obtained as 21 ± 2.3, 25 ± 2.5, 31 ± 2.6, 35 ± 3.0, and 43 ± 3.1.

Figure 2.11: False alarm probability variation

2.7.6 Individual False Alarm Probability at each KMP

The second simulation with random and systematic errors of 0.1% each processed less products (Figure 2.11a), and more campaigns had been recorded since a large amount of material went to recycle storage (Figure 2.11b). Figure 2.11c explains that different false alarm probabilities were set for KMP 1, KMP 2, and KMP 3 for the second simulation. Since the same numerical alarm threshold was given for the ID distribution with a large measurement error of 0.1%, higher false alarm probabilities were expected. The average shorter time was needed to complete a campaign by passing material directly from a KMP to recycle storage. Figure 2.11d also proves that varying the false alarm probability at each KMP does not influence melter failure.

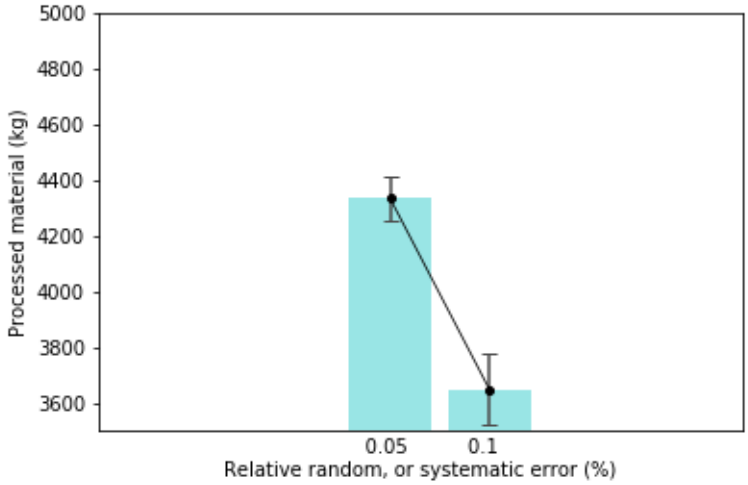

Figure 2.12a: The first simulation with the relative random and systematic errors of 0.05% each processed more products. The average number of processed material for the first simulation run is 4332 ± 81.8 kg, and that of the second simulation is 3647 ± 126 kg.

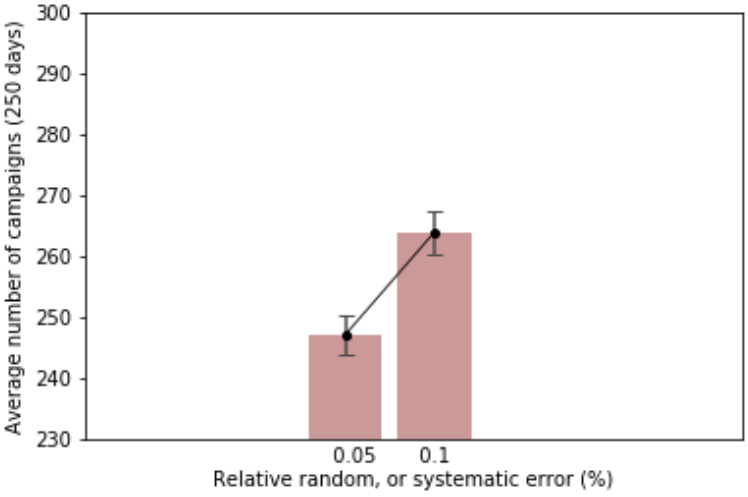

Figure 2.12b: Herein, a higher number of campaigns went through during the second simulation with the relative random and systematic errors of 0.1% each. The average number of campaigns for the first simulation is 247 ± 3.2, and that for the second simulation is 264 ± 3.5.

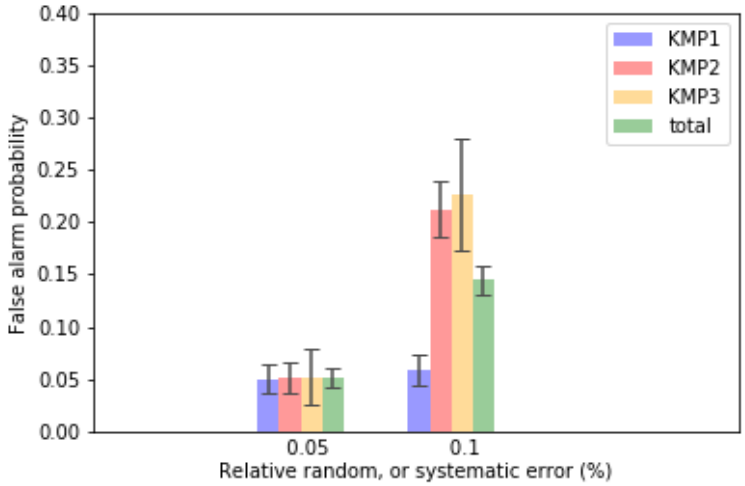

Figure 2.12c: By modifying the relative measurement errors and using the exact same numerical value for the alarm threshold for every KMPs, the false alarm probabilities can vary. Table 2.2 contains the detailed numerical output.

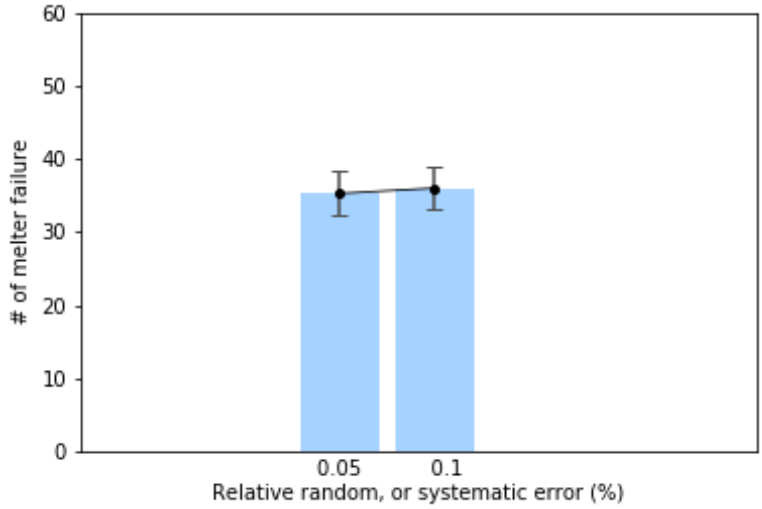

Figure 2.12d: Varying the false alarm probability at each KMP does not affect melter failure. For the first simulation, the average number of melter failures is 35 $\pm$ 3.0, and that of the second simulation is 36 $\pm$ 2.9.

Figure 2.12: Individual false alarm probability at each KMP

2.7.7 Changes in Heel Amount

We predicted that changes in heel amount do not induce changes in false alarm probabilities because alarm threshold functions defined in the KMP class automatically calculate appropriate alarm thresholds. As expected, the false alarm probability of 5% provided the same number of campaigns about 247 $\pm \sim 3$. The average number of melter failures were also around 35 times. However, the amount of processed material decreased when the average of heel amount increased (Figure 2.13). If a large amount of heel is left in a crucible every campaign, the total products after 250-day operation would be small. In fact, a relatively small amount decreased by adding an extra amount to the heel, and it is less than the uncertainty error of processed material.

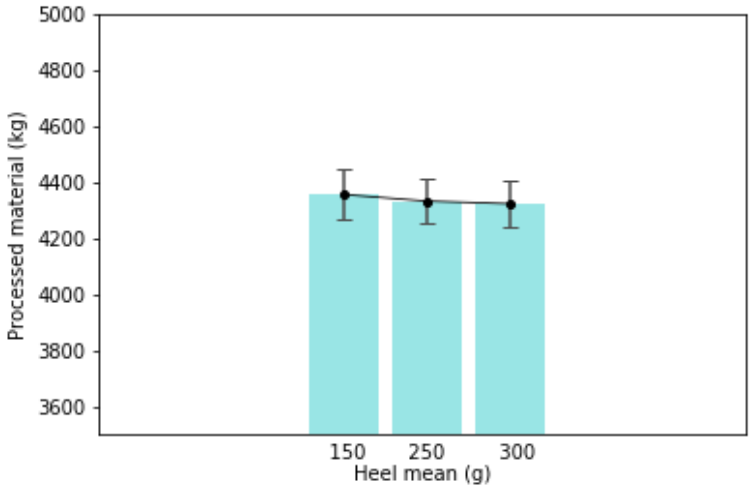

Figure 2.13: Changes in heel amount. The average amounts of processed material given the heel amounts of 0.15 kg, 0.25 kg, and 0.3 kg are 4355 kg, 4332 kg, and 4322 kg.

2.7.8 Inventory Verification

By using Equation 2.13, we can obtain the number of items containing special nuclear material to be inspected, particularly for Pu in this case. A separate function for 'random sampling' was developed different from regular execution routines. Using 20 kg of Pu vessels, nearly the same number of items must be inspected. However, as the average amount of material in vessels decreased, the sample size also decreased (Figure 2.14). For instance, with the average of 100g of 50 vessels, only $\sim$2 vessels had to be inspected given the detection probability of 0.95. However, with the average of 20 kg of 50 vessels, inspection was required for all 50 vessels. In addition, only 19 vessels would

need examination if the average amount were about 100 g for all 500 vessels with the detection probability of 0.95. A relatively small amount of TRU must be stored in each vessel, therefore, in this way, the practical inspection time can be implemented rather than investing all the vessels stored in the storage. Nevertheless, depending on how frequent the material balance period is, all the vessels might need to be inspected.

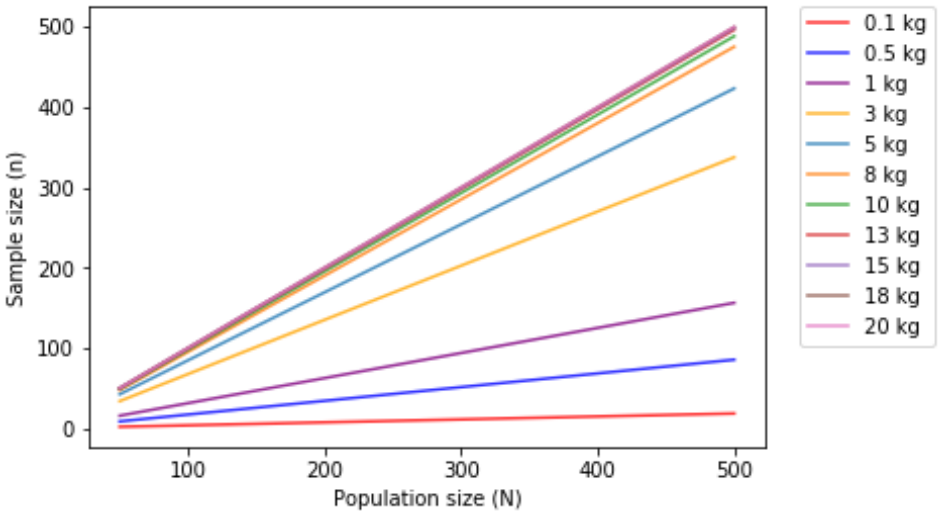

Figure 2.14: The random sampling concept. As the population size increases, the sample size also increases. With a small vessel size, less samples have to be inspected while with a large vessel size of 20 kg of Pu, nearly the population size is used as the sample size.

2.8 Future Work

Near-real world data is still necessary to build the model in a robust manner. Scenarios of further material transfer from a false alarm raise due to accumulated sequential IDs should be implemented to the model. In addition, cumulative IDs for each MBA every year can be calculated to prohibit another type of protracted diversion attempts. We assume that the alarm threshold of 2.4 kg would be used for cumulative IDs, and also the corresponding inspection algorithms must be applied to the model. Addition of auxiliary sub-processes and different KMP locations would be beneficial to adopt the ultimate safeguards model for a commercial-scale fuel fabrication facility. Also, the frequent crucible replacement or material losses from the trimming process would be considered for the advanced model development. The unit test of inventory verification is established, therefore, it can be applied into the execution routines every month or

every year. At last, the development of its user-friendly graphical user interface would be favorable.

2.9 Summary Remarks

The safeguards model on a commercial-scale fuel fabrication facility is useful to avoid both 'abrupt' and 'protracted' diversion attempts. While the first build of a model carried out material balance every campaign, the current model performs ID calculation at every KMP, which brings in two different facility designs processing different amounts of material and passing different campaign numbers. Additional sensitivity analyses by varying the facility input parameters such as false alarm probability, melter failure rate, alarm threshold at each KMP, etc. have been performed. The following are the significant outcome of these testings and the established functionalities included in the current model:

- KMP1 removal resulted in processing a significantly large amount of material given the same false alarm probability of 0.05. The equipment design has the advantage of producing a relatively large amount of products while the baseline design can exactly tell where a diversion attempt might have occurred.
- Different facility designs did not affect melter failure.
- Much less material had been processed with the false alarm probability of 0.1 compared to the false alarm probability of 0.05.
- Changes in heel amount did not affect the false alarm probability. The model automatically corrected numerical values for the alarm thresholds to keep the desired false alarm probabilities.
- A separate unit test using the concept of 'random sampling' for PIV or IIV was implemented, and a small vessel size may be necessary for the practicality of inspection time.
- If the melter fails less than once per month, much more material can be processed.
- Using a different desired false alarm probability for each KMP may be useful for particular sub-processes which possibly contain more or less special nuclear material.

- ID calculation can happen on a desired location. Adding or removing KMP locations is very flexible.
- Adding or removing sub-components is also flexible.

Chapter 3: Hazard and Operability Analysis of a Pyroprocessing Facility

Submitted to *Nuclear Engineering and Design* and under review

3.1 Abstract

Pyroprocessing utilizes electrochemical techniques to develop an advanced fuel concept for nuclear reactors, such as a sodium fast reactor. Since there exist proliferation risks associated with special nuclear material processed in a pyroprocessing facility, we have developed the high reliability safeguards methodology to implement safeguards, safety, and physical security with operations from a design-driven perspective. This paper suggests the design strategies by integrating a hazard and operability analysis. It is a kind of process hazard analysis, essential for identifying hazards, operability issues, severe accident scenarios, and for mitigating consequences with the corresponding protection methods. It is a preliminary step for eventual quantitative, probabilistic risk analysis, which is critical for obtaining an operating license for a commercial pyroprocessing facility. Our current focus of HAZOP is on major pyroprocessing subsystems; voloxidation, electroreduction, electrorefining, electrowinning, and the argon atmosphere control system. We analyzed the derived deviations from normal operations and thoroughly prepared the methods to prohibit or mitigate off-normal situations. Importantly, pressure buildup or high temperature in the systems can increase the risk of initiating fire/explosion, which may eventually release radiation to the outside. Safety relief valve installation, valve actuation, heater automatic shut down systems, etc., would be helpful to alleviate operation problems. This enhanced HAZOP also suggests a strong safeguards design for the facility by proposing nuclear material accounting locations for the purpose of reducing the potential proliferation risk.

3.2 Introduction

3.2.1 Motivation

The systematic risk assessment on a complex operation is imperative in order to identify and evaluate hazards, associated consequences, and potential strategies to mitigate risks. It is particularly a requisite for nuclear materials operations carrying SNM

due to its potential proliferation risks. In the effort to enhance energy independence, nations have considered the establishment or expansion of nuclear power as part of their domestic energy portfolio. As a result, the deployment of, or transition to advanced nuclear energy systems can assure resource sustainability. Some of these advanced systems require nuclear fuels different from those fabricated currently.

Pyroprocessing uses electrochemical technologies to extract actinides and uranium from used nuclear fuel to fabricate metal fuel. For instance, the IFR project had been under development at Argonne National Laboratory (ANL) since the 1980s to process used metallic nuclear fuel for the closed fuel cycle concept [91], [92], [93], [94]. A pyroprocessing facility, however, faces new challenges in order to maintain high proliferation resistance because SNM, such as plutonium, is in a different chemical and physical form than fuels fabricated for contemporary light-water reactors. Therefore, the concept of integrating safeguards, safety, and security with facility design; i.e., safeguardability, or safeguards- and security-by-design [3], [4] was put forth fairly recently as an approach to address these issues in a systematic manner.

3.2.2 The High Reliability Safeguards Methodology and Related Work

The HRS focus area was developed based on this initial concept of safeguardability [5], [6], for two main research directives: (1) optimizing safeguards, safety, and physical security with facility operations from a design-driven perspective and (2) integrating design strategies within a risk-informed context, similar to typical safety-based risk assessments for nuclear power plants, but incorporating initiating events that span all aspects of 3S. The overarching goal for HRS is to quantify proliferation risk for different facility designs in a systematic manner based on established risk assessment principles. Prior work has focused on formulating design options [7], [8], [9], and recent work focuses on the operational side [63], [59], which stresses the HRS approach using discrete event simulation for material throughput in fuel fabrication and tests the means by which safeguardability can be quantified for facility design concepts.

3.2.3 Goals for this Study

Here, we turn to the risk-informed directive and apply a HAZOP study of a pyroprocessing facility to identify the highest risk deviations from normal operations and develop mitigation options for these potential hazards and operability problems. A HAZOP analysis is a preliminary and necessary step prior to undertaking the com-

prehensive quantitative, probabilistic risk analysis critical to obtaining an operating license for the facility. Additionally, beyond this traditional HAZOP analysis, we also analyze how these deviations from normal operations affect nuclear materials accounting and potential proliferation risks, and we suggest how these can be mitigated from a safeguards perspective. In order to design a safeguardable facility, accounting for SNM is paramount. This can be achieved by establishing KMPs at MBA boundaries. Throughput considerations are important to the operator, as they have the incentive to process a target amount of material; e.g., several metric tons per year of used fuel. SNM throughput, therefore, must be monitored regularly, and the means by which SNM can be monitored are discussed in this HAZOP study. This enhanced form of HAZOP then can lend critical insight into the design of a safeguardable facility. This current study is part of a continually developing body of research that focuses on a risk-informed approach to pyroprocessing facility design [5], [6].

3.3 Background

3.3.1 Pyroprocessing Material Flowsheet

For our HAZOP study, the PFD outlined in Figure 3.1 is used [63]. We based our facility design on the "Korean Innovative, Environment Friendly, and Proliferation Resistant System for the 21st Century (KIEP-21)" advanced fuel cycle concept developed by the Korea Atomic Energy Research Institute (KAERI) [5], [6], [95], [96] and lab-scale or engineering-scale experiments performed by Idaho National Laboratory (INL) and ANL [97], [98], [99], [100], [101], [102]. The intent is to provide a credible HAZOP analysis that can be applied widely to pyroprocessing facility design concepts without being site-specific. For instance, nuclear materials are commonly processed in hot cells at high temperature; therefore, we assume that an inert Ar atmosphere is needed for operational safety. The operation starts by chopping and decladding used fuel. Next, voloxidation oxidizes used fuel to produce U_3O_8 powder. Electroreduction reduces the powder to a metal in $LiCl$-Li_2O salt. Electrorefining and electrowinning extract uranium and TRU metals in eutectic $LiCl$-KCl salt. Metal fuel slugs are then finally fabricated and stored. For more details, an extensive literature review of the pyroprocessing facility is contained in Borrelli [5], and we thoroughly describe the design intent of each subprocess in greater detail in Section 3.4.

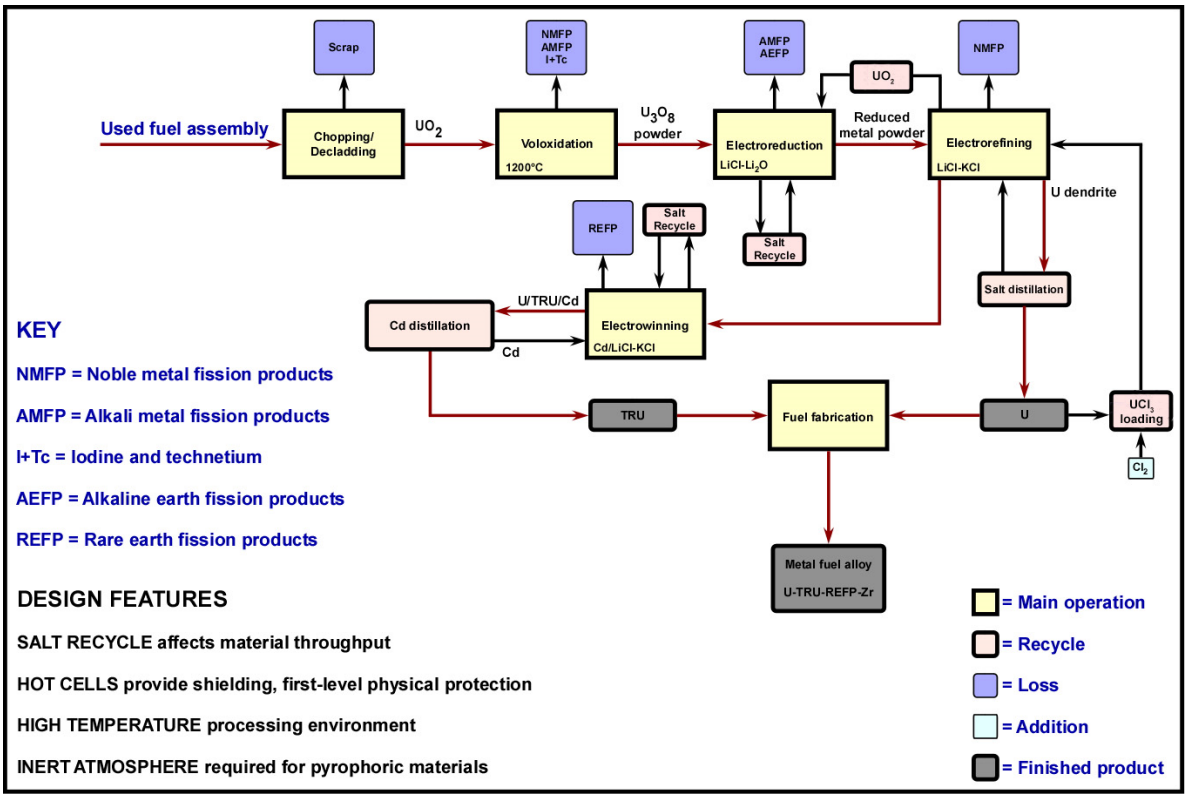

Figure 3.1: Process flow diagram of the pyroprocessing system used for the HAZOP analysis. Used uranium oxide fuel enters the system as shown in the top left. Main subsystems are voloxidation, electroreduction, electrorefining, electrowinning/cadmium distillation, and metal fuel fabrication. They are indicated by the yellow boxes with the primary material flow shown by the red arrows. Material losses are shown for each subsystem. A metal fuel alloy is prepared by the fuel fabrication process for use in an advanced reactor concept.

3.3.2 General HAZOP Methodology

Hazard identification techniques involve the identification of potential hazards and operability issues [103]. They study possible scenarios, which might cause undesirable consequences in the system, and suggest the corresponding mitigation methods. In particular, a structured systematic approach of HAZOP is to identify the causes and consequences of deviations from the design intent. The goal of HAZOP is to eliminate or reduce hazards by analyzing possible deviations that could lead to safety, health, or environmental problems [104]. HAZOP has some advantages over other process hazard identification methods since it provides a detailed, systematic plan for process performance, including operation conditions and control instrumentation. This qualitative

risk assessment also lists the failure consequences, for which we can suggest mitigation methods before actual operation. Furthermore, HAZOP can be used during the life cycle of the facility.

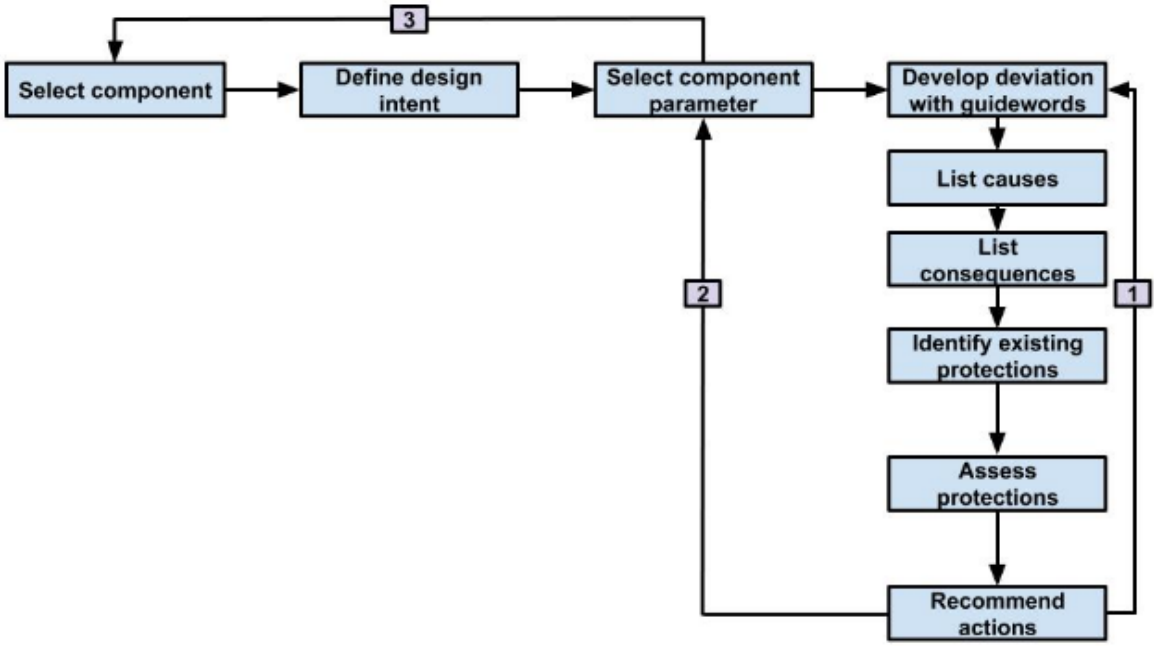

Figure 3.2: The HAZOP parameter-first approach contains three 'procedural loops.' First, the system component (study node) is selected. Here, we have selected pyroprocessing subsystems. The design intent for each is identified. From this, relevant parameters are selected. Deviations are then derived by combining the parameters with the corresponding guide words. Resulting hazards and consequences due to the deviations follow. Existing protections are identified and assessed. Finally, risk mitigation actions are recommended. This is repeated for the same node, under a different guide word; e.g., first high pressure is analyzed, then low pressure. Once the analysis of all the corresponding guide words is complete, a new parameter is selected and the process repeats. Once all the parameters are analyzed, a component is selected, and the entire process begins again. In this way, all the deviations given for the nodes are categorized with related mitigation strategies.

HAZOP breaks down the complex design into simpler sections called study nodes, and each node must be addressed by determining deviations from the initial design intent [104]. These deviations can be generated with the parameter-first approach. Process parameters are coupled with guide words to derive meaningful deviations, for which we propose protection methods in advance of accidents. Figure 3.2 shows the flow diagram of the HAZOP parameter-first approach. After specifying system compo-

nents (study nodes), we then develop their design intent. From the design purpose and detailed process description, parameters for a node can be selected. Deviations are derived by combining the parameters with the corresponding guide words, based off which their possible causes and consequences are determined. They describe how the process conditions may depart from the design intent. By analyzing all the deviations given for the node, we suggest the mitigation methods, which may reduce the probability of accident occurrence. When all the nodes are reviewed, the HAZOP study is completed. Here, Table 3.1 describes the standard guide words and their meanings [105].

Table 3.1: Standard guide words and their meanings

Guide word	Meaning
No, Not, None	No operation takes place.
More of	A quantitative increase in an activity
Less of	A quantitative decrease in an activity
Part of	Only part of the design intent is completed.
Reverse	Inversion of an activity
Other	Other than normal operations, such as shutdown, maintenance, start-up, etc.
As well as	Another activity happens as well as the initial activity.
Sooner/Later than	The timing is different from the design intent.

3.3.3 Prior Nuclear-related Uses of HAZOP

HAZOP was first published in the 1970s by Lawley [106], and numerous HAZOP studies for chemical industries have been proposed since then [107], [108], [109], [110]. Some have their focus on nuclear facilities. For instance, HAZOP combined with the risk priority number was introduced for a light water reactor passive cooling system [111], [112], and was also implemented on a heavy water reactor passive cooling system [113]. Furthermore, HAZOP application to the Ignalina Nuclear Power Plant (INPP) decommissioning projects [114] and the Korea Research Reactor-1 decommissioning project [115] were demonstrated successfully. Some of the notable HAZOP

studies on aqueous reprocessing plants include the one performed by British Nuclear Fuels Ltd. on the thermal oxide reprocessing plant [116] and the probabilistic safety assessment using HAZOP on the Tokai Reprocessing Plant conducted by the Japan Nuclear Cycle Development Institute [117]. Although copious research related to HAZOP on nuclear facilities has been achieved, HAZOP development specifically on a pyroprocessing facility has not been studied yet. This is imperative for scaling up pyroprocessing to a commercial facility.

3.3.4 Preliminary Safety Study on Pyroprocessing

While HAZOP for pyroprocessing has not been carried out yet, the preliminary safety study on a conceptual design of the Reference Engineering-scale Pyroprocess Facility (REPF) had been established [118]. Moon evaluated hazards in detail to optimize its system processes and structures of equipment. Not only were the key major systems and components classified with the ranks of safety, seismic, and quality classes, overall potential hazards in the facility were also identified with their possible causes and consequences. Possible accident scenarios for the conceptual design of an engineering-scale pyroprocess facility, called the Advanced Fuel Cycle facility, were ranked by using the risk ranking matrix adopted from Mitchell [119] to evaluate their impacts [120]. However, these studies did not categorize hazards for specific sub-processes and instead focused on a general hazards analysis for the facility. In contrast, our HAZOP study identifies more specific hazards in major sub-processes, establishes mitigation methods for potential accidents, and formulates suggestions within the context of safeguardability.

3.4 Results and Discussion: HAZOP Analysis on Study Nodes

3.4.1 Approach

One of the notable guidelines on HAZOP, according to Dunjó, is provided in "HAZOP: Guide to Best Practice [110]." We primarily apply this methodology on a commercial-scale pyroprocessing facility. Several other literatures such as [105], [121], and [122] support HAZOP approaches comparable to Crawley's [104]. We first identify and analyze components (study nodes) under the HAZOP methodology. We then examine design intent, process details, and several system parameters such as temperature, flow rate, pressure, etc. We provide an additional degree of detail to this analysis

by including process flow diagrams (PFDs).

3.4.2 Component (Study Node) Identification

While a HAZOP can become exceedingly detailed, as any industrial system can contain hundreds to thousands of single components, we select main subsystems given for the conceptual commercial pyroprocessing facility design as the components for this analysis. Use of subsystems for the study nodes here can yield substantive results in terms of safeguardability because there has not yet been a HAZOP analysis of this kind. This type of analysis also provides the framework for future, more detailed risk-informed studies. The study nodes are defined for the following fundamental sub-systems: voloxidation, electroreduction, electrorefining, electrowinning, and the Ar atmosphere control system. A commercial-scale pyroprocessing facility contains other auxiliary systems depending on its design approaches and site-specific features. However, for this HAZOP study, we address the most fundamental system components common for any pyroprocessing plants.

3.4.3 Use of PFDs for Sub-processes for HAZOP

Piping and instrumentation diagrams of engineering-scale machineries for electrochemical processes from the PRIDE facility, operated by KAERI, and the Fuel Conditioning Facility (FCF) at INL are not open to public. Therefore, we perform our study by generating expected PFDs (Figure 3.7, Figure 3.8, Figure 3.9) for processes on the engineering judgement and past work in this field, including relevant literature sources. This can be a good basis to facilitate further development to implement more inherently safe processes [103].

3.4.4 Design Intent for Pyroprocessing Operational Steps

A literature review of pyroprocessing is shown in Borrelli [5]. Here, adding on to it, we thoroughly discuss several major pyroprocessing subsystems for our HAZOP study mentioned earlier as study nodes. We assume the operation starts with the receipt of spent uranium oxide fuels. The pre-treatment of disassembling, rod extraction, rod cutting, and fuel decladding before voloxidation is not considered for the current HAZOP study because it is well characterized due to established aqueous reprocessing technologies at the head-end process stages [123], [124]. We assume these processing stages are

similar in the pyroprocessing plant. Otherwise, other possible alternative methods can be applied from Bond [125], Westphal [126], Lee [127], and Bodine [128].

3.4.4.1 Voloxidation

The voloxidation process oxidizes UO_2 into U_3O_8, allowing a greater surface area for the active electrochemical reaction, thus increasing the efficiency of electroreduction [129]. The engineering design of a high-capacity voloxidizer developed by KAERI is considered for our HAZOP study (Figure 3.3). While the fuel pellets are ground into powders in the presence of air/O_2, volatile fission gases are removed and sent to an off-gas system. An adequate amount of air flow is needed to prohibit fuel powders from escaping, as well as to maintain the acceptable level of pressure in the cell. Increasing the system temperature eliminates fission gas products easily, however, the sintering process of U_3O_8 powder is not favorable above 1000^oC. More details about this process can be found through a joint project between KAERI and INL on development of the voloxidation process for LWR spent fuel treatment [130], [131].

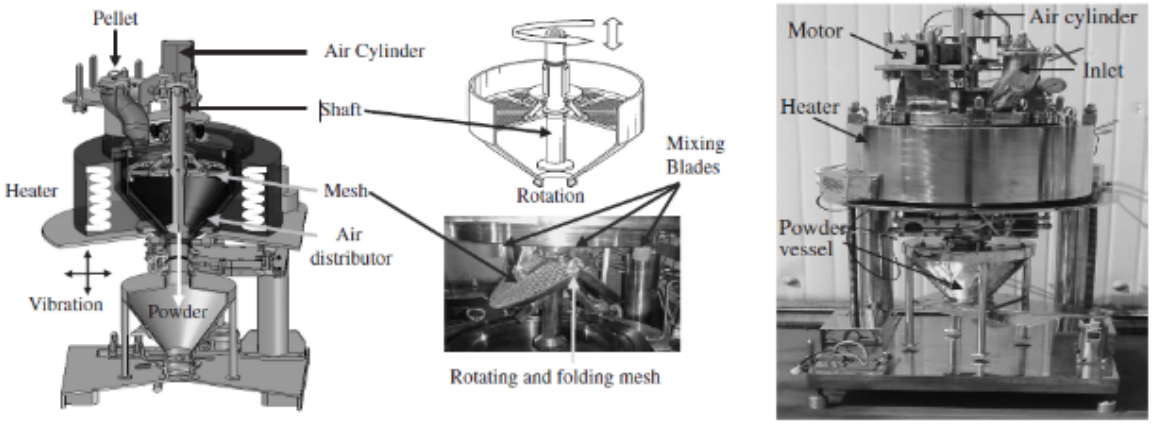

Figure 3.3: Experimental voloxidation apparatus [132]. UO_2 pellets are pulverized to U_3O_8 powder using air at high temperature. Pulverization results in a density decrease, and therefore volume increases for more efficient electroreduction. Volatile, gaseous fission products; e.g., Kr, Xe, I, etc., are eliminated by voloxidation.

3.4.4.2 Electroreduction, Electrorefining, and Electrowinning

After the U_3O_8 powder preparation, it is electrochemically reduced in the molten salt electrolyte of $LiCl$-Li_2O at 650^oC [13], [14], [15], [16], [133], [134]. Figure 3.4 is the schematic diagram of electroreduction process. The MgO cathode container is often

used to reduce the metals while oxygen gas is generated at the Pt anode [129]. A Ni/NiO reference electrode is commonly used but not shown in Figure 3.4 [135]. Other alternative materials for the cathode containment and the anode shroud are described in Choi [136]. Through this process, the dense metals reduce the volume of spent fuels, and high heat load fission products (alkali metals and alkaline earth fission products; e.g., Cs and Sr) are dissolved in the molten salt and finally removed as wastes [96]. We also consider the design concepts of a laboratory-unit electrolytic reduction system called the Hot Fuel Dissolution Apparatus at the Hot Fuel Examination Facility (HFEF) [135] and the engineering-scale electrolytic reducer at the PRIDE facility to review detailed design and engineering issues.

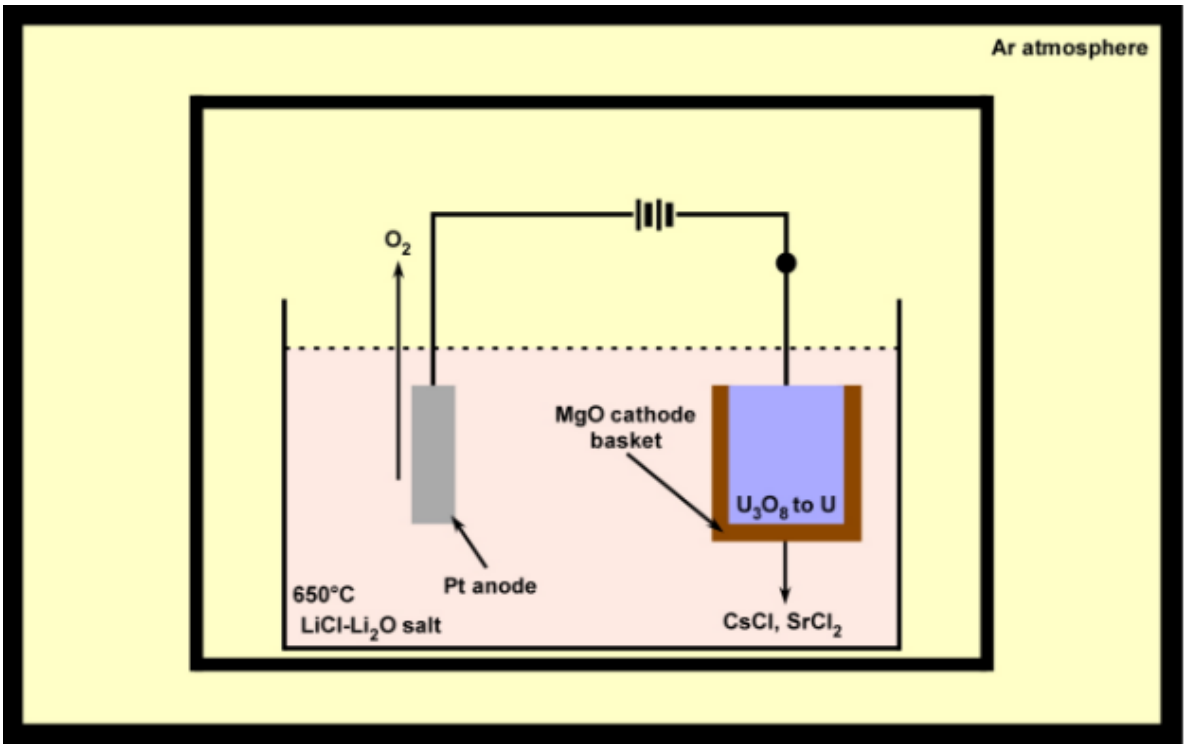

Figure 3.4: Notional representation for electroreduction. U_3O_8 powder is reduced to U metal, containing TRU with some noble metals in a cathode basket. Oxygen gas is evolved at the anode. Alkali metals and alkaline earth fission products form chlorides in the $LiCl$-Li_2O molten salt at 650^oC. Most importantly, high heat Sr and Cs fission products form chlorides in the salt and are removed from the metal [101], [137].

INL has developed an electrorefining process by treating used metallic fuel from the EBR-II reactor in the FCF [138]. Two engineering-scale electrorefiners called the Mark-IV and Mark-V ERs have processed approximately 830 kg heavy metal of driver fuel up to 2012 [98]. Their system designs are used to identify the associated hazards and

operability issues. The reduced metals from electroreduction process get transferred into an anode basket to selectively recover uranium [15], [96]. The eutectic salt of $LiCl$-KCl is used as an electrolyte, and the working temperature is about 500^oC [139]. UCl_3 is added for initiating the uranium deposition on the cathode. Noble metals stay in the anode basket while TRU and rare earths are dissolved in the salt [140]. By controlling the applied cell voltage, uranium dendrites can be deposited on a solid cathode often made of graphite, and the collected uranium deposits are distilled in a salt distiller. After removing the salt from uranium deposits, they are melted and casted into ingots for subsequent fuel fabrication. Figure 3.5 shows the chemistry behind this process.

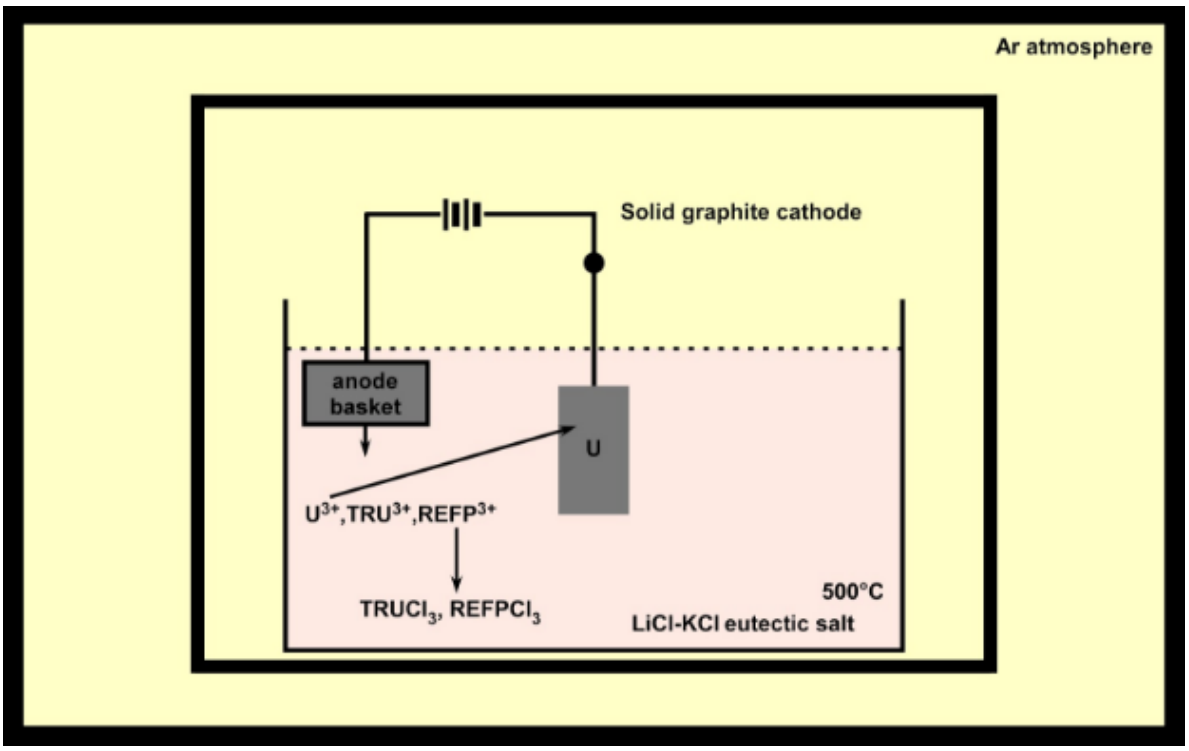

Figure 3.5: Schematic diagram of electrorefining process. Electroreduced metal creates trivalent cations in eutectic $LiCl$-KCl salt at 500^oC. Rare earth fission products and TRUs form chlorides in the salt. U metal dendrites collect on a solid cathode due to the difference in Gibbs free energy of formation. The salt is loaded with UCl_3 to initiate uranium deposition.

Electrowinning recovers TRU on a liquid Cd cathode along with some uranium and trace amounts of rare earths [17]. The same electrolyte for electrorefining, which is the $LiCl$-KCl molten salt, is also used for this process [139]. Uranium is prevented to deposit on a liquid Cd cathode by using the mesh agitator [96]. Figure 3.6 describes how electrowinning performs. Cl_2 gas might be produced at the inert anode. The

output TRU stream is combined with uranium metal recovered from the electrorefining process to fabricate new metal fuels. Additionally, Cd distillation separates Cd and the actinides recovered from the electrowinning process. We do not consider the Cd distiller in this HAZOP study as it is an auxiliary system of the facility.

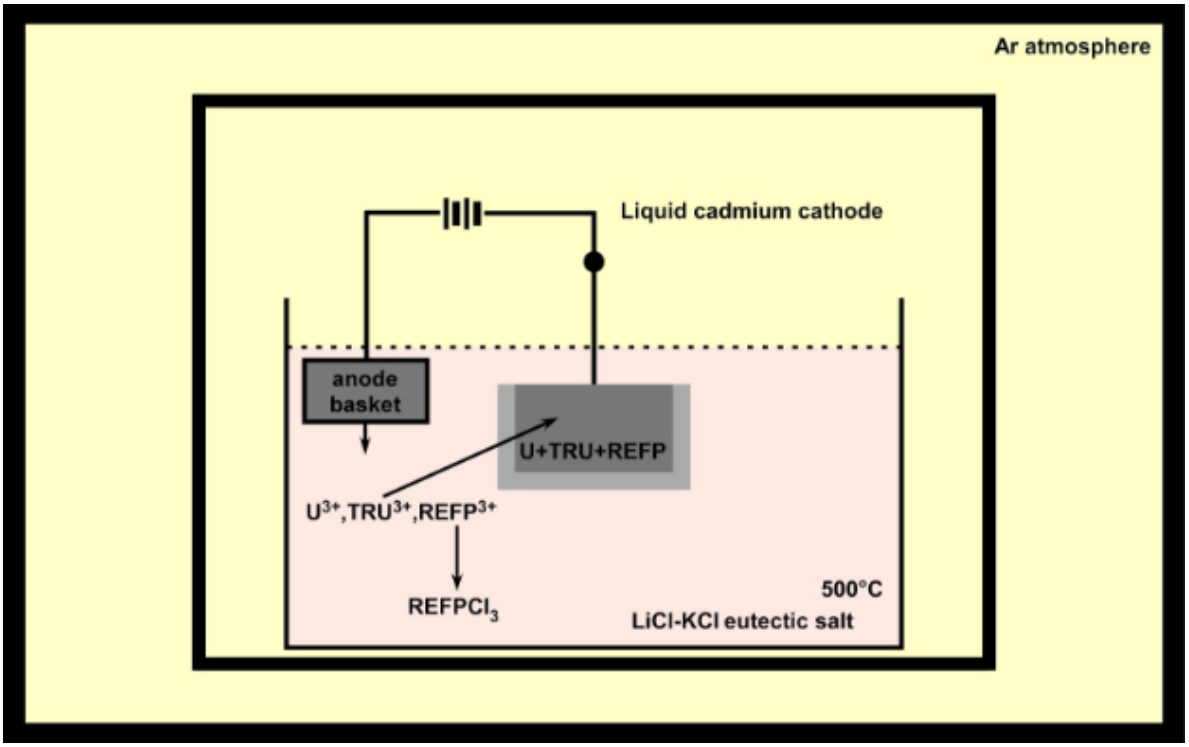

Figure 3.6: Notional depiction of electrowinning. The process uses the same eutectic *LiCl-KCl* salt as electrorefining. Trivalent cations of U, TRU, and rare earth fission products collect on a liquid cadmium cathode. TRU elements are not individually extracted due to small differences in Gibbs free energy of formation.

3.4.4.3 Ar Atmosphere Control System

The PRIDE facility is designed for continuous pyroprocessing operation. The Ar atmosphere control system installed for PRIDE, which consists of one large-scale hot cell for sub-operations [141], is chosen for our HAZOP. However, several different hot cells might be needed for a commercial-scale facility for the implementation of a strong safeguards design. This is discussed more in Section 3.4.5. Pyroprocessing involves a substantial amount of radioactive materials and a high temperature environment, therefore, an inert Ar atmosphere must be maintained by controlling the amount of oxygen and moisture concentration. The design intent of the Ar control system is to

circulate the gas flow to maintain the inert environment.

3.4.5 Operational Deviation Analysis

3.4.5.1 Voloxidation (Node 1)

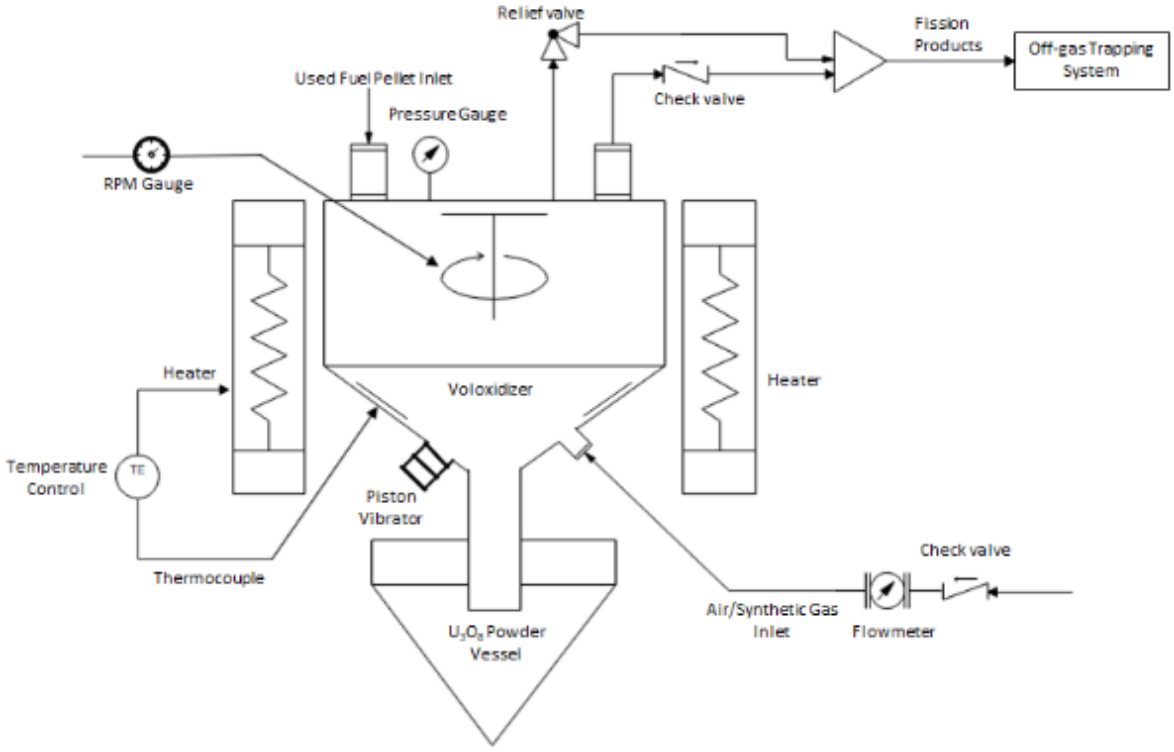

Figure 3.7: PFD of a voloxidizer. A RPM gauge measures the speed of the folding mesh. A pressure gauge monitors the system pressure, and the relief valve prevents overpressure. The temperature control reads the voloxidizer temperature using the thermocouples, and also acts as an automatic shutdown system in the event of system overheating. Flowmeters can control the air flow going into the system, and the check valve blocks the counterflow. Voloxidation process can generate fission gas products, and they are released to an off-gas trapping system.

Figure 3.3 is the schematic diagram of an experimental voloxidation apparatus developed by KAERI. Our team based the HAZOP on this model and built the PFD of this equipment (Figure 3.7). Mechanically pre-treated uranium fuel is fed into the top-end of a voloxidizer through valves that control the feed flows. Thermocouples and pressure gauges continuously monitor temperature and pressure in the voloxidizer.

Given the PFD and the design intent of producing U_3O_8 powder, the HAZOP table for voloxidation is presented in Table 3.2. The process parameters of pressure, gas flow rate, feed flow rate, temperature, time, agitation, and utility failure are chosen for this first study node. Among all the derivations shown in Table 3.2, the following are the primary deviations, which might possibly deliver severe accident scenarios to the system. The consequences are listed with their corresponding protection methods.

- **High pressure:** If the outlet valve is stuck, excess hot gases can build up in the machine. The safety relief valve helps to depressurize the system, or a valve can be actuated by an operator. Excessive air flow or the overloaded feed material may cause high oxidation of the feedstock. In this case, the machine might not function as intended and may cause fission gas products to reside within. As a protection method, flowmeters can be installed to control the air flow. High RPM speeds of the motors for the folding mesh and the piston vibrator improve the oxidation efficiency. However, if the exhaust gas cannot escape the machine, high oxidation efficiency may not be the ideal situation. A large amount of fission gases in a high temperature and pressure environment can cause explosion/fire, which may eventually release radioactive materials to the outside of the system. The manual control systems for motors are necessary, and indeed this whole system must be installed in a hot cell facility.

- **High air flow and high feed flow:** A large amount of oxygen and the feed material produce more U_3O_8 while generating more fission gases, for which the off-gas system is needed. If pressure is built up, the machine may explode, leading to a fire. A high air flow can also disperse the used fuel powder and allow it to escape from the system, which is undesirable for the potential radioactive material release. Flowmeters must be installed to monitor the air flow, and valve actuation to control the amount of feedstock would be needed.

- **Reverse air flow:** If the exhaust gas is going back into the voloxidizer, it may be due to a malfunctioning off-gas system connected to the voloxidizer, or issues with the valves. In this case, fission gases can build up and may induce the equipment rupture. Therefore, the off-gas system must be repaired as a corrective protection method, or for the temporary purpose, valves can be actuated to depressurize the system. The safety relief valve can be used for the same purpose. A check valve can also be used to make sure reverse flow does not occur.

- **High temperature:** Heater malfunction can lead to high temperatures. As a corrective action, the heater must be repaired. Thermocouples must be installed to monitor temperature during operation. The automatic heater shut down system can prevent temperature to increase beyond the limit.

Table 3.2: HAZOP table for voloxidation

Guide word	Deviation	Possible causes	Consequences	Protection methods
Parameter: **Pressure**				
More of	High pressure	Excess hot gas in the machine (fission gas product build up) from: Stuck valve, Fast air flow, High RPM speed of the motor for the folding mesh, High power piston vibrator	Machinery rupture, Explosion/fire, Fission gas release	Safety relief valve, Valve actuation, Installation of the flowmeters, Periodic check-up of motors, Manual control of electric motors for rotating the folding mesh and running the piston vibrator, Use of proper materials for the equipment or the piping systems, which are designed to withstand high pressure (steel)
Less of	Low pressure	Malfunctioning valves, Low air flow, Low RPM speed of the motor for the folding mesh, Low power piston vibrator	Low efficiency of oxidation (No severe accidents)	Pressure gauge installation, Valve repair, Flowmeter installation, Motor repair
None of	No pressure	No oxidation from: No air gas flow (gas supply line rupture), No feed (malfunctioning hatch value)	No yellowcake production	Flowmeter repair, Installation of backup loop for the gas supply line, Valve actuation
Parameter: **Gas flow (rate)**				
More of	High flow	Flowmeter malfunction	Fast flowmeter wear out, High oxidation efficiency can build many gaseous fission products in the system, Fuel powders may escape (Yoo et al., 2008)	Frequent flowmeter calibration, Flowmeter repair
Less of	Low flow	Small pipe leaks, Pipe rupture, Valve partial opening	Low oxidation efficiency	Pipe repair, Valve actuation

Table 3.2 (*Continued*)

Guide word	Deviation	Possible causes	Consequences	Protection methods
None of	No flow	Valve closed, Loop disconnected	No air feed, No products	Valve Actuation, Pipe rupture repair, Flowmeter installation for monitoring purpose
Reverse	Reverse flow (Exhaust gas going back into the voloxidizer)	Malfunctioning off-gas system	Fission gas build up	Off-gas system repair, Valve actuation to stop the reverse flow, Safety relief valve
Parameter: **Feed flow (rate)**				
More of	High flow	More fuel loaded	More fission gas buildup, Work overload; it may stop the machine	Precise scaling of the feed needed, visual inspection
Less of	Low flow	Less fuel loaded	Reduced oxidation efficiency	More fuels can be loaded
None of	No flow	Valve (hatch) closed	No products	Valve actuation
Parameter: **Temperature**				
More of	High temperature	Heater malfunction	Fire/explosion, Radiation release	Use of thermocouples to monitor temperature, Automatic heater shut down, Heater repair
Less of	Low temperature	Heater malfunction	Low oxidation efficiency	Use of thermocouples to monitor temperature, Heater repair
Parameter: **Time**				
More of	Too long	Low RPM speed of motors induces long residence time, Low gas flow, Large feed material load	Low process efficiency, Economic loss (time)	RPM speed up, Fast air flow, Reduced fuel load

Table 3.2 (*Continued*)

Guide word	Deviation	Possible causes	Consequences	Protection methods
Less of	Too short	Fast RPM speed of motors induces short residence time, A lot of gas flow, Low feed material load	Economic loss (utility)	RPM slow down, Low gas flow, More feed material can be loaded
Parameter: **Agitation**				
More of	Fast mixing	High RPM motors	Fast machinery wear out, Economic loss (utility)	Motor speed control
Less of	Low mixing	Low RPM motors	Low oxidation efficiency	Motor speed control
None of	No mixing	Malfunctioning motors, No power	Very low oxidation efficiency	Backup power and motors
Parameter: **Utility failure**				
None	Failure	Power outage	No feed flow (if valves are digitally controlled), No motors for mixing	Backup generator

- **Too long process time or short process time:** Malfunctioning motors might increase or decrease the process time to achieve the operation goal, which is the production of the U_3O_8 powder. Gas and feed flow rates also affect the length of process time. Flow and motor controls are necessary to prohibit economic losses such as time loss or capital loss.

- **Power loss:** A backup generator is needed to operate the system without interruption of power outage.

Safeguardability approach. The two main severe consequences in the voloxidizer due to the operational deviations include radiation release of fission product gases and potential dispersal of used fuel powder. The release of fission gas is undesirable, and several mitigation options have been presented, but this does not affect nuclear materials accounting. However, if the U_3O_8 powder is dispersed, then there might be an accounting challenge. While a State may not likely attempt a diversion of small quantities of the powder, unaccounted material violates IAEA treaty obligations for a non-weapons State. From a safety perspective, since the off-gas system for fission gases generated

from the voloxidizer might malfunction, we propose the installation of a separate hot cell for this equipment to contain a radiation release. From a safeguards perspective, installation of protective membranes to trap the powder is recommended.

From the standpoint of safeguardability, we assume that the used fuel would be characterized upon receipt at the facility, which is the typical procedure for aqueous facilities. Chopping and decladding in the head stages of the pyroprocessing facility would be no different, and the characterization and accounting of SNM at this point would be the same. In particular, the $^{244}Cm/Pu$ ratio is usually determined at this stage. ^{244}Cm is the dominant contributor to neutron emission in used fuel [7]. Upon exit of the voloxidizer, the material is powder, and, therefore, likely a homogeneous mixture. Sampling at a KMP at this location (exit of the process) could give a robust SNM accounting. The weight can be measured, as well as a radiation measurement with coincidence counting for spontaneous neutron emission of ^{244}Cm. This can then be used to determine the Pu content. Accounting at the exit of the voloxidizer must include the loss of mass due to fission gas release. Therefore, the KMP should specify a limit for this loss, where if exceeded, could indicate a diversion.

3.4.5.2 Electroreduction, Electrorefining, and Electrowinning (Node 2, Node 3, Node 4)

Despite different operation purposes of nodes for electroreduction, electrorefining, and electrowinning, these processes carry very similar HAZOP studies because they are all batch type processes and apply electrochemistry to reduce the targeted material on a cathode (Figure 3.8). Therefore, one HAZOP table (Table 3.3) is constructed for all the processes while the operation parameters, such as reactions, electrolytes, operation temperature ranges, pressures, etc., are specific for each node. Figure 3.4, 3.5, and 3.6 show the chemistry of electroreduction, electrorefining, and electrowinning, respectively.

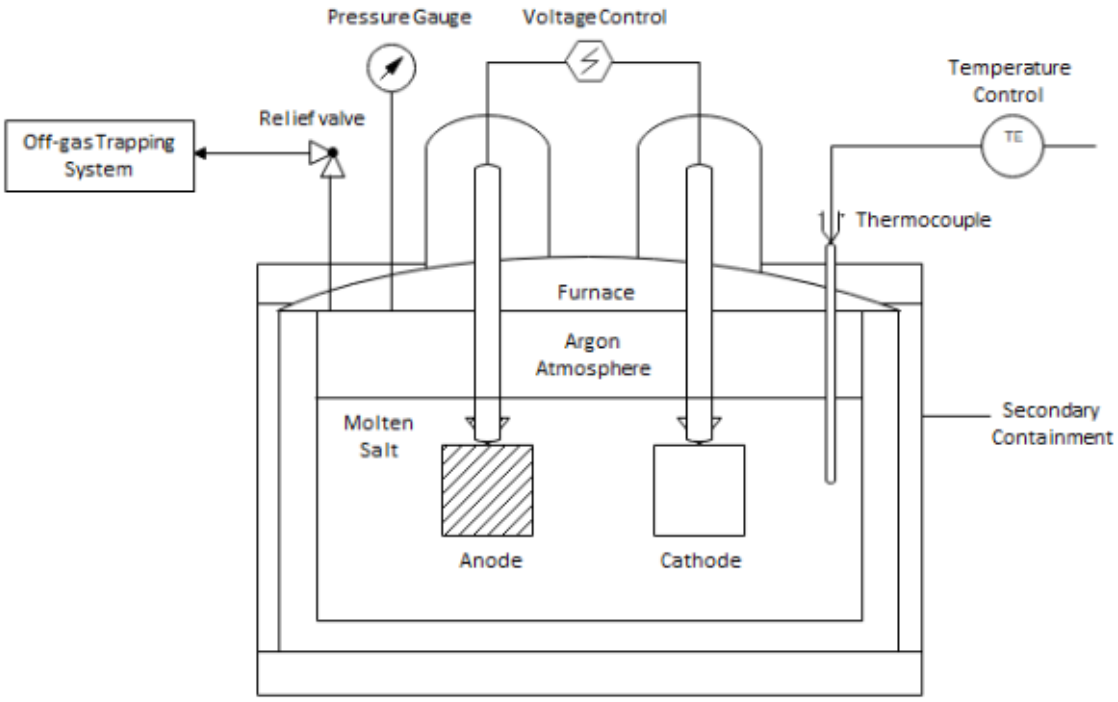

Figure 3.8: PFD of an electroreducer, an electrorefiner, and an electrowinning apparatus. Cathodes, salt electrolytes, temperature conditions, etc. are different for different processes. A pressure gauge is to monitor the system pressure, and a thermocouple measures temperature in the salt. The secondary containment is for blocking radiation spill, and the relief valve is to release pressure in the furnace.

- **Less pressure in the electroreducer, the electrorefiner, or the electrowinning device:** If there was a leak of molten salt from the batch, and the pressure decreased, radioactive materials in the salt can be released to the outside of the furnace. Therefore, the secondary containment, which is the surrounding storage container for preventing material spillage, can be installed around this primary equipment. A pressure gauge must be installed to monitor pressure change in the system.

- **High temperature:** High temperature (much higher than 650^oC) delivers the risk of fire ignition. Thermocouple installation to check the functionality of the heater is critical. The malfunctioning heater must be repaired before re-starting the operation again. The automatic system for power shutdown can limit the maximum operating temperature.

- **High pressure:** Gas buildup can induce high pressure, and the resulting equip-

ment rupture is not favorable due to the possibility of salt spillage. Safety relief valve installation or valve actuation releases the pressure in the system. High voltage may increase the system pressure by generating Cl_2 gas, which is a hazardous material. When the pressure exceeds a certain threshold, the system must automatically shut down, or the operator can actuate the system shutdown.

- **More or less reaction time:** Optimizing the reduction productivity with various lab-scale or engineering-scale experiments determines the ultimate reaction time of the process along with other operation conditions, such as the amount of feed material, cathode and anode types, salt type, etc. If it took more or less time than the determined reaction time given for producing a targeted amount of products, we expect the process efficiency to be low. In this case, further inspection would be needed to check if there are any mechanical failures with the equipment or operation problems.

- **Fast or slow reaction speed:** The electroreduction rate can be fast or slow depending on the amount of Li_2O in the electrochemical cell. If the Li_2O concentration is larger than ∼3 wt%, it can react with the products, which induces less reduction efficiency [136]. If it is less than ∼3 wt%, anodic dissolution might occur, which is not desirable because the anode must not be part of the reaction, and it may increase the impurities in the salt by providing Pt ions. These ions can possibly travel to a cathode and be reduced with the products, which also increase impurities in them. For electrorefining, UCl_3 is loaded for the reaction initiation [95]. Without UCl_3, this process may significantly slow down since it takes some time for uranium ions to travel to a cathode. Additionally, high or low voltage affects the reaction rate, and the frequent calibration for voltage supply equipment would be helpful to bring accurate potential levels for reactions.

- **High voltage supplied:** High voltage may dissolute the anode and produce a hazardous material of Cl_2 gas. The electric potential of <3.4V is to prevent Cl_2 gas generation for the electroreduction process [142]. Electrorefining recovers the U product at the cell voltage of -1.4V [129]. Electrowinning requires a higher cell potential than that for electrorefining to recover TRU. The automatic power shutdown system or the power shutdown actuation temporarily gives some time to resolve issues associated with the malfunctioning voltage supply equipment.

Table 3.3: HAZOP table for electroreduction, electrorefining, and electrowinning

Guide word	Deviation	Possible causes	Consequences	Protection methods
Parameter: **Pressure**				
More of	High pressure	Cl_2 buildup in the system, High voltage	Machinery rupture, Hazardous material release, Explosion/fire	Use of proper materials for the equipment, which are designed to withstand high pressure, Actuation for power shutdown, or the automatic power shutdown installation, Safety relief valve, Valve actuation, Pressure gauge installation
Less of	Low pressure	Small leaks of gas/molten salt	Molten salt/gas might be released to the outside of the reactor	Secondary containment, Pressure gauge installation
Parameter: **Salt level**				
More of	High level	More than required molten salt is provided	Low power efficiency; It takes more time to heat up large amount of salt to a certain temperature	Salt level monitor
Less of	Low level	Less molten salt is provided	The cathode and the anode might not be fully immersed in the salt; Less reduction efficiency	Salt level monitor; more salt needs to be transferred into the electrolytic reducer
Parameter: **Temperature**				
More of	High temperature	Heater malfunction	Machinery malfunction, Fire may be started, Possible low reduction efficiency	Thermocouple installation, Heater repair, Actuation for power shutdown, or the automatic power shutdown installation
Less of	Low temperature	Heater malfunction	Low reduction efficiency, Solidification of molten salt	Thermocouple installation, Heater repair

Table 3.3 (*Continued*)

Guide word	Deviation	Possible causes	Consequences	Protection methods
Parameter: **Time**				
More of	Too long	Long process time	Reduced process efficiency; A lot of metal products deposit on the cathode, and some might fall off from the cathode	Reaction time set up; It must provide optimum reduction efficiency
Less of	Too short	Short process time	Reduced reduction efficiency; Too less metal products on the cathode	Reaction time set up; The cathode basket is separated from the salt after process
Parameter: **Reaction**				
More of	Fast reaction	Large load of Li_2O (electroreduction), Large load of UCl_3 (electrorefining), High voltage; High current	Less reduction efficiency, Reaction between Li_2O and produced uranium metal (electoreduction)	< ~ 3% of Li_2O added[a], Adequate amount of UCl_3 loading [b], Voltage supply equipment calibration
Less of	Slow reaction	Small load of Li_2O (electroreduction), Small load of UCl_3 (electrorefining), Low voltage; Low current	Less reduced products, Anodic dissolution of the anode (electroreduction), Slow reaction initiation (electrorefining)	
None of	No reaction	No salt, or salt does not touch the cathode or the anode (no complete circuit), No fuel elements loaded (electroreduction, electrorefining), No voltage applied (power failure)	No reduction; no products	Salt transfer to the machine, Fuel elements added in a cathode basket, Backup power
Parameter: **Utility**				
None	Failure	Power for the heater not supplied, No electrolysis	No product generation	Backup power

Table 3.3 (*Continued*)

Guide word	Deviation	Possible causes	Consequences	Protection methods
Parameter: **Voltage**[c]				
More of	High voltage	Malfunctioning voltage supply	Anodic dissolution, Cl_2 production (hazardous material)	Automatic power shutdown system, or power shutdown actuation
Less of	Low voltage	Malfunctioning voltage supply	Low extraction efficiency	Voltage supply equipment repair

[a]Less than 3 wt% of Li_2O can be added to speed up the reduction rate. It also prohibits the anodic dissolution. Adding much Li_2O is not an ideal case since it can induce the reaction between Li_2O and the produced uranium metal [136].
[b]UCl_3 loading is for initiating the reaction. A large amount of UCl_3 must be added when the U throughput per batch load is substantial vice versa [95].
[c]For electroreduction, the electric potential of <3.4V is needed not to generate Cl_2. For the U recovery, the cell voltage of -1.4V is given for electrorefining [129]. Electrowinning requires a higher cell potential to reduce TRU.

Safeguardability approach. Electroreduction uses a different salt than electrorefining and electrowinning. In the event of a low pressure malfunction, there could be loss of environment or salt leakage. Since TRUs remain in either of the salts, any leak presents an accounting challenge because TRUs have to be extracted and recovered from the leaked quantity, and this may be extremely challenging. Salt cannot be disposed and expelled from the facility unless safeguards are terminated on the material. With all of these processes in a single hot cell, cleanup could pose a higher potential of material diversion because the accurate TRU measurement becomes impractical, especially if the salts inadvertently mixed. We then suggest a separate cell for electroreduction, isolated from electrorefining and electrowinning. If there is a KMP installed at the exit of the voloxidation process, in the event of a leak in the electroreduction cell, maintaining continuity of knowledge in accounting can pose less difficulty.

Another KMP should be installed at the exit of electroreduction. Batch weight measurements might be problematic because there are uncertainties due to the extraction of the fission products, such as Sr and Cs. Product reduction efficiency is dependent on parameters such as applied voltage, temperature, electrolyte type, salt type, etc. Therefore, accurate batch weight measurements might be difficult to determine early in the facility life cycle with a lack of operational history of electroreduction on a commercial scale. However, the $^{244}Cm/Pu$ ratio and coincidence counting still might be

useful at this stage [64], [68]. Destructive assay at this KMP may be prudent if a weight measurement is not reliable. With the design suggestion of two separate hot cells for electroreduction separate from electrorefining and electrowinning, additional material transfer between these cells may affect overall materials processing goals. However, equipment failures due to operational deviations might lead to false alarms; i.e., Type I errors [11], which could shut down the facility for extended periods of time in order to resolve them.

Because electrorefining and electrowinning employ the same salt, design concepts typically include these processes as a single unit, where the solid and liquid cathodes are inserted into the salt, and extraction occurs simultaneously. We assume this would be the standard design approach for a commercial facility. With the KMP installed at the exit of an electroreduction cell, continuity of knowledge again can be maintained. Accounting on exit at the end of these processes may be difficult because TRU metal is collected on the liquid cadmium cathode, sent to a distillation process to remove the Cd salt, and fabricated into ingots, which are used as feedstock for fuel fabrication. Here, use of the $^{244}Cm/Pu$ ratio may not be reliable as an accounting technique for electrorefining because this ratio in the salt is not same as that in the cathode deposition [45], but this still requires experimental validation. Additionally, for a 20 kg batch of electroreduced metal product, only several hundred grams of TRU can be extracted, and several kilograms of TRU are needed per batch as feed into the fuel fabrication process [7], [8]. Therefore, while destructive assay seems necessary at this stage, excessive assay on each TRU batch might waste too much of the material. Since operational history of extraction efficiency during commercial activity has not yet been acquired, use of weight measurements might also not be reliable. Therefore, due to the need of several kilograms of TRU for a single batch of metal fuel fabrication, a period of time is needed to build a storage buffer of this material. A KMP could be installed prior to distillation, where several batches of TRU/Cd could be compared collectively. Ideally, each would exhibit nearly equal weights within uncertainties. This could reduce the amount of material used for destructive assay.

A fire poses catastrophic consequences. Due to which, the materials in these processes can volatilize, and the continuity of knowledge might be not be maintained. Avoidance of a fire is dependent upon maintaining a robust Ar atmosphere control system and applying defense in depth. This is discussed in the subsequent study node.

3.4.5.3 Ar Atmosphere Control System (Node 5)

An inert atmosphere environment is essential to safely utilize the high-temperature molten salt technology [141]. Accidents such as a component eruption, fire, or the radiation release can possibly happen in the facility handling radioactive materials at high temperatures. Therefore, proper control of oxygen and moisture concentration in hot cells is a key point for the system safety. We consider the Ar atmosphere control system for Node 5, and its PFD is shown in Figure 3.9. Process parameters such as pressure, flow rate, temperature, composition, and time are coupled with suitable guide words. The corresponding deviations determine abnormal situations associated with the Ar atmosphere shown in Table 3.4.

- **High pressure and temperature in a hot cell facility:** If the Ar gas were not circulated well, it would build up the pressure and induce cracks on the windows (cells). The following explosion or radiation release is not favorable. Also, high heat generated from the sub-processes and the loss of Ar may start the fire. The materials processed in the facility are pyrophoric, which can spontaneously ignite when exposed to air [118], [143]. The ventilation fans and relief valves can release pressure to prevent these severe consequences [141]. Similarly, for the pipings, safety relief valves and valve actuation decrease the system pressure when it exceeds the pressure limit. In addition, pressure and temperature sensors can continually monitor cell conditions and alarm if there are any abnormal situations.

- **No pressure induced from no Ar supply:** A disconnected pipe loop can not supply the Ar gas into the hot cell. Broken pumps or closed valves also halt gas circulation. In these cases, the residual Ar gas in the cell cannot be circulated and would be heated. Both pressure and temperature buildup may eventually cause fire or induce radiation release. The consequences are described in detail above. The backup loop installation helps to supply Ar in a safe and timely manner while repairing the disconnected pipes. In addition, valve actuation lets the flow enter the cell.

- **Too long process time:** If it took much time for the Ar circulation, the hot cell might heat up, which may induce high pressure and consequently, cracks on cell walls. This may lead to radiation release to the outside of the cell.

- **Ar supply process skipped:** Ar gas might not be supplied to the cell because of pump failure or closed valves. Heat may build up in the cell, and it follows the same consequences for the long process time.
- **Less flow to the cell and low concentration:** It increases the impurities of the Ar atmosphere. The flowmeter must be installed to control the Ar flow going into the cell, and the analyzers measure the oxygen and moisture concentrations. Alarms can possibly alert the risk of fire. Indeed, malfunctioning pumps or pipe leaks must be fixed.

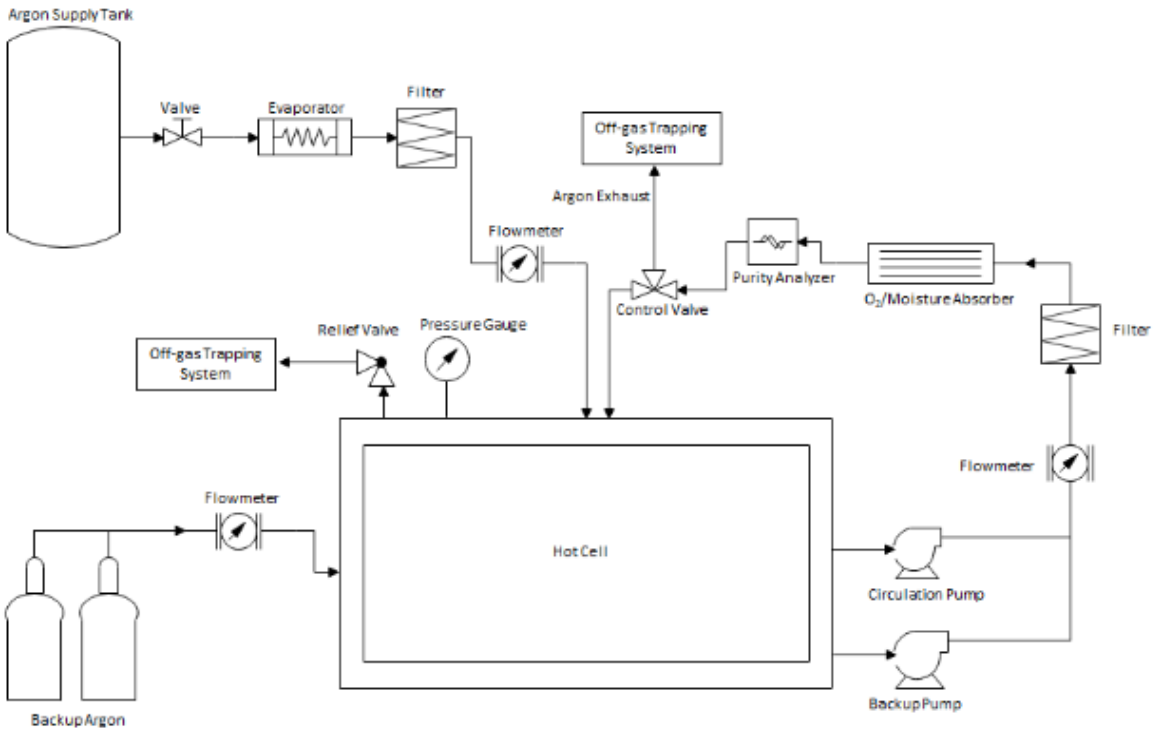

Figure 3.9: PFD of the Ar atmosphere control system. The backup Ar tanks are needed in the event of primary Ar supply failure. The flowmeter controls the Ar gas flow, and circulation pumps maintain the Ar flow in and out of the hot cell. The oxygen/moisture absorber controls the oxygen/moisture content in the gas.

Safeguardability approach. Given that the materials processed in the facility are pyrophoric, the Ar atmosphere is crucial. Loss of the Ar atmosphere clearly affects NMA if air ingress to the hot cells results in a fire, possibly releasing SNM and other radioactive materials. The Ar atmosphere is required for the hot cells designed for electroreduction, electrorefining, and electrowinning. In case radioactive materials are

released from these subsystems, the installation of the nuclear grade high efficiency particulate air (HEPA) filtration systems is mandatory to constrain radiation in the hot cells. Some radiation monitoring systems also show the radiation levels in the cells. Part of maintenance on the Ar system can be to test for leaks regularly. Within the context of safeguardability, a shutdown may be necessary if a leak is discovered above a certain threshold. One of the benefits to locating subsystems in separate hot cells would be that a leak in one cell does not affect other materials in different cells. This can maintain continuity of knowledge if the damaged cell is then shut down, and any transfers into and out of it are halted.

Table 3.4: HAZOP table for the argon (Ar) atmosphere control system

Guide word	Deviation	Possible causes	Consequences	Protection methods
Parameter: **Pressure**				
More of	High pressure	Stuck valve, Heat introduced to the Ar atmosphere	Windows (cells) cracked or broken	Safety relief valve, Use of proper materials, which are designed to withstand high pressure, Ventilation fans, Valve actuation
Less of	Low pressure	Small pipe rupture/leakage	Low Ar supply to cells	Pressure gauge installation, Pipe rupture repair
None of	No pressure	Loop disconnected (Ar can not be supplied.), Broken pumps, Closed valves	Loss of the Ar atmosphere, or Pressure and heat buildup in hot cells (no gas circulation)	Installation of backup loop for Ar supply to hot cells, Pipe repair
Parameter: **Flow (rate)**				
More of	High flow	Pump malfunction	Fast pump wear out, Economic loss	Sensitive flow meter installation
Less of	Low flow	Small pipe leaks, Pipe rupture, Pump malfunction, Valve partial opening	Increased impurities in Ar atmosphere, Low Ar supply to cells	Flow meter installation, Pipe rupture repair, Pump replacement, Valve actuation
None of	No flow	Valve closed, pump failure	No Ar circulation, Heat buildup in hot cells, Windows (cells) cracked or broken, Pressure buildup in the piping system	Valve actuation and repair, Pump repair Safety relief valve
Reverse	Reverse flow	Pump failure	High pressure, temperature in the cell,	Pump repair
Parameter: **Temperature**				
More of	High temperature	Stuck valve, Pump failure	Heat buildup, Pressure buildup	Use of proper shielding materials which are designed to withstand high heat,

Table 3.4 (*Continued*)

Guide word	Deviation	Possible causes	Consequences	Protection methods
			Windows (cells) cracked or broken	Ventilation fans, Safety relief valve, Valve actuation, Pump repair
Less of[a]	Low temperature	Well-circulated Ar gas	N/A	
Parameter: **Composition**				
More of[b]	High Ar concentration	Operating Ar circulation system[c]	N/A	
Less of	Low Ar concentration	Pipe rupture, Flow leak, Malfunctioning circulation system	Fire, or explosion in hot cells	Installation of oxygen & moisture analyzers, Alarms (moisture > 15 ppm, oxygen > 40 ppm) (Ku, J.H. et al, 2012)
Parameter: **Circulation Time**				
More of	Too long	Low capacity of Ar flow allowed in pipes, Slow pump speed, Valve partial opening	Poor Ar circulation, Heat buildup in hot cells	Pump speed control, Safety relief valve, Valve actuation
Less of	Too short	High capacity of Ar flow allowed in pipes, Fast pump speed	Unnecessary electricity cost for pump, Fast equipment wear out	Modification in pipe size, Adjustment of pump speed
None of	Ar supply process skipped	Valve closed, pump failure	Heat buildup & pressure buildup in cells, Windows cracked or broken	Ar control system repair

[a]When the Ar gas is circulated well in the facility, temperature in hot cells might get low compared to the expected value. It may overuse the power or wear out the pumps fast. However, we don't anticipate severe accident scenarios from the 'low temperature' situation.
[b]High concentration of Ar in hot cells will help to safely perform all the sub-processes for reprocessing spent nuclear fuel. Though, excess power may be used in this case.
[c]More details of the Ar circulation system is shown in [141].

3.4.6 Future Work

There exists substantial upcoming work to develop the full HAZOP analysis on this facility. This is a worthwhile beginning in that no HAZOP studies on a commercial pyroprocessing facility have been performed in the past. The present study primarily focuses on operation processes, which carry chemical changes of feed materials. The following outcomes would be useful to facilitate the implementation of a safe, reliable commercial pyroprocessing facility and for the subsequent quantitative risk assessment.

The next phase of HAZOP analysis will cover metal fuel fabrication and the auxiliary systems for salt distillation and salt recycle. Following this, analysis will focus on waste treatment and termination of safeguards. Fuel fabrication is a complex process. Major study nodes will be identified for the injection casting system and for the trimmer. Subsequent nodes will include the processes necessary for rod and assembly production. Moreover, the HAZOP study on material transfers, including salt transfer, must be addressed since moving radioactive materials through pipes requires strict regulations for the system safety. Transfer technologies, such as gravitational transfer or a Vacuum Induced Salt Transfer and Storage (VISTAS) system, must be studied in detail to assess operational problems as well as safeguards issues. Additionally, further study includes human reliability due to errors from using manipulators for remote handling. Incorporating human errors into HAZOP is complex, and this will be performed after the complete HAZOP for machinery and operability problems.

3.4.7 Summary Remarks

HAZOP is a useful tool in studying operational deviations of an industrial process, determining consequences, and developing protective measures. In this paper, we have applied an enhanced HAZOP approach to a commercial pyroprocessing facility that not only includes identification of hazards, but additionally provides risk-informed design suggestions within the concept of safegurdability. The operability issues caused by off-normal situations have been studied and planned with protection methods to mitigate or prevent their potential accident scenarios. We identified the following severe consequences:

- Pressure buildup from heated atmosphere may lead to cracked or broken windows (cells). Consequently, radioactive materials can be released to the outside of the cell. In particular, pressure buildup in the pipelines of the Ar control system or

in individual subsystems may result in pipe or equipment rupture, and eventual radiation release. High pressure in the confined container may possibly cause explosion.

- An economic loss of cost can induce from the unnecessary power supply, too much feed, too much gas flow, etc.
- Process inefficiency is introduced because of low or no gas flow, low or no feed, much salt in the batch, electrodes not fully immersed in the salt, and an inadequate amount of Li_2O or UCl_3. In addition, abnormal operating conditions decrease the system efficiency.
- A high cell potential may produce an undesired hazardous material, Cl_2.
- Ar loss may start fire due to the existence of pyrophoric materials in the cell and the air supplied.

We also have suggested the following design components as part of the safeguardability approach:

- The U_3O_8 powder dispersal is an accounting challenge. To confine the used fuel powder, protective membranes must be installed.
- The $^{244}Cm/Pu$ ratio and coincidence accounting can possibly be used for some subprocesses to frequently monitor the Pu content in SNM. The weight measurement at KMP can also be used as a SNM counting technique, and KMP locations are determined for implementation of strong safeguards.
- From the safeguards perspective, installation of several hot cells for subprocesses is necessary.

This HAZOP will certainly facilitate obtaining a license for installation of a commercial-scale pyroprocessing facility, and possible severe consequences would not occur or be mitigated. A quantitative risk assessment will be introduced next. The risk-informed design suggestions in the context of safeguardability will allow the design specifications for the facility operation with robust safeguards.

References

[1] C. Behar, "Technology roadmap update for generation IV nuclear energy systems," in *OECD Nuclear Energy Agency for the Generation IV International Forum*, 2014.

[2] International Atomic Energy Agency (IAEA), "Climate change and nuclear power 2016," 2016.

[3] M. H. Ehinger and S. J. Johnson, "Lessons learned in international safeguards - Implementation of safeguards at the Rokkasho reprocessing plant," *ORNL/TM-2010/23, Oak Ridge National Laboratory*, 2009.

[4] S. J. Johnson and M. Ehinger, "Designing and operating for safeguards: Lessons learned from the Rokkasho reprocessing plant (RRP)," Pacific Northwest National Laboratory (PNNL), Richland, WA (US), Tech. Rep., 2010.

[5] R. Borrelli, "The high reliability safeguards approach for safeguardability of remotely-handled nuclear facilities: 1. Functional components to system design," *J. Nucl. Mater. Manage*, vol. 42, no. 3, p. 4, 2014.

[6] ——, "The high reliability safeguards approach for safeguardability of remotely-handled nuclear facilities: 2. A risk-informed approach for safeguards," *J. Nucl. Mater. Manage*, vol. 42, no. 3, p. 27, 2014.

[7] ——, "Use of curium spontaneous fission neutrons for safeguardability of remotely-handled nuclear facilities: Fuel fabrication in pyroprocessing," *Nuclear Engineering and Design*, vol. 260, pp. 64–77, 2013.

[8] ——, "Use of curium neutron flux from head-end pyroprocessing subsystems for the high reliability safeguards methodology," *Nuclear Engineering and Design*, vol. 277, pp. 166–172, 2014.

[9] ——, "Functional components for a design strategy: Hot cell shielding in the high reliability safeguards methodology," *Nuclear Engineering and Design*, vol. 305, pp. 18–27, 2016.

[10] G. A. Wainer and P. J. Mosterman, *Discrete-event modeling and simulation: Theory and applications*. CRC Press, 2016.

[11] R. Avenhaus, *Material accountability: theory, verification, and applications*. John Wiley & Sons, 1977.

[12] IAEA, "IAEA safeguards glossary, 2001 edition," *International Nuclear Verification Series No.3*, 2002.

[13] S. Herrmann, S. Li, M. Simpson, and S. Phongikaroon, "Electrolytic reduction of spent nuclear oxide fuel as part of an integral process to separate and recover actinides from fission products," *Separation Science and Technology*, vol. 41, no. 10, pp. 1965–1983, 2006.

[14] S. D. Herrmann, S. X. Li, and B. R. Westphal, "Separation and recovery of uranium and group actinide products from irradiated fast reactor MOX fuel via electrolytic reduction and electrorefining," *Separation Science and Technology*, vol. 47, no. 14-15, pp. 2044–2059, 2012.

[15] S. Herrmann and S. Li, "Separation and recovery of uranium metal from spent light water reactor fuel via electrolytic reduction and electrorefining," *Nuclear Technology*, vol. 171, no. 3, pp. 247–265, 2010.

[16] S. Phongikaroon, S. D. Herrmann, and M. F. Simpson, "Diffusion model for electrolytic reduction of uranium oxides in a molten $LiCl$-Li_2O salt," *Nuclear Technology*, vol. 174, no. 1, pp. 85–93, 2011.

[17] S. X. Li, S. D. Herrmann, and M. F. Simpson, "Experimental investigations into U/TRU recovery using a liquid cadmium cathode and salt containing high rare earth concentrations," Idaho National Laboratory (INL), Tech. Rep., 2009.

[18] ——, "Electrochemical analysis of actinides and rare earth constituents in liquid cadmium cathode product from spent fuel electrorefining," *Nuclear technology*, vol. 171, no. 3, pp. 292–299, 2010.

[19] C. Trybus, J. Sanecki, and S. Henslee, "Casting of metallic fuel containing minor actinide additions," *Journal of nuclear materials*, vol. 204, pp. 50–55, 1993.

[20] D. E. Burkes, R. S. Fielding, and D. L. Porter, "Metallic fast reactor fuel fabrication for the global nuclear energy partnership," *Journal of Nuclear Materials*, vol. 392, no. 2, pp. 158–163, 2009.

[21] C. Lee, J. Cheon, S. Kim, J. Park, and H. Joo, "Metal fuel development and verification for prototype generation IV sodium-cooled fast reactor," *Nuclear Engineering and Technology*, vol. 48, no. 5, pp. 1096–1108, 2016.

[22] J. Battles, W. Miller, M. J. Lineberry, and R. Phipps, "IFR fuel cycle," Argonne National Lab., IL, Tech. Rep., 1992.

[23] H. F. McFarlane and M. J. Lineberry, "The IFR fuel cycle demonstration," *Progress in Nuclear Energy*, vol. 31, no. 1-2, pp. 155–173, 1997.

[24] S. Kuk, K. Kim, J. Kim, H. Song, S. Oh, J. Park, C. Lee, Y. Youn, and J. Kim, "Phase characteristics of rare earth elements in metallic fuel for a sodium-cooled fast reactor by injection casting," *Journal of Nuclear Materials*, vol. 486, pp. 53–59, 2017.

[25] A. Houshyar, "Review of extend^{TM} performance in modeling a nuclear fuel transfer activity," *Simulation*, vol. 68, no. 6, pp. 403–412, 1997.

[26] H. E. Garcia and A. Houshyar, "Discrete event simulation of fuel transfer strategies for defueling a nuclear reactor," *Simulation*, vol. 70, no. 2, pp. 104–118, 1998.

[27] H. E. Garcia, "Operational analysis and improvement of a spent nuclear fuel handling and treatment facility using discrete event simulation," *Computers & industrial engineering*, vol. 38, no. 2, pp. 235–249, 2000.

[28] H. Lee, S. Kim, and B. Park, "Discrete event system simulation approach for an operation analysis of a headend process facility," *Nuclear Engineering and Technology*, vol. 41, no. 5, pp. 739–746, 2009.

[29] H. Lee, K. Kim, H. Kim, and H. Lee, "Discrete event dynamic system (DES) - based modeling for dynamic material flow in the pyroprocess," *Annals of Nuclear Energy*, vol. 38, no. 4, pp. 860–875, 2011.

[30] H. Lee, W. Ko, I. Kim, and H. Lee, "Design for integrated pyroprocessing plant level simulator," *Annals of Nuclear Energy*, vol. 60, pp. 316–328, 2013.

[31] T. Riley, C. Pope, and R. Benedict, "Safeguards performance model for evaluation of potential safeguards strategies applied to pyroprocessing facilities," *Nuclear Engineering and Design*, vol. 301, pp. 157–163, 2016.

[32] H. E. Garcia, M. Simpson, W. Lin, T. Yoo, and R. Carlson, "Detecting proliferation activities via system-centric integration and interpretation of multi-modal data collected from a system of sensors," *Proc. 54th Annual INMM, Palm Desert, California*, 2013.

[33] H. E. Garcia, M. F. Simpson, W. Lin, R. B. Carlson, and T. Yoo, "Application of process monitoring to anomaly detection in nuclear material processing systems via system-centric event interpretation of data from multiple sensors of varying reliability," *Annals of Nuclear Energy*, vol. 103, pp. 60–73, 2017.

[34] PRPPWG, "Evaluation methodology for proliferation resistance and physical protection of generation IV nuclear energy systems," 2011.

[35] ——, "PR&PP evaluation: ESFR full system case study final report," 2009.

[36] R. A. Bari, "Proliferation resistance and physical protection evaluation methodology: Objectives, accomplishments, and future directions," *Nuclear Technology*, vol. 179, no. 1, pp. 35–44, 2012.

[37] B. D. Boyer, H. H. Erpenbeck, and C. P. Scherer, "Implications for advanced safeguards derived from a proliferation resistance and physical protection case study for a generation IV nuclear energy system," *Nuclear Technology*, vol. 179, no. 1, pp. 61–69, 2012.

[38] G. G. Cojazzi, G. Renda, J. S. Choi, and J. Hassberger, "Applying the GIF PR&PP methodology for a qualitative analysis of a misuse scenario in a notional generation IV Example Sodium Fast Reactor," *Nuclear Technology*, vol. 179, no. 1, pp. 76–90, 2012.

[39] P. F. Peterson, "Elements of the proliferation resistance and physical protection evaluation methodology," *Nuclear Technology*, vol. 179, no. 1, pp. 45–51, 2012.

[40] J. F. Pilat, "The proliferation resistance debate and the proliferation resistance and physical protection evaluation methodology," *Nuclear Technology*, vol. 179, no. 1, pp. 31–34, 2012.

[41] ——, "Implementation of the PR&PP methodology: the role of formal expert elicitations," *Nuclear Technology*, vol. 179, no. 1, pp. 52–60, 2012.

[42] J. J. Whitlock, N. Inoue, M. Senzaki, D. Bley, and E. Wonder, "Proliferation resistance of a hypothetical sodium fast reactor under an assumed breakout scenario," *Nuclear Technology*, vol. 179, no. 1, pp. 91–96, 2012.

[43] M. D. Zentner, G. A. Coles, and I. U. Therios, "A qualitative assessment of diversion scenarios for an Example Sodium Fast Reactor using the generation IV PR&PP methodology," *Nuclear Technology*, vol. 179, no. 1, pp. 70–75, 2012.

[44] B. B. Cipiti, F. A. Duran, B. Key, Y. Liu, I. Lozano, and R. Ward, "Modeling and design of integrated safeguards and security for an electrochemical reprocessing facility," *Sandia National Laboratories, SAND2012-9303, Albuquerque, NM, USA*, 2012.

[45] M. Gonzalez, L. Hansen, D. Rappleye, R. Cumberland, and M. Simpson, "Application of a one-dimensional transient electrorefiner model to predict partitioning of plutonium from curium in a pyrochemical spent fuel treatment process," *Nuclear Technology*, vol. 192, no. 2, pp. 165–171, 2015.

[46] H. Kim, H. Shin, and S. Ahn, "Status and prospect of safeguards by design for the pyroprocessing facility," in *Symposium of International Safeguards*, 2010.

[47] S. Kim, C. Kim, K. Kim, and H. Kim, "Study on graphic simulator to analyze a possibility of remote operation for process equipments using a pride digital mockup," in *Control Automation and Systems (ICCAS), 2010 International Conference*. IEEE, 2010, pp. 775–778.

[48] S. Kim, K. Kim, and H. Kim, "Analysis of accessibility for the remote operation of process equipments in the pride digital mockup," in *Control, Automation and Systems (ICCAS), 2011 11th International Conference*. IEEE, 2011, pp. 1041–1044.

[49] G. You, W. Choung, E. Lee, D. Hong, W. Lee, J. Ku *et al.*, "Concept and safety studies of an integrated pyroprocess facility," *Nuclear Engineering and design*, vol. 241, no. 1, pp. 415–424, 2011.

[50] Y. Hwang, "Summary of the KAERI's KIEP-21 pyroprocessing, v0.5," *Korean Atomic Energy Research Institute, Republic of Korea*, 2009.

[51] UCBNE-KAERI collaboration, "A summary on metallic fuel fabrication: Systems assessment for advanced nuclear fuel cycle," UC-Berkeley, Berkeley, California, Tech. Rep., 2009.

[52] ——, "KAERI activity of metallic fuel fabrication: Systems assessment for advanced nuclear fuel cycle," Presentation, 2010.

[53] R. Borrelli, L. Kim, E. Blandford, Y. Hwang, E. H. Kim, and P. F. Peterson, "High reliability safeguards for remote-handled nuclear materials," in *Proceedings of the 2010 International Congress on Advances in Nuclear Power Plants-ICAPP'10*, 2010.

[54] C. H.L., "Systems assessment for advanced nuclear fuel cycle," Email discussion, 2011.

[55] H. H. Lee, W. I. Ko, H. L. Chang, D. Y. Song, E. H. Kwon, and J. W. Lee, "Basic requirements for a preliminary conceptual design of the Korea advanced pyroprocess facility (KAPF)," Korea Atomic Energy Research Institute, Tech. Rep., 2008.

[56] F. Gao, W. I. Ko, C. J. Park, and H. H. Lee, "Criticality safety evaluation of materials concerning pyroprocessing," *Journal of nuclear science and technology*, vol. 48, no. 6, pp. 919–928, 2011.

[57] J. McCool, *Using the Weibull distribution: reliability, modeling, and inference*. John Wiley & Sons, 2012, vol. 950.

[58] S. Deming, Y. Michotte, D. L. Massart, L. Kaufman, and B. Vandeginste, *Chemometrics: a textbook*. Elsevier, 1988, vol. 2.

[59] R. Borrelli and M. Tolman, "Development of a discrete event simulation model for pyroprocessing safeguardability," *Trans Am. Nucl. Soc*, vol. 115, p. 901, 2016.

[60] J. Zhang, "Safeguards in pyroprocessing: An integrated model development and measurement data analysis," The Ohio State University, Columbus, OH (United States). Research Foundation, Tech. Rep., 2017.

[61] T. Bjornard, R. Bean, P. C. Durst, J. Hockert, and J. Morgan, "Implementing safeguards-by-design," Idaho National Laboratory (INL), Tech. Rep., 2010.

[62] IAEA, "International safeguards in nuclear facility design and construction," *IAEA nuclear energy series*, no. NP-T-2.8, 2013.

[63] J. Lee, M. Tolman, and R. Borrelli, "High reliability safeguards approach to remotely handled nuclear processing facilities: Use of discrete event simulation for material throughput in fuel fabrication," *Nuclear Engineering and Design*, vol. 324, pp. 54–66, 2017.

[64] P. C. Durst, I. Therios, R. Bean, A. Dougan, B. Boyer, R. Wallace, M. H. Ehinger, D. N. Kovacic, and K. Tolk, "Advanced safeguards approaches for new reprocessing facilities," Pacific Northwest National Laboratory (PNNL), Richland, WA (US), Tech. Rep., 2007.

[65] S. Johnson, R. Abedin-Zadeh, C. Pearsall, K. Hiruta, C. Creusot, M. Ehinger, E. Kuhn, B. Chesnay, N. Robson, H. Higuchi *et al.*, "Development of the safeguards approach for the Rokkasho reprocessing plant," *IAEA*, vol. 367, no. 8, p. 01, 2001.

[66] J. Lee and R. Borrelli, "Hazard and operability analysis of a pyroprocessing facility," *Nuclear Engineering and Design*, 2018 [under review].

[67] D. Rappleye *et al.*, "Developing safeguards for pyroprocessing: Detection of a plutonium co-deposition on solid cathode in an electrorefiner by applying the signature-based safeguards approach," 2012.

[68] R. Bean, "Project report on development of a safeguards approach for pyroprocessing," Idaho National Laboratory (INL), Tech. Rep., 2010.

[69] C. L. Murphy, "Developing a signature based safeguards approach for the electrorefiner and salt cleanup unit operations in pyroprocessing facilities," Los Alamos National Lab.(LANL), Los Alamos, NM (United States), Tech. Rep., 2016.

[70] D. Rappleye, M. Simpson, R. Cumberland, D. McNelis, and M. Yim, "Simulated real-time process monitoring of a molten salt electrorefiner," *Nuclear Engineering and Design*, vol. 273, pp. 75–84, 2014.

[71] U.S. Congress, "Nuclear safeguards and the International Atomic Energy Agency," *Washington, DC, Office of Technology Assessment*, vol. Regulatory Guide 5.33, 1995.

[72] R. O. Hoover, S. Phongikaroon, M. F. Simpson, S. X. Li, and T. Yoo, "Development of computational models for the mark-IV electrorefiner–effect of uranium, plutonium, and zirconium dissolution at the fuel basket-salt interface," *Nuclear technology*, vol. 171, no. 3, pp. 276–284, 2010.

[73] A. G. Le Coq, "Design of a safeguards instrument for plutonium quantification in an electrochemical refining system," Ph.D. dissertation, 2013.

[74] R. M. Cumberland and M. Yim, "Development of a 1D transient electrorefiner model for pyroprocess simulation," *Annals of Nuclear Energy*, vol. 71, pp. 52–59, 2014.

[75] P. L. Lafreniere, D. S. Rappleye, R. O. Hoover, M. F. Simpson, and E. D. Blandford, "Demonstration of signature-based safeguards for pyroprocessing as applied to electrorefining and the ingot casting process," *Nuclear Technology*, vol. 189, no. 2, pp. 173–185, 2015.

[76] W. Zhou, Y. Wang, and J. Zhang, "Integrated model development for safeguarding pyroprocessing facility: Part II–case studies and model integration," *Annals of Nuclear Energy*, vol. 112, pp. 48–61, 2018.

[77] U.S. Atomic Energy Commission, "Statistical evaluation of material unaccounted for," *Directorate of regulatory standards*, 1974.

[78] D. G. Cacuci, *Handbook of Nuclear Engineering: Vol. 1: Nuclear Engineering Fundamentals; Vol. 2: Reactor Design; Vol. 3: Reactor Analysis; Vol. 4: Reactors of Generations III and IV; Vol. 5: Fuel Cycles, Decommissioning, Waste Disposal and Safeguards*. Springer Science & Business Media, 2010, vol. 3.

[79] J. Doyle, *Nuclear safeguards, security and nonproliferation: achieving security with technology and policy*. Elsevier, 2011.

[80] K. Pillay, "Fundamentals of materials accounting for nuclear safeguards," Los Alamos National Lab., NM (USA), Tech. Rep., 1989.

[81] D. C. LeBlanc, *Statistics: concepts and applications for science*. Jones & Bartlett Learning, 2004, vol. 2.

[82] B. N. Taylor and C. E. Kuyatt, "Guidelines for evaluating and expressing the uncertainty of NIST measurement results," 1994.

[83] Bureau International des Poids et Mesures (BIPM), "Commission électrotechnique internationale and organisation internationale de normalisation," *Guide to the expression of uncertainty in measurement. International Organization for Standardization*, 1995.

[84] S. L. Ellison, M. Rosslein, A. Williams *et al.*, "Quantifying uncertainty in analytical measurement," in *Quantifying uncertainty in analytical measurement*. Eurachem, 2000.

[85] M. Zhao, M. Penkin, C. Norman, and S. Balsley, "International target values 2010 for measurement uncertainties in safeguarding nuclear materials," *ESARDA Bulletin*, vol. 48, pp. 3–24, 2012.

[86] E. Hakkila, R. Dietz, and J. Shipley, "The role of near-real-time accounting in international safeguards for reprocessing plants," 1979.

[87] D. M. Beazley, *Python essential reference*. Addison-Wesley Professional, 2009.

[88] D. Phillips, *Python 3 object-oriented programming*. Packt Publishing Ltd, 2015.

[89] M. Lutz, *Programming Python: Powerful Object-Oriented Programming*. " O'Reilly Media, Inc.", 2010.

[90] IAEA, "Use of nuclear material accounting and control for nuclear security purposes at facilities," *IAEA Nuclear Security Series No. 25-G*, 2015.

[91] M. Lineberry and R. Phipps, "A demonstration facility for the IFR fuel cycle," in *RECOD 87*, 1987.

[92] J. P. Ackerman, "Chemical basis for pyrochemical reprocessing of nuclear fuel," *Industrial & Engineering Chemistry Research*, vol. 30, no. 1, pp. 141–145, 1991.

[93] C. E. Till and Y. I. Chang, *Plentiful energy: The story of the Integral Fast Reactor, the complex history of a simple reactor technoloogy, with emphasis on its scientific basis for non-specialists*. Charles E. Till and Yoon Il Chang, 2011.

[94] C. Till, Y. Chang, and W. Hannum, "The Intergral Fast Reactor - An overview," *Progress in Nuclear Energy*, vol. 31, no. 1-2, pp. 3–11, 1997.

[95] H. Lee, G. Park, J. Lee, K. Kang, J. Hur, J. Kim, S. Paek, I. Kim, and I. Cho, "Current status of pyroprocessing development at KAERI," *Science and Technology of Nuclear Installations*, 2013.

[96] H. Lee, G. Park, K. Kang, J. Hur, J. Kim, D. Ahn, Y. Cho, and E. Kim, "Pyroprocessing technology development at KAERI," *Nuclear Engineering and Technology*, vol. 43, no. 4, pp. 317–328, 2011.

[97] R. Benedict, C. Solbrig, B. Westphal, T. Johnson, S. Li, K. Marsden, and K. Goff, "Pyroprocessing progress at Idaho National Laboratory," *Advanced Nuclear Fuel Cycles and Systems (GLOBAL 2007)*, 2007.

[98] M. F. Simpson, "Developments of spent nuclear fuel pyroprocessing technology at Idaho National Laboratory," Idaho National Laboratory (INL), Tech. Rep., 2012.

[99] H. S. Shin, S. K. Ahn, D. Y. Song, T. H. Lee, H. D. Kim, J. S. Seo, H. I. Im, and J. N. Jang, "Analysis on the present status of conceptually designed pyroprocessing facilities for determining a reference pyroprocessing facility," Korea Atomic Energy Research Institute, Tech. Rep., 2009.

[100] B. Westphal, G. Fredrickson, G. Galbreth, D. Vaden, M. Elliott, J. Price, E. Honeyfield, M. Patterson, and L. Wurth, "Pyroprocessing of fast flux test facility nuclear fuel," Idaho National Laboratory (INL), Tech. Rep., 2013.

[101] J. J. Laidler, J. Battles, W. Miller, J. Ackerman, and E. Carls, "Development of pyroprocessing technology," *Progress in Nuclear Energy*, vol. 31, no. 1-2, pp. 131–140, 1997.

[102] A. A. Frigo, D. R. Wahlquist, and J. L. Willit, "A conceptual advanced pyroprocess recycle facility." Argonne National Lab.(ANL), Argonne, IL (United States), Tech. Rep., 2003.

[103] M. Glossop, A. Loannides, and J. Gould, *Review of hazard identification techniques*. Health & Safety Laboratory, 2000.

[104] F. Crawley and B. Tyler, *HAZOP: Guide to best practice*. Elsevier, 2015.

[105] G. Wells, *Hazard identification and risk assessment*. IChemE, 1996.

[106] H. Lawley, "Operability studies and hazard analysis," *Chemical Engineering Progress*, vol. 70, no. 4, pp. 45–56, 1974.

[107] D. P. Nolan, *Application of HAZOP and What-If safety reviews to the petroleum, petrochemical and chemical industries*. Noyes Publications,, 1994.

[108] V. Venkatasubramanian, J. Zhao, and S. Viswanathan, "Intelligent systems for HAZOP analysis of complex process plants," *Computers & Chemical Engineering*, vol. 24, no. 9-10, pp. 2291–2302, 2000.

[109] L. Cui, J. Zhao, T. Qiu, and B. Chen, "Layered digraph model for HAZOP analysis of chemical processes," *Process Safety Progress*, vol. 27, no. 4, pp. 293–305, 2008.

[110] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *Journal of hazardous materials*, vol. 173, no. 1-3, pp. 19–32, 2010.

[111] A. C. Guimaraes and C. M. F. Lapa, "Hazard and operability study using approximate reasoning in light-water reactors passive systems," *Nuclear Engineering and Design*, vol. 236, no. 12, pp. 1256–1263, 2006.

[112] L. Burgazzi, "Evaluation of uncertainties related to passive systems performance," *Nuclear Engineering and Design*, vol. 230, no. 1-3, pp. 93–106, 2004.

[113] M. Hashemi-Tilehnoee, A. Pazirandeh, and S. Tashakor, "HAZOP-study on heavy water research reactor primary cooling system," *Annals of Nuclear Energy*, vol. 37, no. 3, pp. 428–433, 2010.

[114] S. Rimkevičius, M. Vaišnoras, E. Babilas, and E. Uškpuras, "HAZOP application for the nuclear power plants decommissioning projects," *Annals of Nuclear Energy*, vol. 94, pp. 461–471, 2016.

[115] K. Jeong, D. Lee, K. Lee, and H. Lim, "A qualitative identification and analysis of hazards, risks and operating procedures for a decommissioning safety assessment of a nuclear research reactor," *Annals of Nuclear Energy*, vol. 35, no. 10, pp. 1954–1962, 2008.

[116] G. Sheppard and J. Taylor, "The safety case for the thermal oxide reprocessing plant at Sellafield," *IAEA*, p. 59, 1993.

[117] M. Ishida, T. Nakano, K. Morimoto, and I. Nojiri, "PSA application on the Tokai reprocessing plant," in *Probabilistic Safety Assessment and Management*. Springer, 2004, pp. 543–548.

[118] S. Moon, S. Seo, W. Chong, G. You, J. Ku, and H. Kim, "Identification of safety controls for engineering-scale pyroprocess facility," *Nuclear Engineering and Technology*, vol. 47, no. 7, pp. 915–923, 2015.

[119] G. W. Mitchell, S. W. Longley, J. S. Philbin, J. A. Mahn, D. T. Berry, N. F. Schwers, T. E. Vanderbeek, and R. E. Naegeli, "Hot cell facility (HCF) safety analysis report," Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US), Tech. Rep., 2000.

[120] S. Moon, W. Chong, G. You, J. Ku, H. Kim, Y. Lim, and H. Chang, "Preliminary safety study of engineering-scale pyroprocess facility," *Nuclear Engineering and Technology*, vol. 46, no. 1, pp. 63–72, 2014.

[121] T. A. Kletz, *HAZOP and HAZAN: Identifying and assessing process industry hazards.* IChemE, 1999.

[122] D. Macdonald, *Practical HAZOPs, trips and alarms.* Elsevier, 2004.

[123] P. Mellinger, K. Harmon, and L. Lakey, "Summary of nuclear fuel reprocessing activities around the world," Pacific Northwest Lab., Richland, WA (USA), Tech. Rep., 1984.

[124] L. Mac Toth, W. D. Bond, and L. R. Avens, "Aqueous and pyrochemical reprocessing of actinide fuels," *JOM*, vol. 45, no. 2, pp. 35–39, 1993.

[125] W. Bond, J. Mailen, and G. Michaels, "Evaluation of methods for decladding LWR fuel for a pyroprocessing-based reprocessing plant," Oak Ridge National Lab TN, Tech. Rep., 1992.

[126] B. Westphal, K. Bateman, C. Morgan, J. Berg, P. Crane, D. Cummings, J. Giglio, M. Huntley, R. Lind, and D. Sell, "Effect of process variables during the head-end treatment of spent oxide fuel," *Nuclear Technology*, vol. 162, no. 2, pp. 153–157, 2008.

[127] J. Lee, H. Ryu, G. Park, and K. Song, "Recent progress on the DUPIC fuel fabrication technology at KAERI," *Gas*, vol. 1, p. 3, 2008.

[128] J. Bodine, I. Groce, J. Guon, and L. Hanson, "Oxidative decladding of uranium dioxide fuels," *Nuclear Science and Engineering*, vol. 19, no. 1, pp. 1–7, 1964.

[129] J. Yoo, C. Seo, E. Kim, and H. Lee, "A conceptual study of pyroprocessing for recovering actinides from spent oxide fuels," *Nuclear Engineering and Technology*, vol. 40, no. 7, pp. 581–592, 2008.

[130] J. Park, I. Jung, and J. Shin, "Development of voloxidation process for treatment of LWR spent fuel," Korea Atomic Energy Research Institute, Tech. Rep., 2007.

[131] J. J. Park, J. Lee, and G. Park, "Development of advanced voloxidation process for treatment of spent fuel," Korea Atomic Energy Research Institute, Tech. Rep., 2010.

[132] Y. H. Kim, H. J. Lee, J. K. Lee, J. H. Jung, B. S. Park, J. S. Yoon, and S. W. Park, "Engineering design of a high-capacity vol-oxidizer for handling UO_2 pellets of tens of kilogram," *Journal of Nuclear Science and Technology*, vol. 45, no. 7, pp. 617–624, 2008.

[133] S. Jeong, J. Hur, S. Hong, D. Kang, M. Choung, C. Seo, J. Yoon, and S. Park, "An electrochemical reduction of uranium oxide in the advanced spent-fuel conditioning process," *Nuclear Technology*, vol. 162, no. 2, pp. 184–191, 2008.

[134] J. Hur, I. Choi, S. Cho, S. Jeong, and C. Seo, "Preparation and melting of uranium from U_3O_8," *Journal of Alloys and Compounds*, vol. 452, no. 1, pp. 23–26, 2008.

[135] S. D. Herrmann, S. X. Li, and M. F. Simpson, "Electrolytic reduction of spent oxide fuel – Bench-scale test results," Idaho National Laboratory (INL), Tech. Rep., 2005.

[136] E. Choi and S. Jeong, "Electrochemical processing of spent nuclear fuels: An overview of oxide reduction in pyroprocessing technology," *Progress in Natural Science: Materials International*, vol. 25, no. 6, pp. 572–582, 2015.

[137] H. Ohta, T. Inoue, Y. Sakamura, and K. Kinoshita, "Pyroprocessing of light water reactor spent fuels based on an electrochemical reduction technology," *Nuclear technology*, vol. 150, no. 2, pp. 153–161, 2005.

[138] K. Goff, J. Wass, K. Marsden, and G. Teske, "Electrochemical processing of used nuclear fuel," *Nuclear engineering and technology*, vol. 43, no. 4, pp. 335–342, 2011.

[139] K. Song, H. Lee, J. Hur, J. Kim, D. Ahn, and Y. Cho, "Status of pyroprocessing technology development in Korea," *Nuclear Engineering and Technology*, vol. 42, no. 2, pp. 131–144, 2010.

[140] H. Lee, J. H. Lee, S. B. Park, Y. S. Lee, E. H. Kim, and S. W. Park, "Advanced electrorefining process in KAERI," in *Proceedings of International Conference ATALANTE*, 2008, pp. 19–23.

[141] J. Ku, S. Moon, I. Cho, W. Choung, G. You, and H. Kim, "Development of pyroprocess integrated inactive demonstration facility," *Procedia Chemistry*, vol. 7, pp. 779–784, 2012.

[142] S. M. Jeong, J. M. Hur, S. B. Park, S. S. Hong, D. S. Kang, M. S. Jung, and C. S. Seo, "Inactive test of the electrolytic reduction system in the ACP hot cell," Korea Atomic Energy Research Institute, Tech. Rep., 2006.

[143] C. L. Pope, C. W. Solbrig, and J. P. Andrus, "Fuel conditioning facility inert gas filled reprocessing hot cell leak rate measurement," *Annals of Nuclear Energy*, vol. 111, pp. 676–682, 2018.

Appendix A: Copyright Letter

Appendix B: User's Manual

1.0 SYSTEM OVERVIEW

The current discrete event simulation (DES) model was developed for implementing strong safeguardability to a commercial-scale fuel fabrication facility. More conceptual details about high reliability safeguards approach are provided in [63], . This user's manual provides precise guidance on how to run the 250-day operation one time or multiple times. In addition, several different sensitivity analyses can be performed by varying facility input parameters such as false alarm threshold, failure rate parameter, false alarm probability, heel amount, etc. This manual also includes paths for execution files, input, output, documentations, etc. It is open source and provided in a github repository below: https://github.com/lee7632/fuel.fabrication.des.model.

2.0 GIT REPOSITORY SET UP

The following tips are useful to set a new git repository, make changes on a local branch, and perform a pull request. On your local machine,

- To initiate git tracking, follow the git command below.

  $ git init

- Fork 'https://github.com/TheDoctorRAB/pyroprocessing_system.model'

- The repository provided on a remote server can be cloned.

  $ git clone https://github.com/[user's name]/pyroprocessing_system.model.git

After logging in to your account, a new repository must be created by clicking '+' button on the top-right location.

- After modifying any files, they can be added to staging.

  $ git add -u

- To commit changes,

  $ git commit -m "message"

- To push the committed changes to a remote,

  $ git remote add origin git@github.com:[user's name]/

  pyroprocessing_system.model.git

  $ git push origin master [or branch]

*A new SSH key may be needed to push changes on a remote.

- To create a pull request, click 'pull request' button in the repo header.
- Next, choose a head branch, and write your pull request title and its description.

See https://github.com/TheDoctorRAB/pyroprocessing_system.model/blob/master/CONTRIBUTING.md for more details on contributing to the model development.

3.0 PREREQUISITE

The current model only supports up to Python2.x. Spyder would be ideal to run the simulation and observe its process. It allows users to edit code and run files using IPython console.

4.0 DOCUMENTATION

The 'documentation' directory contains documents with the general overview of the model, the list of variables used, operation routine, assumptions, etc.

5.0 ROOT DIRECTORY & SIMULATION DIRECTORY

Examples with root directory and simulation directory settings are provided below. 'global_vars.py' contains 'root_dir' and 'simulation_dir' variables.

- root_dir = [where the repository is located]/fuel.fabrication.des.model/model.kmp1.included
- simulation_dir = [where the repository is located]/fuel.fabrication.des.model/model.kmp1.included/simulation/[user's value provided for simulation]

*Windows supports '/' instead of '\' for file paths. For Mac, 'root_dir' does not need to be modified while Windows might require changes.

6.0 EXECUTION

Users need to modify the 'lib' directory first to specify desired inputs. After changes, 'simulation.set.up.py' is run to create a new simulation directory under 'simulation'. It copies input files from the 'lib' directory and pastes them into '[simulaton_dir]/fuel.fabrication/input.' In addition, it helps users to change the root directory and create a readme file for the specific simulation directory created.

- 'main.py' is used to execute the 250-day operation one time.
- 'execution.py' is used to execute the 250-day operation multiple times. Currently, the model runs the simulation 1000 times. To run a different number of simulations, the range specified for the 'for' loop in 'execution.py' must be modified.

The 'output' directory under '[simulaton_dir]/fuel.fabrication' contains the results from executing 'main.py.' The results from executing 'execution.py' are stored in '[root_dir]/simulation/1000.test.runs.'

7.0 BASELINE VS. EQUIPMENT

In '[where the repository is downloaded and placed on your local machine]/ fuel.fabrication.des.model,' two different directories called 'model.kmp1.included' and 'model.kmp1.removed' are included. 'model.kmp1.included' is for the baseline design, and 'model.kmp1.removed' is for the equipment design.
Some source codes under 'oo.fuel.fabrication,' such as 'facility_command_module.py' and 'kmp_measurement_point_module.py' are modified for the equipment design.

8.0 SENSITIVITY ANALYSES

In the 'final.output/[a specific analysis that user chooses]' directory, the subdirectory called 'gold' contains all graphs constructed by performing sensitivity analyses varying false alarm thresholds, failure rate parameter, false alarm probability, heel mean, heel variance, and weight measurement error.

For instance, after running 'execution.py,' output in '[root_dir]/simulation/1000.test.runs' was copied and pasted into the 'final.output/[a specific analysis that user choose]/ [parameter variation]' directory first. Next, by executing 'campaign.py', 'false_alarm.py', 'melter_failure.py', and 'processed_material.py,' the results, such as number of campaigns, false alarm probability, number of melter failure, and amount of processed material, were obtained given a particular facility input parameter variation.

*If another analysis other than the listed ones above is chosen by a user, not only does it have to be updated in execution files, but also a directory may need to be created for containing new output.

9.0 AUXILIARY FILES

- README.md under the root directory explains the general overview of the current version.
- The 'log.txt' file shows the detailed operation routine and output, such as measured weight, expected weight, operation time, etc.
- The 'system.diagram' directory contains the schematic diagrams and graphs related to the safeguards model.
- The concept of random sampling is introduced using 'random.sampling.py' under 'unit.testings.'
- 'unit.testings.py' is for testing gaussian distribution related to weight measurement or inventory difference. It also monitors melter failure by constructing the probability density function and its cumulative distribution function.

10.0 FOR DEVELOPERS

All source files are in the 'src' directory. Developers must test any functionalities or modification made on source code before the pull request.