SAFEGUARDS ENVELOPE METHODOLOGY

A Dissertation

by

RICHARD ROYCE METCALF

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

December 2011

Major Subject: Nuclear Engineering

SAFEGUARDS ENVELOPE METHODOLOGY

A Dissertation

by

RICHARD ROYCE METCALF

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Pavel Tsvetkov
Committee Members,	William Charlton
	Sean McDeavitt
	Justin Yates
Head of Department,	Raymond J. Juzaitis

December 2011

Major Subject: Nuclear Engineering

ABSTRACT

Safeguards Envelope Methodology. (December 2011)

Richard Royce Metcalf, B.S.; M.S., Texas A&M University

Chair of Advisory Committee: Dr. Pavel Tsvetkov

Nuclear safeguards are intrinsic and extrinsic features of a facility which reduce probability of the successful acquisition of special nuclear material (SNM) by hostile actors. Future bulk handling facilities in the United States will include both domestic and international safeguards as part of a voluntary agreement with the International Atomic Energy Agency. A new framework for safeguards, the Safeguards Envelope Methodology, is presented. A safeguards envelope is a set of operational and safeguards parameters that define a range, or “envelope,” of operating conditions that increases confidence as to the location and assay of nuclear material without increasing costs from security or safety. Facilities operating within safeguards envelopes developed by this methodology will operate with a higher confidence, a lower false alarm rate, and reduced safeguards impact on the operator. Creating a safeguards envelope requires bringing together security, safety, and safeguards best practices. This methodology is applied to an example facility, the Idaho Chemical Processing Plant. An example diversion scenario in the front-end of this nuclear reprocessing facility, using actual operating data, shows that the diversion could have been detected more easily by changing operational parameters, and these changed operational parameters would not sacrifice the operational efficiency of the facility, introduce security vulnerabilities, or create a safety hazard.

ACKNOWLEDGEMENTS

I would like to first thank my mentor when I first began this work, Robert Bean. Secondly I thank Pavel Tsvetkov for guiding me through this process. My committee has been fair and tough; thank you William Charlton, Sean McDeavitt, and Justin Yates. Duc Cao was a research assistant for years, as was Aaron Bevill, I wish them luck in their own research. Finally, the amazing staff of the Idaho National Laboratory gave me time during and outside of work, above and beyond the call of duty or even friendship; thank you.

DEDICATION

To those countless unnamed who have given their lives for this great country, this work and all work I shall ever write is in your Honor.

TABLE OF CONTENTS

Page

CHAPTER

CHAPTER Page

LIST OF FIGURES

Page

Page

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION AND PREVIOUS WORK

Introduction

Modern nuclear reprocessing facilities are crucial to the sustainment of nuclear power beyond the existing uranium reserves. The United States' current policy is a once-through fuel cycle, but the U.S. has experimented with large pilot-scale reprocessing facilities and may revisit civilian nuclear fuel reprocessing. Other countries, such as the United Kingdom, France, Japan, India, and South Korea, have pursued reprocessing nuclear fuel for their civilian fuel cycles.

Because these facilities are so crucial to the nuclear fuel cycle, and some of the countries listed above rely very heavily on nuclear power for their base-load needs, it is reasonable to expect that these facilities would be optimized in every way. Unfortunately this is not the case. The Rokkasho Reprocessing Plant (RRP) in Japan, based on the reprocessing technology used at the La Hague Plant in France and adapted by AREVA[1], has not been designed with safeguards[i] or security in mind. These facilities are ultimately chemical facilities, and so they have been designed with the toolbox of the chemical engineer: safety, reliability, and chemical efficiency.

Prior work has explained the idea of "Safeguards by Design," integration of the safeguards and security of a facility into the early design phases, but no facility has used this methodology. Even facilities currently being built in the United States are not designed with

This dissertation follows in the style of *Nuclear Technology*.

[i] The author recognizes the term safeguards to mean, in this case, both domestic (security/materials control) and international (protection from state-based theft). The author refers primarily to domestic safeguards, with an expectation in the United States that domestic safeguards will include international safeguards requirements pursuant with the Additional Protocol to the Treaty on the Nonproliferation of Nuclear Weapons.

safeguards and security in mind, which will force expensive retrofitting. A significant aspect of this cost is the loss of efficiency due to safeguards requirements. Furthermore, these retrofits often relate only to stops in a process for materials control and accountability.

This research offers a different method for the integration of safeguards and security into nuclear reprocessing facilities. Similar to the idea of an operating safety envelope, a safeguards envelope can be created to define the bounds of operating conditions to maximize the ability of a safeguards engineer or safeguards inspector to verify that no material has been removed. This methodology represents a departure from prior safeguards methods, in that operations and safeguards are directly linked and impact each other during production. Nuclear safeguards are intrinsic and extrinsic features of a facility which reduce probability of the successful acquisition of special nuclear material (SNM) by hostile actors. The term ”domestic safeguards” typically refers to an all-threat scenario and includes physical security aspects, while international safeguards are only concerned about the host state as the hostile actor. Future bulk handling facilities in the United States will include both domestic and international safeguards as part of a voluntary agreement with the International Atomic Energy Agency (IAEA). A safeguards envelope is a set of operational and safeguards parameters that define a range, or “envelope,” of operating conditions that increases confidence as to the location and assay of nuclear material. This methodology focuses on the integration of safeguards and security in such a way to make the operation of the facility a "free variable" in optimizing the safeguards while minimizing impact to the facility.

Outline

Chapter I includes the introduction, outline, brief on safeguards applied in nuclear systems (with a focus on reprocessing) and a review of prior work in this area of research. Chapter II describes the safeguards envelope methodology in detail, including the options for optimization depending on the safety and security analysis already performed in the given nuclear facility. Chapter III describes this methodology applied to the front end of a nuclear reprocessing facility in the United States.

Nuclear Safeguards as a Requirement in Nuclear Systems

Nuclear phenomena are irreversibly tied to nuclear weapons. The most significant advances in the creation of early nuclear reactors, the first large-scale fuel reprocessing, and the billions of dollars of research into transuranic chemistry were all related to nuclear weapons. Other industrial facilities such as chemical treatment plants have no such requirements, making safeguards a nuclear-industry specific requirement.

In the first generations of the fuel cycle, it was often believed that the nuclear fuel cycle would be out of reach of all but the most advanced of nations. Effectively, nuclear civilian uses were derived from military applications, and so it was an absurd notion that nuclear material needed to be safeguarded. In the modern era, nuclear power has become a reliable part of the energy security of states which do not have nuclear weapons. South Korea, for example, exports nuclear technology and construction components for the Westinghouse AP1000 design while Japanese Steel Works is one of the few other companies that makes nuclear-grade pressure vessels.

Traditional pressurized-water and boiling-water reactors are not difficult to safeguard. Containment and surveillance (C/S) and tagging are the most common safeguard mechanisms because the large fuel assemblies can be counted. Gross partial defects (removal of a significant portion of the plutonium-bearing pins) can be detected using digital or analogue Cerenkov viewing devices. The technology needed to safeguard these facilities and the impact of safeguards on the operational viability (economic cost) is stabilized and reasonably low, so there is little remaining research in this area, minus a few glaring faults. Actual measurement of plutonium, for detecting partial-defect pin removal, remains a significant challenge, especially at the accuracy and efficiency required under modern safeguards.

Similar to the way nuclear-reactor technology has proliferated through the world, nuclear reprocessing, in the form of both aqueous and pyroprocessing, has undergone a resurgence of research and interest. The prestige of owning and operating a nuclear reactor is not sufficient, and countries are seeking to gain total energy security through building nuclear reprocessing capabilities or facilities. Japan, a country with very limited natural energy resources, constructed such a reprocessing facility, the Rokkasho Reprocessing Plant (RRP). The Rokkasho facility requires disproportionate resources to safeguard compared to the many nuclear reactors around the world, an unfortunate but expected consequence of the difficulty in safeguarding bulk-handling facilities.

Nuclear reprocessing facilities differ significantly from nuclear reactors: the material that is handled is diluted significantly into a bulk form, the most attractive material is separated from fission products, the pathway for material in the facility is not one-way, and material tends to accrete on the pipes (holdup). Bulk facilities are (on average) much more difficult to safeguard compared to item facilities because the amount of material that can be removed is no longer discrete. This variable removal makes detection much more difficult: item accounting facilities can test explicitly to determine the detection probability and failure rates of their detector systems, but the added variable (theft amount) makes this much more difficult in reprocessing facilities. While concrete requirements exist for detection of the amount of material removed in a particular material balance period (MBP), diverting or stealing material over several MBPs is significantly more difficult to detect. Detection is also more challenging because, in some areas of most reprocessing facility designs, the most attractive materials[2] are isolated without fission products, reducing the viability of gross containment/surveillance systems to detect the removal of the material. In other areas of the facility, curium and (□, n) reactions dominate the neutron signature so strongly that plutonium cannot be discriminated. These signatures are also taken under extreme gamma-load: while high energy gamma sources can be easily discriminated, the repair, maintenance, and calibration of these detectors becomes extremely difficult. And all of this occurs using a baseline measurement that occurs at an accountancy tank several steps into the process, after a recycle for the primary solvent of these facilities (nitric acid) has been reintegrated into the system. The flow of materials is not one-way: solvents are reused to minimize waste, but this provides an opportunity for removal of poorly scrubbed solvent that bears plutonium. This multi-solvent recycle also adds miles of piping, valves, and other potential extraction points from which to siphon off valuable material. Finally, bulk materials tend to get "held-up" inside of the facility. Though constituent materials from which reprocessing facilities are built are designed to resist the accretion of of material on their walls, the entire periodic table exists in the dissolutions, and partially dissolved solids mixed with saturated nitric acid naturally will plate out in the facility. This unavoidable holdup presents as material that simply disappears. Measurement of this holdup, inside one of the most radioactive environments on the planet, provides a significant challenge.

Early reprocessing facilities, from which almost all others have been copied, were designed and maintained by chemical and industrial engineers. The emphasis was on the final product and generating as much of it as possible, rather than on concern for any product that had gone missing. Why would there be concern for an extra recycle to ensure the last 1% of product is removed from the bottom of the tank if a 15% efficiency gain can be found by simply moving more material through the process at a faster rate?

However, it soon became clear that this material must be protected and safeguarded. To address these challenges, nuclear reprocessing facilities have followed one of two potential paths: weapon-state nuclear reprocessing facilities have mitigated losses as well as reasonably possible, but focused on physical security to prevent theft (there is little imperative for a weapons-state to steal its own plutonium), while the only non-weapons-state reprocessing facility, RRP, has been highly instrumented to take thousands of very expensive and time-consuming destructive analysis samples. One of the methods suggested to solve the problem of safeguarding material during reprocessing is to use the solution-monitoring system of the facility to provide not merely additional qualitative confidence but additional quantitative confidence to ensure that the materials have not been misplaced.

This approach is designed to be prescriptive, for both domestic and international safeguards. Both types of safeguards have specific requirements that must be fulfilled; and the workhorse of this technique, accountancy, is the basis for all applied safeguards. The layering of process monitoring as a transparency or confidence-building mechanism does not provide any quantitative benefit, discouraging its use as a safeguards tool. Other developmental technologies are similarly not able to contribute meaningfully to safeguards in a quantitative fashion.

Furthermore, these prescriptive methods are seen as a layer of defense applied over an operating facility. Using an approach of defense in depth, multiple measurements are taken in tanks specially homogenized to provide good measurements. Additionally, this defense in depth in modern U.S. facilities will likely include international safeguards requirements as well as domestic safeguards requirements, significantly increasing safeguards burden through efficiency degredation. This paradigm works very well for small to medium sized facilities, but the efficiency degredation in large facilities creates an adversarial relationship between operator and safeguarding personnel.

United States domestic safeguards are a combination of security and accountancy measurements. Accountancy, as a technical term, means the assay (isotopics and amount) of material to ensure that no material has gone missing. Domestic safeguards in the United States have undergone significant changes, often with exceptions for individual facilities. However, material is commonly graded into class based on its attractiveness. Attractiveness is determined by the quantity and quality of material in an individual facility. The requirements are rather arcane, representing multiple forms of material (e.g. uranium concentrations of 100g/kg representing class B materials, provided that uranium metal concentration is U-235) that are combined with quantity to provide a Category.[3] [ii] In general, the requirements are as follows:

1) Probability of Nondetection < 3% at $p<0.05$ (95% confidence).

[ii] To further complicate matters, the protection requirements for reprocessing facilities (Category 1) are classified..

2) Material Unaccounted For < 2% of active material or a Category II material; in nitric acid or solution (such as in a reprocessing plant) this represent 2 kg Pu/U-233 or 6 kg U-235.

3) Materials are accounted for at least bi-monthly.

These requirements are much more stringent than international safeguards. Consider an assumptive pilot-scale reprocessing facility that reprocesses 100 tons of heavy metal per year of irradiated nuclear fuel at discharge burnup. Under the assumption of 1% plutonium and no prior or expected holdup (generous), measurement error cannot exceed 1.2% of the plutonium at 95% confidence, driving the actual mean estimation to ~ 0.5% of the throughput of any solution bearing plutonium. This level of confidence is difficult to achieve in practice and is greatly complicated with materials stuck inside of the facility; holdup between book-closures can be the primary driver of uncertainty.

It is clear that U.S. reprocessing facilities will be safeguarded, but a campaign method relying exclusively on destructive analysis samples is not acceptable in a modern facility. This echoes the drastic over-design of first-generation nuclear reactors for safety. A clear parallel exists between the lack of neutronic-thermohydraulic coupling and overdesign in safety analysis to the lack of process-safeguards coupling and overdesign in reprocessing safeguards. The requirement to secure the materials is not in its infancy, but the drastic differential budget between a nuclear security programs and civilian nuclear reprocessing changes the requirements from an effectively infinite budget to one much more limited and requiring much greater efficiency from the safeguards system to make the closed nuclear fuel cycle more economically viable.

Historical Background

While the idea of a safeguards envelope using the operational characteristics as a free variable appears to be novel, the topics of nuclear safeguards, safeguards by design, nuclear-fuel-cycle optimization, process-monitoring methods, and reprocessing safety have extensive literature. For brevity, a limited selection of prior work in safety envelopes and solution monitoring analysis are presented.

Prior Work in Safety Envelopes

Operating facilities make use of safety envelopes, also commonly called operating envelopes. Safety envelopes are normally the boundaries around which normal operation can occur. Exceeding these boundaries leads to non-normal response: rapid temperature increase in a chemical reactor may lead to heat-steam rerouting to reduce reaction rates to prevent a Boiling Liquid Expanding Vapor Explosion (BLEVE) or a power reduction in a nuclear power plant with a radiation area monitor alarm. These operating envelopes are a standard part of the operating environment for most facilities as simply a state of practice.

Prior Work in Solution Monitoring / Process Monitoring Methods

Research by Ehinger at Oak Ridge National Laboratory is the earliest known non-simulated data published and analyzed. An Integrated Equipment Test (IET) facility was constructed as an example pilot-scale facility, running synthetic plutonium in depleted uranium.[4] A mass-tracking system, integrating a pair of dip-tube measurements (providing level and density), was developed at this facility, to resolve events. Because of the (relative) simplicity of the facility, the research was able to design modules to handle each aspect of the facility, but designed in an integrated manner. Most importantly, this facility was actually tested against diversion: at one point, guest researchers were provided the opportunity with a team of welders to alter the facility and remove material. The code developed by Ehinger was able to detect the removal of the material (though the false alarm rate was significant, often one or two false alarms per day).[5] This rather severe false alarm rate and the requirement for a custom system for each small plant limits the application, but this early research was the foundation for the process monitoring systems at the Idaho Chemical Processing Plant, the prime example of this Dissertation (See Appendix 1).

Early approaches at Argonne National Laboratory in integrated system tracking (focused on nuclear power plants) were based on a code named PRODIAG. This technique used neural networks to train expert systems to identify off-normal conditions. [6] Unfortunately, due to overtraining of the neural network systems, this technique was dropped in favor or IGENPRO. IGENPRO, developed at Argonne National Laboratory, is a technique and code used in order to resolve events using first principles thermohydraulic codes instead of event-based structure. This methodology is especially relevant because it is one of the first cases in which the abstracted event structures (prescripted) are replaced with higher fidelity of for online assessment. [7] As the methodology progressed, fuzzy logic was used to eliminate noise in the incoming signals, through their more advanced code, PROTREN. [8]

Tom Burr of Los Alamos National Laboratory (LANL) and John Howell of Glasgow University of the UK have an extensive library of research on process monitoring methodologies.[9] [10] [11] [12] [13] [14] [15] [16] It is their intention to remove process monitoring methods from a qualitative "additional measure" or containment/surveillance (C/S) system to a quantitative-safeguards-relevant system. Burr and Howell primarily have focused on static plutonium tank-to-tank transfers (solution monitoring), generalized to any tank-to-tank transfer. Their models take into account multiple uncertainty types, including data amalgamation errors. In brief, the Burr and Howell methodologies revolve around:

1) Marking an event for start and stops, during or immediately after an event, from measurements of level, temperature, and density.

2) Analyzing the cumulative residuals from the measured datapoints

   a) This may take the form of linear tests or nonlinear regression tests.[17]

   b) This may take the form of multivariate analysis, combining independent measurements to figures of merit (e.g. mass from density and volume.). Literature in Burr has considered fractal analysis, fuzzy logic, linear process fault detection and diagnosis, and nonlinear time series analysis.

3) Classifying the event (e.g. transfer, boiling, evaporation, etc), to assist in resolving errors for less statistically focused inspectors.

Burr has continued his research in testing multiple statistical tests against expected diversion sets. In this case, Burr and Howell tested for the lowest probability of nondetection (PND) under the conditions of a static false alarm rate (FAR), using the same developed tank-to-tank transfer simulator described previously. Croiser's cumulative sum residual method was established to be the superior test under his conditions.

Finally, methodologies based on event marking and using time between events as the discriminator have been developed by Garcia. This method relies on sequential probability ratio tests (SPRTS) in which the time vector is one of the primary tested in a multivariate analysis of change from nominal conditions. The reason for this change is that the physical models of process characteristics often lack the fidelity (especially real-time) to estimate the correct values.

It is clear that in the current trend of research for solution monitoring, the physical models are not explicitly used, but serve only as a guide to support the data-driven analysis. While differing levels of fidelity exist (Burr and Howell's focus on the actual measurements, Garcia's time-series event marking), the actual process is ignored in favor of abstraction for safeguards.

Broad scale analyses of the uncertainties in the measurements of safeguards as the material moves through a facility are rare. Work by Cipiti and Duran has generated a lab-view model of a nuclear reprocessing facility (PUREX) with synthetic measurements interspersed in the facility. This research takes into account systematic and random error and includes a start-up and shut-down cycles, in order to accurately simulate actual uncertainties. This model is intended to be used as the framework for analyzing the impact of new technologies in reprocessing facilities: a factor of 100 in measurement certainty may not be actually valuable if that measurement certainty is only applicable on a stream with low SNM. A rudimentary security model, using different probabilities of detection based on the current perceived threat level by the facility (base level and alerted) shows that rapid detection of material removal by process monitoring safeguards equipment can actively benefit the detection and neutralization of security threats.

Objectives

The primary objective of this research is to develop an alternative, more operations-friendly methodology of applying safeguards—one that will have higher confidence, lower false alarms, and reduced safeguards burden—by changing operational parameters of the facility and including transparency measures as quantifiable data. This methodology is unique in operational integration and treating safeguards as a fundamental aspect of operating a facility, instead of a layered defense over an operating facility. Higher confidence will be established through leveraging more data in making decisions regarding the location of nuclear material, rather than treating these data as noise. Lower false alarm rates can be achieved by integrating these data as a second-check before an alarm is triggered. With lower alarm rates and higher confidence, facilities operating under safeguards envelopes will not require as many shutdown/flushes that decrease throughput, reducing the negative impact to operational efficiency from safeguards.

The tasks that support this are 1) defining a common quantifiable metric between solution monitoring and material accountancy, 2) implementing a form of solution monitoring on an area of a facility, 3) changing operation to increase efficiency of the solution monitoring, and 4) demonstrating this change did not reduce efficiency of the plant as a whole.

CHAPTER II

THE SAFEGUARDS ENVELOPE

Introduction

Rather than an independent analysis of solution monitoring and accountancy without considering alterations in the process, this Dissertation proposes the direct integration of the operation of the facility as a free variable to create an operating space known as the safeguards envelope. A safeguards envelope must explicitly address the safety, security (domestic safeguards), and international safeguards requirements, with the intention of optimizing the cost efficiency of the facility. This is shown as Figure 1. The region of viability is the area in which a facility can operate because operation outside of this envelope would be illegal from one or more regulatory standpoints. The efficiency distribution within the region of viability is never determined explicitly. Typically, the operations of the facility are fixed, limited by the boundaries of safety, safeguards, and security. In some advanced facilities, safety is directly integrated and operations can be changed or designed to be operated in such a way to increase safety, but operational changes intending to adjust for all three systems have not yet been proposed and demonstrated.

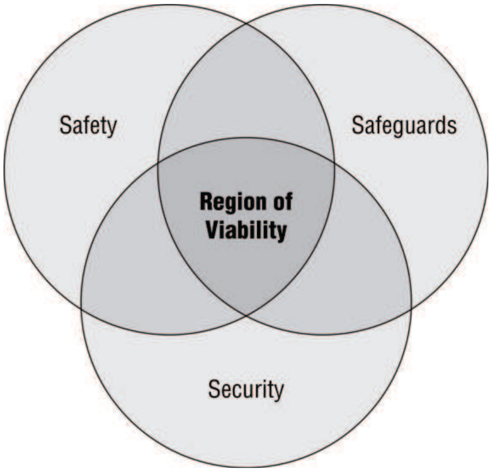


Figure 1. Region of viability for operations in a nuclear facility.

An increase in efficiency of reprocessing in the nuclear fuel cycle could bring reprocessing below the threshold needed to make this technology viable economically. It is unlikely that the safeguards burden alone increases the cost beyond the more economical once-through cycle.[18] With a significant increase in the cost of uranium world-wide or a choice to pursue reprocessing as an energy-security (strategic) choice, reprocessing may be pursued. This work suggests a safeguards envelope operation to reduce the cost per kilogram in an example reprocessing facility and assumes that this reprocessing facility has already been constructed. The safeguards envelope method is intended to address the safeguards effects that are only found in nuclear facilities. Thus, generating a safeguards envelope is a nuclear fuel cycle specific problem.

Any safeguards envelope is subject to several constraints:

1) Operating facilities are prone to local changes and perturbations on a daily basis, so a safeguards envelope must cope with expected slight operational changes.

2) Operating facilities are prone to equipment failure, which should be explicitly addressed.

3) Operating facilities are ultimately controlled by human beings, requiring human-factors integration. Rather than treat this explicitly, the envelope methodology suggested must be clearly definable in a few variables, such as operating speed, valve conditions, or detection limits.

4) The envelope must represent not only the ideal operating conditions, but conditions of the facility that the operator can move to for maintenance, changes, or special packages with clear requirements at these stages.

5) The envelope must provide for an overarching uncertainty related to safeguards while addressing the more explicit requirements of safety and security, as well as a local requirement for the same. Specifically, a local material balance area may be out of a solution-monitoring-only envelope due to equipment failure, requiring expensive accountancy measurements, but this increase in uncertainty should be mitigated and integrated into the rest of the envelope.

6) The envelope must be based on the common metric of probability of success at a certainty level for safety, security, and safeguards.

Under these requirements, this work cannot provide the recommended changes to a given facility; each facility will be sufficiently unique that a common analysis is impossible. However, this methodology explains **how** to evaluate potential changes into a facility, and when such computational power is available, to establish the **ideal** operating conditions. The severe computational requirements required to establish the true ideal are outlined in the final chapter of this Dissertation.

Security in the Safeguards Envelope

The requirements described above, especially for a common metric, work well with the frontrunner in security evaluation methods. There are multiple ways of evaluating security at nuclear facilities, but the forerunning methodology has been developed by M. L. Garcia, and the author directs readers to her publications for details.[19] [20] This methodology is quantitative, rather than qualitative, although there remains some additional uncertainty above what would be expected because the method cannot predict human behavior. Instead, it attempts to capture these elements into probabilities derived from historical simulation data of attacks against facilities. This method has been adopted and evolved by the DOE to form part of their standard assessment of nuclear facilities. This evaluation is semi-quantitative. Through the steps outlined below, a probability of detection, interception, and neutralization (made of several conditional probabilities) is generated from an average of these probabilities for a set of scenarios. The combined probability must meet a threshold determined by DOE.

To make an evaluation of the physical security of a high value nuclear target (Category IV facilities, as expected for nuclear reprocessing facilities), several steps are taken:

1) A model of barriers is developed between the a stationary target and a potential adversary at the fenceline or inside of the facility in the case of theft.

    a) Each barrier has an associated delay time and an associated detection probability.

2) A simulation is run, effectively tallying each pathway through each set of barriers . Figure 2 shows this visually: the red pathway is an optimal pathway through a set of

concentric barriers, where thickness of the barrier represents time or difficulty associated with crossing the barrier.

a) The associated delay for each of these barriers is tabulated, as well as at what point the adversary was detected. In this analysis, the detection probability is the only nondeterministic number.

b) The probability of intercepting and neutralizing the threat must exceed a certain value. As in the example Figure 2, the most efficient (lowest barriers) path is the limiting case.

3) A force on force exercise through computer using humans controlling avatars is used to establish the realism of these parameters for nontheft scenarios.

4) Very limited live-action force on force exercises are performed at the site for nontheft scenarios.

There are several implicit assumptions in this model, but two are most important in terms of application of the safeguards envelope:

1) The target is stationary and the adversary knows exactly where the target is.

2) The security system works independently of all other systems.

The first assumption is highly conservative, and almost all changes to the system within the safeguards envelope should invalidate this assumption and add security resistance. Unfortunately, this will not be reflected in this methodology, and the author is not aware of widely accepted methodologies in which this is taken into consideration. If the second assumption is removed and the safeguards and security systems are integrated, the probability of detection for theft is expected to rise significantly.[21]

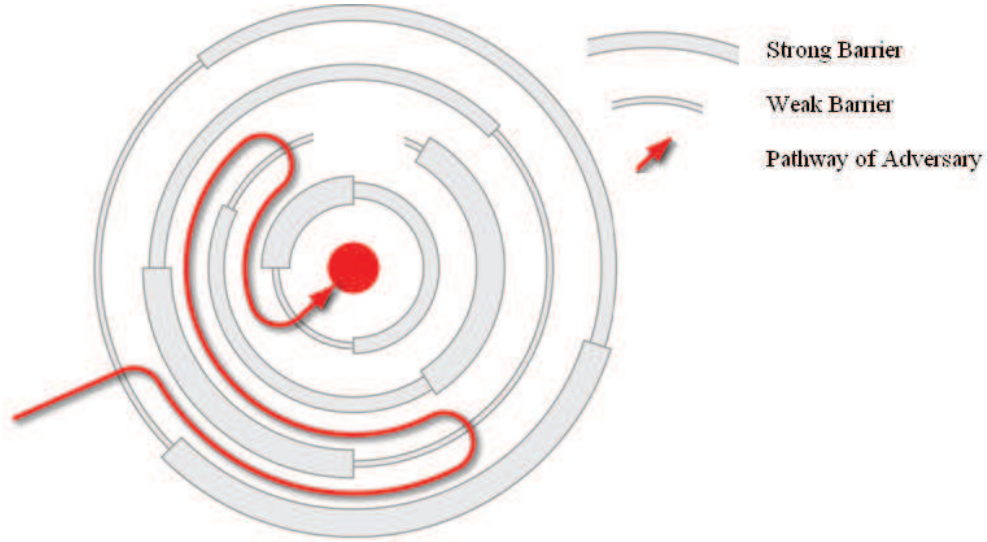


Figure 2. DOE-vulnerability analysis.

This methodology does provide the limiting constraints on adjustments to the system and allows for the security bounding on the safeguards envelopes developed. Presuming that the security system is already at the threshold for unacceptable detection probabilities, the conditions of the safeguards envelope are as follows:

1) Material movement is acceptable or even preferred, even though no credit can be taken for the movement.
2) Material cannot remove security barriers or be moved through a layer of defense without additional security measures being moved into place.
3) New operating parameters can only increase the probability of detection for theft (i.e. operating parameters that obscure C/S sensors are unacceptable or require additional security measures to be moved into place).

Safety in the Safeguards Envelope

The technique used for evaluating safety probabilities in Safeguards Envelope Method is probabilistic risk assessment (PRA). Though other methods have been used in safety analysis, the quantitative nature of PRA and ease of including changes makes it the preferred method. Developed partially in response to the Three Mile Island and high-profile NASA incidents, PRA uses failure-tree analysis to estimate the final probabilities of major target incidents. The most serious of these incidents is major release of nuclear material to the public. While PRA has seen significant use in the nuclear reactor industry, the introduction into reprocessing facilities is more likely to have come from the adoption of PRA by high-risk chemical industrials following the gas release at Bhopal, India.

PRA analysis uses an adapted fault-tree analysis.[22] It is adapted, rather than a pure fault-tree analysis because it allows for contingent-event requirements: multiple subsystems must fail, but not in order. This cross-linking of the multiple subsystems makes this a superior safety analysis tool compared to the design basis accident (DBA), which assumes a set of fault-tree pathways to major accidents (this updated methodology makes sense in light of the relatively minor cascading failures that led to Three Mile Island). An example PRA tree is shown in Figure 3, in which events (yellow) are binary statements that can be either true or false, and conclusions are listed on the right side with green representing acceptable operation and grey representing levels of damage to the facility.

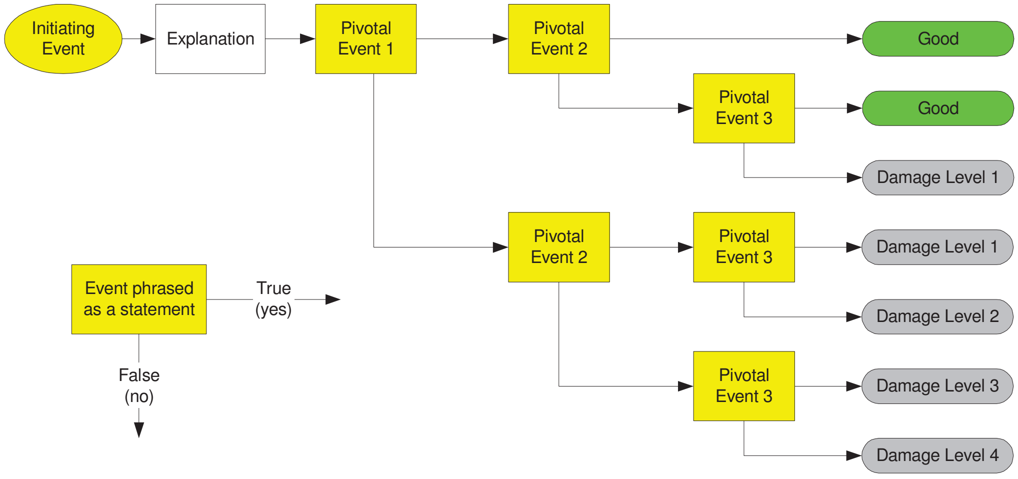


Figure 3. Basic PRA methodology.

The use of PRA in a nuclear reprocessing facility will revolve around a few major incidents:

1) Major disruption to operations that is recoverable within a timeframe that is determined by risk tolerance at the facility.

2) Major disruption to operations that is not recoverable within the above timeframe.

3) Significant release of radiological material to the public (or chemical release inducing a health hazard).

Unfortunately, without a complete, customized PRA for a nuclear reprocessing facility, estimating this probability is difficult at best. However, a replacement for PRA in the chemical industry exists when a full PRA is not available: expert elicitation. Expert elicitation was used as a substitution in this Dissertation. Presuming, as in the security case, that the safety system is already at the threshold for unacceptable detection probabilities, changes which affect the safety system will require additional safety measures. Examples of these changes are listed below:

1) Material which is caustic should not remain in a vessel any longer than required.

2) Pressures and temperatures should not be increased, as both of these lead to more failures of valves and tanks.

3) Changes to the system should not increase residence time of radiological personnel for measurements inside of the hot cells.

4) Maintenance, the primary cause of failures in chemical facilities, should not be affected. Note that some maintenance must be performed in radiological areas, compounding the issue with (3) above.

International Safeguards in the Safeguards Envelope

International safeguards in reprocessing facilities are discussed in the preceding chapter. The use of the probability metric is more difficult for combining subsystems together as the systems-analysis perspective on nuclear reprocessing facilities is limited. Historical reprocessing facilities have been optimized for throughput, without consideration of safeguards; in the case of Rokkasho, the process monitoring subsystem is regarded as a confidence-building measure and not part of a formal safeguards optimization. However, modern safeguards research has called for multiple subsystems to be combined to generate confidence. The following is an example of how to integrate two subsystems in safeguards system, process monitoring (PM) and accountancy.

When supplementing accounting methods with PM measures, either of two systems may be applied. In the first model (union model), either alarm may warrant an investigation. Alternatively, monitors may choose to only investigate cases in which both alarms sound (intersection model). Since both alarms must sound to warrant investigation under the intersection model, a very sensitive PM system is needed.

Sensitivity and specificity are not intrinsic properties of a monitoring system; rather, the monitoring system only relates the two. For example, both α_A, the PND of accountancy and β_A, the FAR of accountancy depend on the material unaccounted for (MUF) alarm threshold. Thus for a given α_{PM}, it is possible to compute β_{PM} such that the overall system sensitivity and specificity remain the same. This represents a threshold for usefulness of a PM detection system: any system producing a higher FAR than the threshold will only interfere with plant operation, and any system with a higher PND poses an unacceptable risk. Using the requirements for international safeguards outlined below, the explicit curves for the probability requirements of the process monitoring system can be calculated to be useful.

Single Sensor Case

Assume the case of a single sensor, from which a set of readings can be taken. These readings may be either a composite of time-delayed readings or a single reading with a known uncertainty. The readings are expected to be along a Gaussian distribution. If there is a diversion of material (i.e., the true mean is moved), the shape of the curve should not change, but the mean will move. This is outlined below in Figure 4, where material unaccounted for (MUF) represents the diversion.

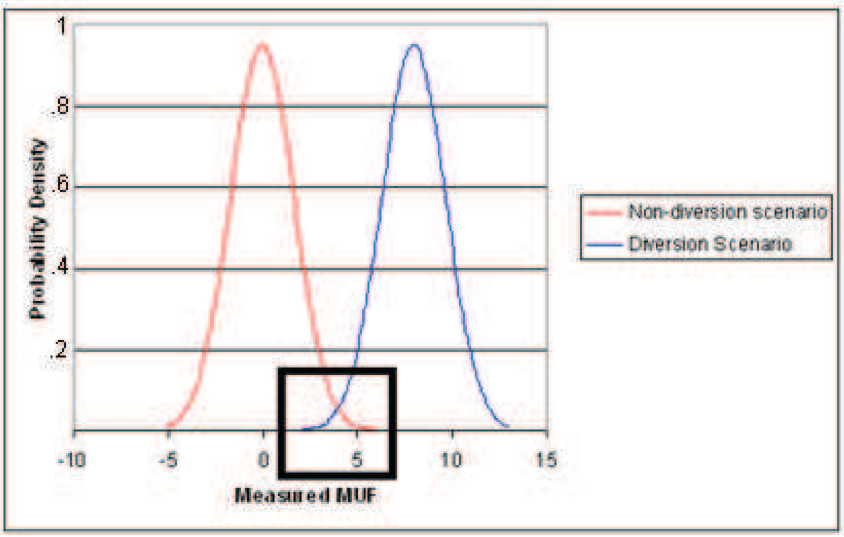


Figure 4. Comparison of the diversion and nondiversion scenarios.

As can be seen, there is overlap between the distributions. In fact, no matter the distance in mean between the two distributions, there will always be more overlap. As the two means become closer (indicating protracted diversion, in our case), discrimination is more difficult. As they move farther apart, discrimination is less difficult. The zoomed in area from Figure 4 is the overlap, displayed in larger form in Figure 5. Consider two thresholds of detection, shown as the green line in panels a and b. The overall error is the integral of the blue and red areas, with the threshold affecting this total amount of error and the amount of each type of error.

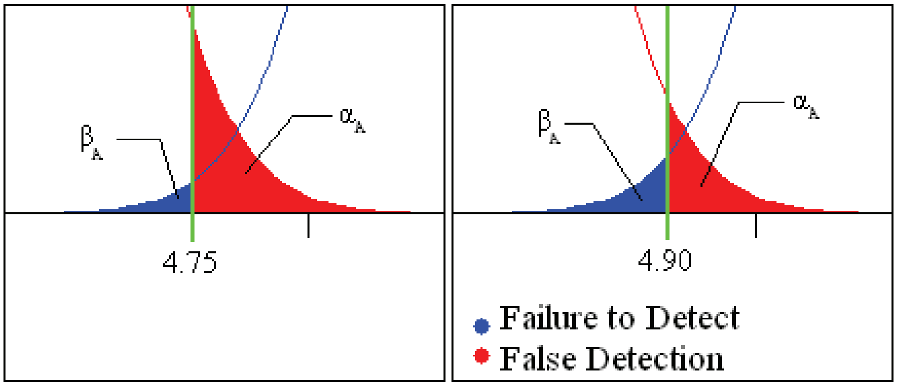


Figure 5, a and b. Threshold impact on error.

Assuming that false alarms and failure to detect are equally damaging, the optimal threshold is precisely at the intersection of the two distributions. This is clearly not the case in nuclear nonproliferation, in which mistakenly believing material has been removed is significantly less relevant than material's being removed with the regulator unaware of the diversion. Regulatory limits set by the IAEA or DOE normally provide a minimum confidence in successful detection. For a single-sensor case with a single measurement set (i.e. strictly accountancy), this threshold is set.

Two Sensor Case

Multiple sensors, and their integration, make up an entire field of research. Methods such as Dempster-Shafer, fuzzy logic, "lean manufacturing," and others seek to make distinctions between normal or off-normal operations. In this section, a multi-sensor approach that is significantly constrained is presented.

Consider the case of two sensors under the following constraints:

1) Sensors may only be combined in unions or intersections. This is to say that Sensor A OR Sensor B may trigger an alarm, or Sensor A AND Sensor B must both trigger to induce an alarm.

2) Optimal thresholds can be determined independently for Sensor A and Sensor B for any configuration. This can be accomplished by Monte Carlo analysis.

3) Sensors are strictly independent.

Because the thresholds of Sensor A and Sensor B are known, the FAR (Type I error, denoted as α) and PND (Type II error, denoted as β) can be calculated for each sensor. This can be seen graphically above in Figure 5, a and b.

The union of Sensor A and Sensor B allows for the calcuation of the overall α and β. Graphically, this is represented by Figure 6. In Figure 6, two sensor detection spaces are overlaid, with the integral of all filled in area the total detection probability, and white space in the domain is area of nondetection.

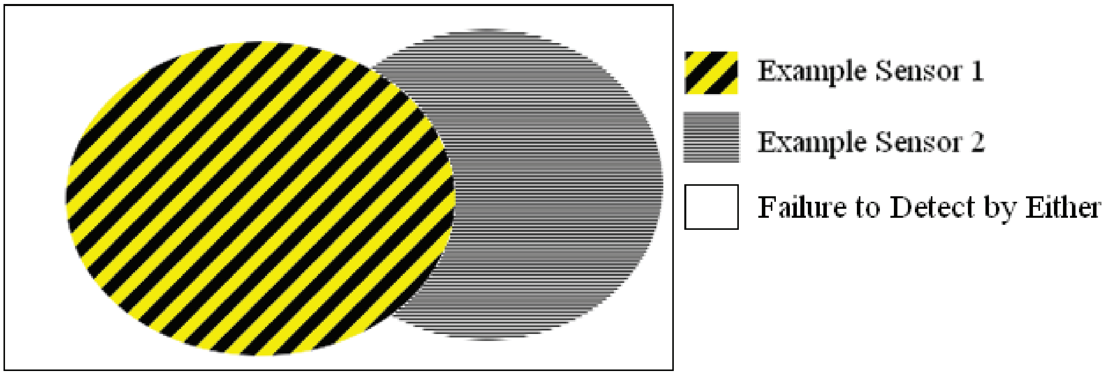


Figure 6. Union of two sensor probabilities.

Equation 1 shows the false alarm rate of the overall system. The area that would appear to overlap between the two probability densities (the area that Sensor 1 cuts into Sensor 2) is subtracted because it would be counted twice (i.e. $\alpha_A\alpha_B$ is counted in both α_A and α_B)

$$\alpha = \alpha_A + \alpha_B - \alpha_A\alpha_B \tag{1}$$

The union of the sensors, both sensors must fail to register a change when there was a change for there to be a failure of detection. Thus, the sensors are effectively serial (intersection) for the probability of nondetection, as shown in Equation 2, below.

$$\beta = \beta_A\beta_B \tag{2}$$

As expected, in the case where Sensor B is nonexistent, the system is $\alpha_B = 0$ and $\beta_B = 1$ implying $\alpha_0 = \alpha_A$ and $\beta_0 = \beta_A$.

If, instead, both Sensor A and Sensor B must alarm in order to detect, the figures are reversed, in that both sensors must fail when there is no diversion to cause a false alarm, but either sensor can fail to detect when there is a diversion for the system to fail to detect. These are shown in equations 3 and 4.

$$\alpha = \alpha_A\alpha_B \tag{3}$$

$$\beta = \beta_A + \beta_B - \beta_A\beta_B \tag{4}$$

Multi-Sensor Case

Multiple sensors can be combined in sets of unions or intersections. Three cases will be presented and then the method will be generalized.

Consider the case that Sensor A AND Sensor B alarming will induce an alarm, but Sensor C alone can also induce a full system alarm. This is an Intersection-Union. A false alarm can be induced by either a failure in Sensor A and Sensor B, or a single point failure in Sensor C, shown in Equation 5. A failure to detect a change requires either Sensor A or Sensor B to fail and Sensor C to fail, shown in Equation 6.

$$\alpha = \alpha_A \alpha_B + \alpha_C - \alpha_A \alpha_B \alpha_C \tag{5}$$

$$\beta = (\beta_A + \beta_B - \beta_A \beta_B)\beta_C \tag{6}$$

This case may be representative of a real life case in which both the gross-neutron and gamma sensors must both alarm to induce a system-wide alarm or a neutron-spectroscropy technique focused on plutonium-specific spectra can trigger an alarm.

Consider the case that Sensor A or Sensor B or Sensor C can trigger a system-wide alarm. This is a Union-Union. A false alarm can be triggered by failure in any given sensor. However, a failure to detect a change requires all three sensors to fail. These conditions are represented below as equations 7 and 8.

$$\alpha = \alpha_A + \alpha_B + \alpha_C - \alpha_A \alpha_B - \alpha_A \alpha_C - \alpha_B \alpha_C + \alpha_A \alpha_B \alpha_C \tag{7}$$

$$\beta = \beta_A \beta_B \beta_C \tag{8}$$

This case may be represented of a real life case of highly enriched uranium, where reliable passive detection techniques are difficult, and as a result multiple layers of defense are required to secure the material.

Finally, consider the case that Sensor A, Sensor B, and Sensor C must each trigger a local alarm to induce a system alarm. This is an Intersection-Intersection. A false alarm is rare, requiring each sensor to independently fail. However, any sensor can fail to alarm locally for the system to fail to detect a change. These conditions are represented below as equations 9 and 10.

$$\alpha = \alpha_A \alpha_B \alpha_C \tag{9}$$

$$\beta = \beta_A + \beta_B + \beta_C - \beta_A\beta_B - \beta_A\beta_C - \beta_B\beta_C + \beta_A\beta_B\beta_C \tag{10}$$

It becomes evident that each addition of a sensor increases the complexity of the analysis significantly. Furthermore, the third constraint, requiring strict independence of measurements, becomes increasingly difficult to verify. In the Intersection-Union example above, the covariance between the gross-neutron sensor and the neutron-spectroscopy method is clearly not zero. A neutron-spectroscopy method will clearly not alarm if there are no neutrons that are detectable by a gross-neutron sensor.

The systems above can be generalized, however, relieving the pressure of the third constraint and also reducing the complexity of the equations. In the two sensor case, Sensor A and Sensor B were reduced to the overall system. If the combination of these two sensors is simply regarded as yet another subsystem (e.g. Sensor AB), the Union-Intersection, Union-Union, and Intersection-Intersection models of Sensors A, B, and C become Union and Intersection of Sensors AB and C. In this framework, the explicit requirements for independence (constraint #3) is only required between Sensor AB and Sensor C. The terms $\alpha_A\alpha_B$ and $\beta_A\beta_B$ are implicitly defined by the reliability of Sensor AB.iii

The Intersection-Union model presented above is demonstrated in terms a Union of Sensors A∩B and Sensor C. In the example below, constraint #3 is still assumed.

$$\alpha = \alpha_{AB} + \alpha_C - \alpha_{AB}\alpha_C \quad = \alpha_A\alpha_B + \alpha_C - \alpha_A\alpha_B\alpha_C \tag{11}$$

[iii] Reminder: $\alpha_{A\mathrm{I}\cap B}$ only equals $\alpha_A\alpha_B$ if A and B are independent. Similarly for $\beta_A\beta_B$.

$$\beta = \beta_{AB}\beta_C \qquad = (\beta_A + \beta_B - \beta_A\beta_B)\beta_C \tag{12}$$

These are the same results as above. Union-Union and Intersection-Intersection are similar. In this way, any set of N sensors that are to be combined, subject to the constraints described above, can be combined into a single sensor.

Effective Uncertainty as a Figure of Merit

Understanding the false alarm rates and failures to detect are less valuable than understanding the effective uncertainty. The requirements for a shorter material balance period are based on the fact that at a certain level of uncertainty, there is no longer sufficient confidence that material has not been removed. σ_{A0} is the current effective measurement uncertainty of the system. In this framework, it is much preferred to provide the new effective measurement uncertainty of the system as a metric for a new material balance period.

Returning to the prior Figure 1 in this section, the α and β could be calculated if the optimal threshold was known, the diversion was known, and the curves were known. If instead of a threshold, a set of measurements were known then the α and β could be calculated using a standard Z-test, using the threshold as the power of the test. This is shown in equation 13, where the power P, is the α of this particular set.

$$P = \Phi\frac{(\bar{x} - 0)}{\sigma} \tag{13}$$

Assuming a minumum detection threshold at 1- α (i.e. able to draw a conclusion in classical statistics), the inverse normal function (quantile) can be applied, resulting in equation 14.

$$\Phi^{-1}(1-\alpha)=\frac{\bar{x}}{\sigma} \tag{14}$$

Similarly, we may invert β, which is originally calculated at power P as equation 15 and then inverted in equation 16

$$P=\Phi\left(\frac{\bar{x}-1}{\sigma}\right) \tag{15}$$

$$\Phi^{-1}\beta=\frac{\bar{x}-1}{\sigma} \tag{16}$$

The subtraction in the standard Z test is normalized over significant quantities in this case. The precision of the diversion against which we are testing allows for this inversion. Note that in all cases as can be seen in Figure 5, a and b; the only change between α and β is the reality of removal of material.

By subtracting these two equations, the random sampling can be removed, as shown in equation 17.

$$\Phi^{-1}(1-\alpha)-\Phi^{-1}\beta=\frac{\bar{x}-\bar{x}+1}{\sigma}=\frac{1}{\sigma} \tag{17}$$

Thus, an effective measurement uncertainty can be described. This result is valid under all conditions except for the constraints above as a figure of merit, but only accurately models reality under the conditions that measurements are Gaussian or where the number of sensors is very large (i.e., the collective uncertainty will approach Gaussian by the central limit theorem).

The analysis of this Dissertation has used accountancy as the base sigma. In this case, σ_{A0} is estimated as or .21125 of an SQ (1.69 kilograms), assuming exactly 5% β_A and 0.1% α_A (single-sided test).

The final equation for the probability requirements is given as equation 18, below:

$$\mathit{\Phi}^{-1}(1-\alpha_{PM+A})-\Phi^{-1}(\beta_{PM+A})=\Phi^{-1}(1-\alpha_A)-\Phi^{-1}(1-\beta_A) \tag{18}$$

where

$$a_{PM+A}=\alpha_{PM}+\alpha_A-\alpha_{PM}\alpha_B$$

$$\beta_{PM+A}=\beta_A\beta_{PM}$$

Φ^{-1} is the inversion of the Normal Gaussian distribution, given below as equation 19.

$$\Phi^{-1}(p)=\sqrt{2}\mathrm{erf}^{-1}(2p-1) \tag{19}$$

$$p\in(0,1) \tag{20}$$

$$\mathrm{erf}^{-1}=\sum_{k=0}^{\infty}\frac{c_k}{2k+1}\left(\frac{\sqrt{\pi}}{2}p\right)^{2k+1} \tag{21}$$

$$c_k=\sum_{m=0}^{k-1}\frac{c_m c_{k-1-m}}{(m+1)(2m+1)}=\left\{1,1,\frac{7}{6},\frac{127}{90},\cdots\right\} \tag{22}$$

$$c_0=1 \tag{23}$$

In the above equations, α is the probability of a false alarm (Type I error), β is the probability of a failure to detect (Type II error), and the subscripts refer to the systems. The PM subscript denotes the process monitoring system, the A subscript designates the accountancy system, and the *PM+A* subscript designates the combined system (note that these do not combine linearly). The C_k are simply analytic constants in the erf function, which is strictly a mathematical construct to invert the normal Gaussian distribution. These curves are shown as Figure 7, where the blue line is the threshold at which the process monitoring system reduces the effective uncertainty in the measurement (and is therefore useful as a safeguards technique).

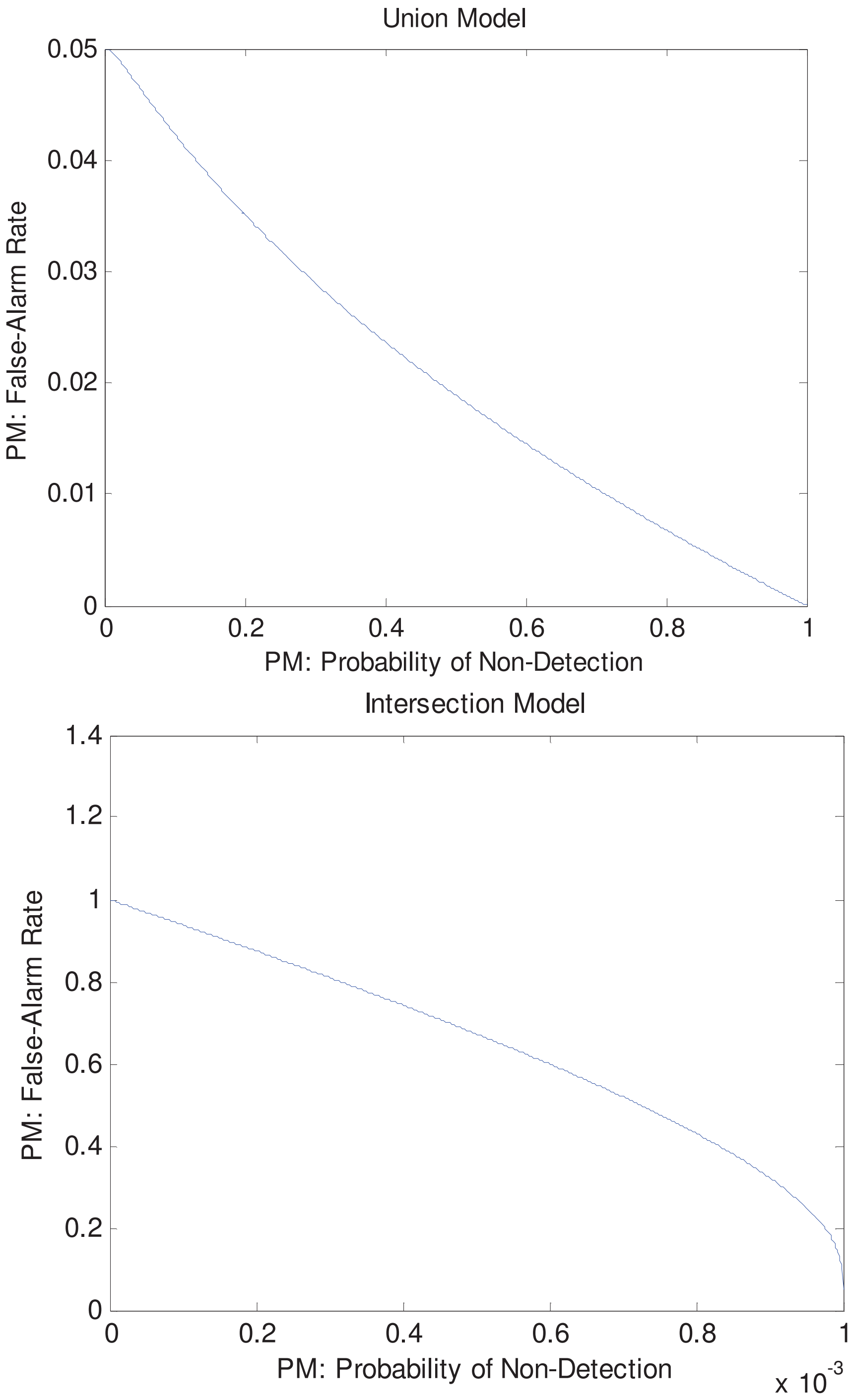


Figure 7, a and b. Threshold of usefulness for PM in a) union and b) intersection analysis.

Integration of the Limits for Safety, Security, and Safeguards with a Common Metric of Efficiency

The integration of safety, security, and safeguards in the methodology is simple to explain in theory, but much more difficult to execute in practice. How should efficiency be calculated? Profit margin appears to be the first choice, but little data exists for analysis. Instead, the effective operating throughput of the facility is recommended: this can be much more easily calculated from the operational parameters. In most cases the exact operating data may not be available, but because of the unique flush-out requirements, extension of a facility's material balance period (MBP) is a reasonable substitute. This is because the flush out is strictly a safeguards requirement that reduces the operating time of the facility.

Additionally, for any safeguards subsystem, (process monitoring is used here as an example), the increase in material balance period can be estimated. Using a baseline of an assumed MBP of eight days, the prior 2D graphs can be rendered into 3D in Figure 8 and Figure 9. In this case Equations 18 above no longer equal, but instead the new effective material balance period can be determined as by Equations 24, 25, and 26, below, where MBP_0 is assumed to be eight and is the base material balance period that exists currently at a facility.

$$MBP(new)=8\frac{\sigma_A}{\sigma_{PM+A}} \tag{24}$$

$$\sigma_{PM+A} = \left[\Phi^{-1}(1-\alpha_{PM+A}) - \Phi^{-1}(\beta_{PM+A})\right]^{-1} \tag{25}$$

$$\sigma_A = \left[\Phi^{-1}(1-\alpha_A) - \Phi^{-1}(\beta_A)\right]^{-1} \tag{26}$$

Figure 8 and Figure 9 show the results, using the assumption of an eight-day MBP.

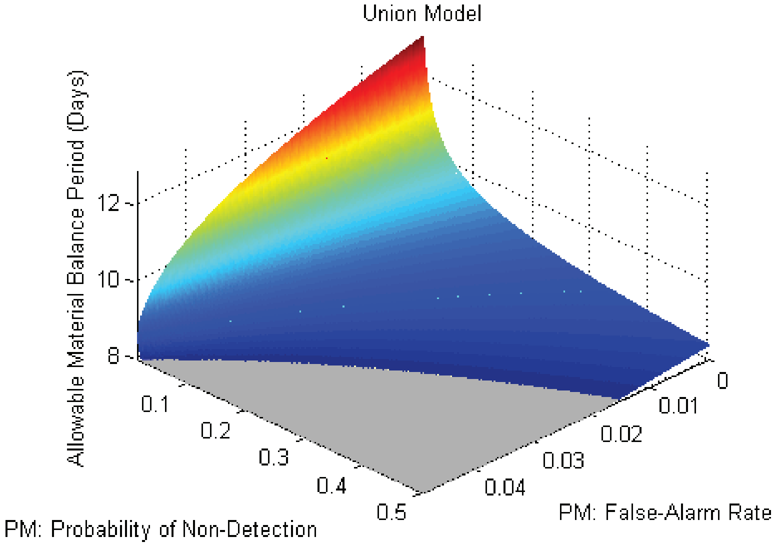


Figure 8. Maximum allowable MBP for given PM characteristics in the Union Model.

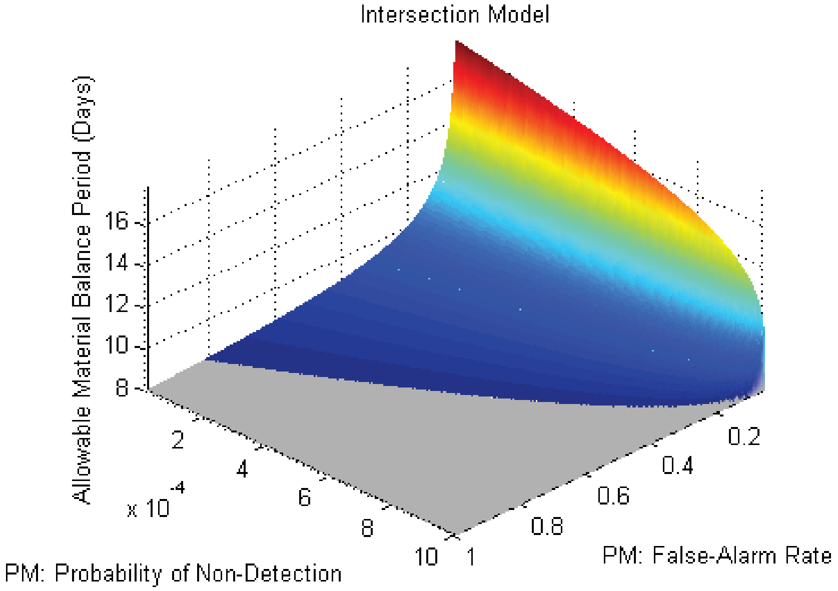


Figure 9. Maximum allowable MBP for PM characteristics in the Intersection Model.

The allowable MBP grows without bound as β_{PM} approaches 0.01% for the Union model or α approaches 5% for the Intersection model. Of course, if one can reach an acceptable level of confidence strictly by PM at cost lower than accountancy, the accounting system becomes unnecessary. This shows the relationship between any two subsystems. Provided there are no conditional statements, a Boolean combination of any set of subsystems can be achieved.

These calculations have assumed that the solution monitoring system does not break any of the conditions set for safety and security. Unfortunately, because of the static and conservative nature of the security assumptions, no official gain can be made in that arena even though there is additional confidence. From a security perspective, this must be evaluated by expert elicitation. However, under the condition that the MBP would exceed the maintenance cycle, the safety system would become the limiting factor. In order to evaluate final effectiveness, a relationship between the final risks and the operational parameters in the PRA for the facility must be created. Provided this is available, the system can be optimized using the operational parameters as free variables.

Note that the value of solution monitoring was monotonically increasing. If the safety analysis also is monotonic (e.g. the solution monitoring system induces an additional degradation factor), this optimization can be found using relatively simple nonlinear optimization techniques that are not as computationally expensive as an unknown space.

CHAPTER III

SAFEGUARDS ENVELOPE EXAMPLE: THE IDAHO CHEMICAL PROCESSING PLANT

Description of the ICPP

Completed in 1953, the ICPP was designed by Oak Ridge National Laboratory (ORNL) personnel to process several types of fuel: aluminum clad fuel from the Material Test Reactor, unclad Experimental Breeder Reactor I (EBR-I) fuel, and Hanford neutron-producing fuel. The amount and type of fuels processed at the ICPP expanded throughout its operational history. During forty years of operation, the facility reprocessed fuel from nearly 100 tests and research facilities around the world and ultimately recovered approximately 32 metric tons of uranium.

The ICPP was equipped with several head-end dissolution processes capable of dissolving the aluminum-, zirconium-, stainless steel-, and custom-clad fuels. The main extraction process separated uranium through a tributyl phosphate (TBP) extraction cycle followed by two methyl isobutyl ketone (MIBK) extraction cycles. History of the facility, description of the data recovery for this facility, and the available data are provided in Appendix 1.

The Safeguards Envelope to be created will focus on a small subsection of the facility, the head-end process immediately before the accountancy tank. This area was chosen because data are available, the tanks in this area receive from multiple other tanks, and the area represents a major safeguards challenge. Figure 10 shows the flow sheet of the ICPP area that is the focus.

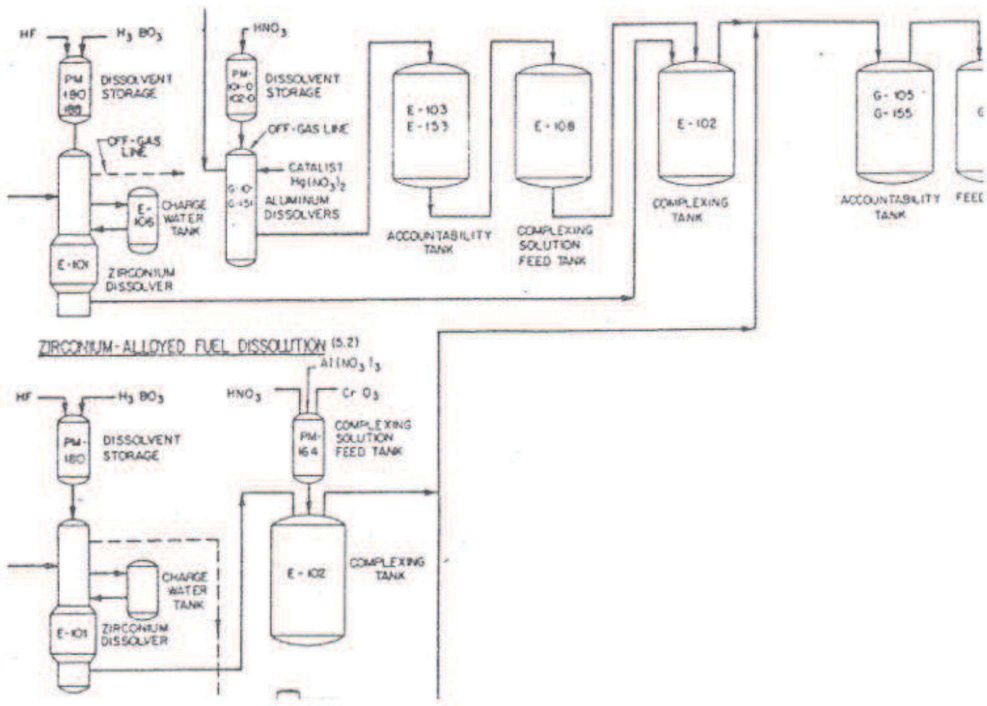


Figure 10. Head-end of the ICPP.

The most important tank in this area is the accountancy tank (G-105). G-105 is flushed immediately prior to measurement (unlike many of the other nearby tanks) and is placed after the solids-removal centrifuges. This material would be relatively easy to clandestinely remove from a sampling tube or second surreptitiously welded pipe (similar to the Ehinger case), without the concern of solids blocking the material or removing excess mass of no use to a proliferator.

Description and Justification of Event #1

Event #1 is a flush event that is duplicated thousands of times over the ICPP operating history. It is shown below as Figure 11.

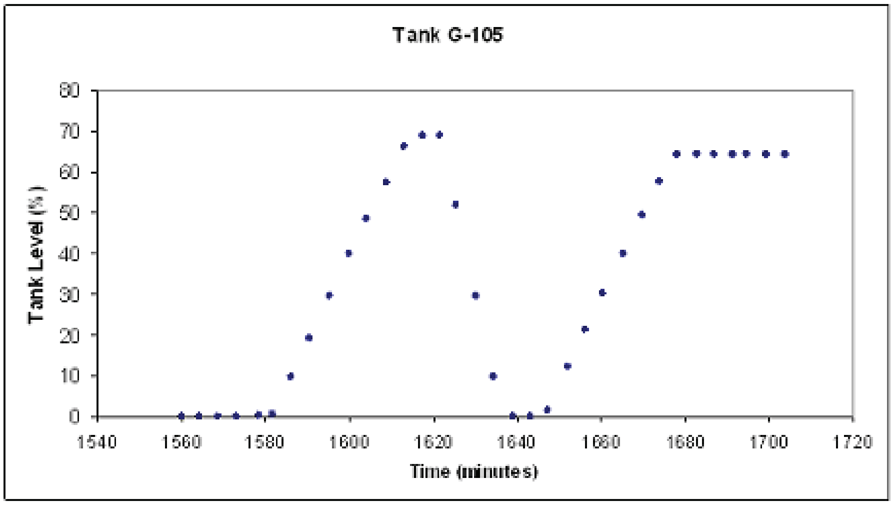


Figure 11. Event #1 is the event that diversions will be tested against.

This event is most relevant because a solution monitoring system does not have the opportunity to acquire enough data to draw conclusions reliably. While this event represents roughly ~2% of operating time, the other events primarily are the hold-modes described in Burr's and Garcia's work and this problem has been effectively solved for safeguards systems. Figure 12 shows the data from operations.

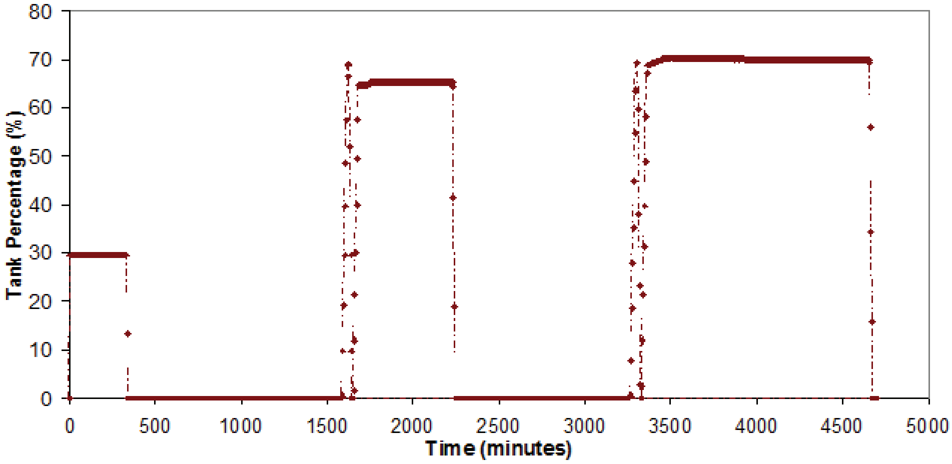


Figure 12. Data for the tank flush.

Despite an increase in fidelity by moving to higher order tests as described in the prior work, the effective decrease in measurement uncertainty is fundamentally limited. This presents a prime opportunity to apply a safeguards envelope, altering the operational parameters in order to increase the overall efficiency.

Process Monitoring Added Without a Safeguards Envelope to Event #1

The most basic form of solution monitoring comes from the application of static change-detection tests. Details of the underlying probabilities of these tests and multisensor integration is provided in the prior chapter. Static change-detection tests, such as a Z-test or students-t test, determine if the expected mean of two sets of data differ significantly at a level of confidence (in this case, the confidence is user-defined). At zero confidence, it can be established all things are the same, at infinite confidence, no two sets of data can be established to have the same mean (unless the sample represents the entire population). As discussed in the prior chapter, the confidence that no material has been removed is 99%, or *p*=0.01, while maintaining that false alarms occur no more than 5% of the time.

A data set containing the actual measurements, taking precisely the same amount of time, should have exactly the same mean, but this technique is even more sensitive to the exact start and stop times of the events. Also, the true mean is difficult to know, even from a historical data set. The estimated mean between the subtraction of the measured value and the "true" (historical) value should have a mean about zero explicitly, however. This allows for a normalized test against the mean, which is much easier in practice. A strict test of the differential between a historical and measured set would violate the requirements for the strict independence of the tests, so the cumulative residual will be tested instead. This has been established to be the most reliable solution monitoring test.

Simulating diversions in the sample is done by reducing the data values of the historical set by a user-defined amount. The amount to be detected in this example is 0.5% removed from the tank over the course of the transient, below the limits for international and domestic safeguards at the ICPP, but likely representative of very large reprocessing facilities like RRP.

Three data sets are created and then tested against each other using a combination of Z tests, students-t tests, Croiser’s cumulative sum tests, and Chi-square tests. The first data set is a hypothetical “historical” set of data for the event. The second data set is an example normal operation set of data, in which no material has been removed. The third data set is a diversion set in which material was removed, peaking at a cumulative 0.5% of the tank removed over the course of the transient in Event #1. Random noise is added to these data, based on the estimated measurement uncertainty expected by the IAEA (0.2%)[23]. Systematic noise has not been added. In a near-continuous operation, systematic noise should be representative of a drift in the data that can be modeled and adjusted. These systems should be recalibrated with each flush out in existing facilities. Assuming a calibration during the flush out at the end of the material balance period (assumed eight days in the base case), the author chooses to assume that the drift of the components over the course of less than thirty days is insignificant. Furthermore, in existing facilities, there are cross-checks from multiple pressure sensors to identify significant calibration drift over the short term.[24] There are also recalibration/verification techniques that have been developed for online use that can be completed within a day.[25] [26] The noise added is shown as Figure 13, a standard Guassian.

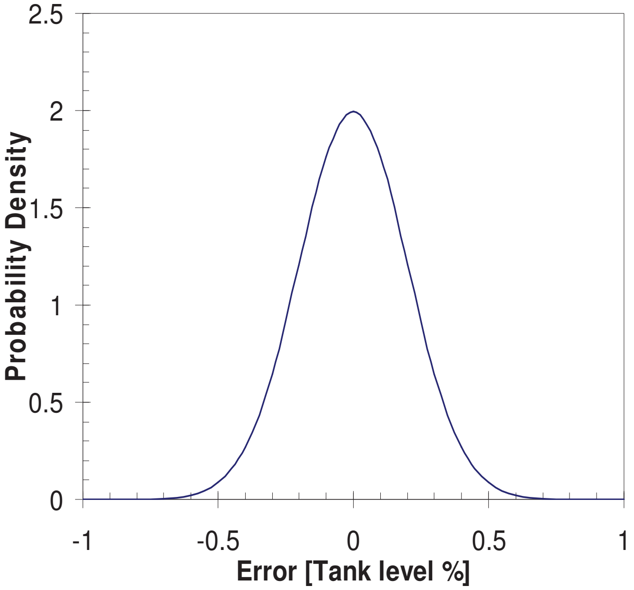


Figure 13. Probability density of measurement error (for the tank level).

Furthermore, as a way of taking advantage of the fact that it is known the historically normal operation should follow a smooth curve, kernel regression is used to smooth the historical set. This reduces the random error in the historical set and allows for the use of a Z test instead of a students-t test.

A test of the normal data set to the historical data set provides a control case: mistaking normal operation for a diversion case represents a false alarm. A test of the diversion data set to the historical data set provides the test case: mistaking a diversion operation for a normal operation case represents a failure to detect. A summation of the false alarms over the total number of normal operation cases yields the false alarm rate. A summation of the failures to detect over the total number of diversion cases yields the probability of nondetection. This is shown below in Figure 14.

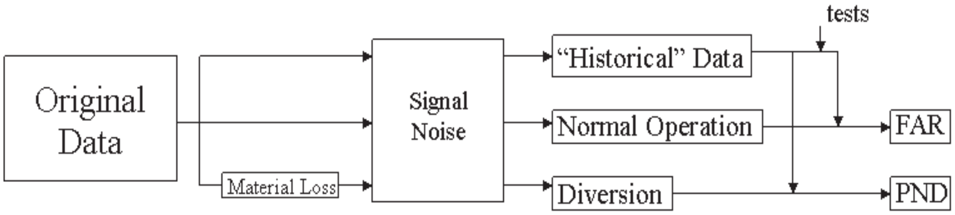


Figure 14. The pathway for analysis for basic process monitoring.

Kernal Regression

To reduce the uncertainty in the historical set, kernel regression was used to create a best-fit function to the data received from ICPP. Kernel regression is a state estimation technique which is considered a nonparametric technique, for unlike linear regression, it does not assume a fundamental distribution in the data[27]. At each observed data point, a Kernel, or weighted function, is centered, and the Kernel assigns a weight to each position based on its proximity to each data point. With a given data set, a kernel (or weight function) is centered at each data point and at each point is used to evaluate the weight of its neighbors for local fitting (see Figure 15).

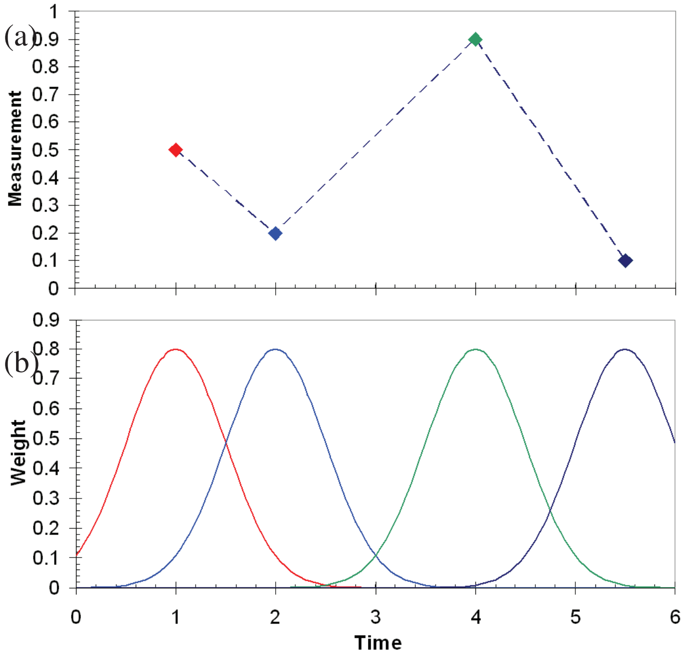


Figure 15 a and b. Plot of a) measurement points which have no linear relationship and b) associated Gaussian weight functions for their respective data points.

In reality, there exist many different kernel functions (e.g. square, quartic, cosine), but the Gaussian remains the most popular. The Gaussian kernel function is as follows:

$$K(x) = \frac{e^{\frac{-(x-X)^2}{2a^2}}}{\sqrt{2\pi}a} \tag{26}$$

where *X* represents the x-value of the measurement point, *x* represents the x-value of the interpolated point, and *a* represents the kernel bandwidth. More will be explained about the kernel bandwidth later, but for now assume it to be any value.

Once applying the weight functions at each desired point, the interpolated y-value can be computed using the Nadaraya-Watson estimator:

$$y_j = \frac{\sum_{i=1}^{n} Y_i K(x_j, X_i)}{\sum_{i=1}^{n} K(x_j, X_i)} \tag{27}$$

where i represents the ith measured point, j the jth interpolated point, Y_i the ith measurement, and y_j the jth weight, interpolated value. As the kernel bandwidth has yet to be chosen, here are the results for Figure 16, a, b, and c. data at various bandwidth values.

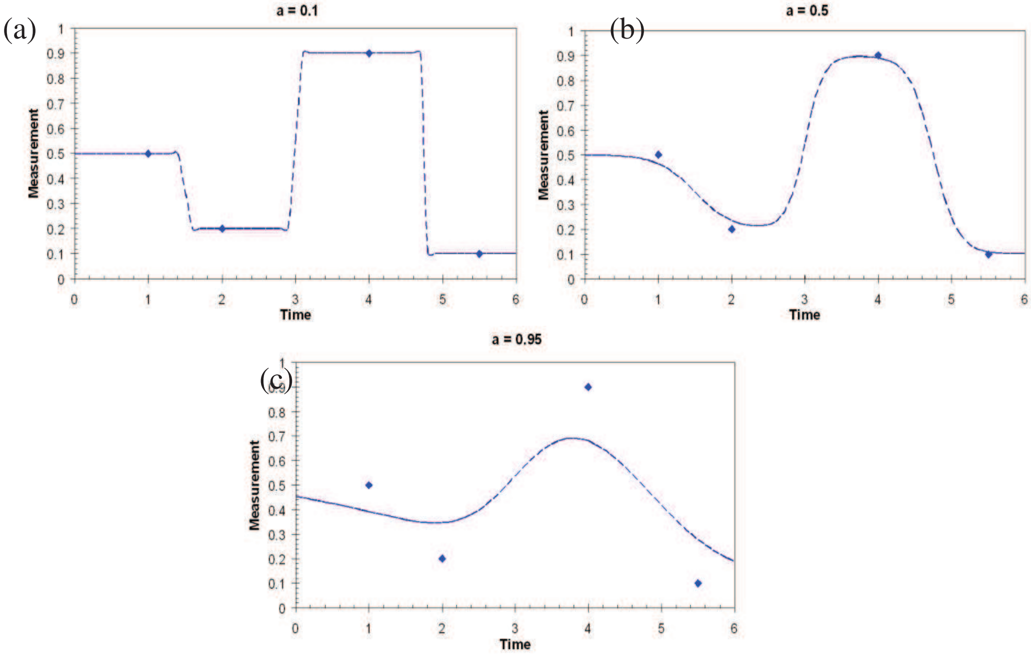


Figure 16, a, b, and c. Kernel smoothing at various kernel bandwidths.

As can be seen from Figure 16, a, b, and c. , various kernel bandwidths give drastically different results. The kernel bandwidth is a user-set parameter that essentially controls the width of the weight function (or rather the “broadening”). Too low a kernel bandwidth results in each measurement point carrying all the weight, resulting in just step interpolation such as in Figure 16, a, b, and c. Too high of a value will "overfit" the data by giving every point nearly equal weight and will approach fitting a single line (linear best fit) to the entire data set. In order to find the best value of the kernel bandwidth, optimization is necessary. This usually requires some outside knowledge that can hint at which value is "right."

The algorithm compares historical and trial data sets and tests the ability to detect a diversion by looking at two items: degree of residual randomness and deviation from the mean. To determine the effectiveness of the statistical tests, Markov Monte Carlo simulation of 500,000+ trials as a simple method for finding out the resultant FAR and PND values.

In reality, data always has noise, and as are result, detecting small diversions is often difficult. To an approximation, we can assume that all measurements take the following form:

$$y_{measured}(t) = y_{true} + \epsilon_{calibration} + \epsilon_{measurement} \tag{28}$$

where $\epsilon_{\text{calibration}}$ is the calibration error and $\epsilon_{\text{measurement}}$ is the measurement error. Calibration error is due to the non-perfect tuning of the measurement device and is usually a static additive error. The error, however, is randomly distributed from one device to another. The more familiar measurement error is that which arises from small fluctuations within the control volume (e.g., miniscule temperature fluctuations or small movement) and is known to be normally distributed. As equation 28 shows, both errors mask the true value and can hamper any verification process. Indeed, both can also be averaged, assuming enough data exist to do so. Unfortunately, this is not the case in most scenarios, including that of our ICPP data. This is the realm in which statistical tests find their application as they look to the overall data trends to discover any abnormalities. Before tests are created, diversion behavior must first be understood.

Material diversions affect two components of measurement data: residual randomness and deviation from the mean or "expected" value. A residual is defined as the difference between the measured value and the true value where $y_{true}(t)$ would be an exact analytical value.

$$y_{\text{residual}}(t) = y_{\text{measured}}(t) - y_{\text{true}}(t) = \epsilon_{\text{calibration}} + \epsilon_{\text{measurement}} \qquad (29)$$

As equation 29 shows, a measurement residual should be nothing more than a time series of errors with a random distribution and mean of zero. In a diversion case, however, the residual would take on an entirely different behavior. First, it is important to understand that abnormal data can be seen as normal data with an added deviation where *diverted(t)* is the nuclear quantity taken as a function of time as shown in equation 30, below.

$$y_{\text{abnormal}}(t) = y_{\text{true}} + \epsilon_{\text{calibration}} + \epsilon_{\text{measurement}} - \text{diverted}(t) \qquad (30)$$

If the residual of this curve was computed with respect to the true values of a normal curve, illustrated in equation 31, below, then it becomes obvious that the residual of an abnormal data curve is just a normal residual, such as equation 29, but with an added non-random and/or non-zero mean function.

$$y_{\text{abnormal}}(t) - y_{\text{true}} = \epsilon_{\text{calibration}} + \epsilon_{\text{measurement}} - \text{diverted}(t) \qquad (31)$$

In other words, to determine whether or not a tank has been tapped, one simply needs to look at the residual of its data; if the residual has neither a purely random distribution nor a zero mean, then assume that a diversion has taken place (see the following section).

Unfortunately, detection with the above methodology is difficult for two reasons: not knowing $y_{\text{true}}(t)$, and having sparse data. Computing the most accurate residuals requires knowing beforehand what $y_{\text{true}}(t)$ is, which is technically impossible. In fact, knowing it would imply perfect measurements, which would make this entire statistical process unnecessary. However, what is known is the historical data, which tell what the measurement "ought" to be. With that, it becomes feasible to make good *approximations* of $y_{\text{true}}(t)$, especially with good fitting techniques. One must take caution, for approximations can be too uncertain if the base data are too sparse. Even the tests themselves can be misleading if not enough information is present. Again, advanced statistics become useful. Numerous techniques have evolved which take advantage of sparse data and create reliable models to work with (e.g., Principle Component Analysis, Least-Squares Fit). With both reliable historical data and advanced statistics, it becomes very possible to distinguish abnormal behavior from normal operating conditions.

Once the three simulated curves were created, Kernel regression was performed on the historical set to later approximate residuals. Kernel regression is a powerful state-estimation technique designed to fit an approximate curve to noisy data. Unlike most familiar regression techniques, Kernel regression is non-parametric and does not actually make any initial assumptions about the shape of the curve. Instead, it applies a Gaussian weight function centered at each data point and gives each neighboring point a contribution that is proportional to their distance. This is seen in Figure 17, a kernel regression applied to some of the ICPP data, where the blue dashed line is the new estimated historical true values and the green were the raw data.

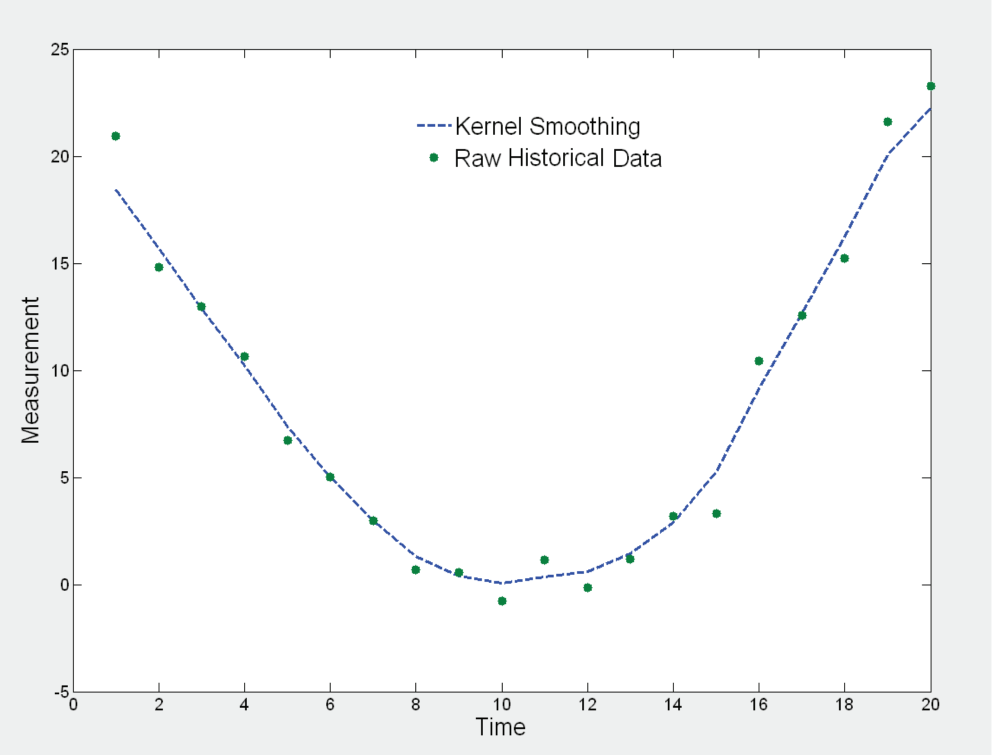


Figure 17. Kernel smoothing on simulated historical data.

The degree of fitting is also a user-set parameter, called the Kernel bandwidth. Too low a value connects the dots poorly, while one too high will "overfit" and produce large errors. This is one of the parameters that can be optimized in the algorithm for best performance.

Once the Kernel-smoothed historical curve is obtained, the difference between that curve and the two trial curves (normal and diversion curve) give each trial curve its respective residual approximations. This is done by simply subtracting the raw data from the Kernel-smoothed curve for both the historical and trial case, as shown in Figure 18.

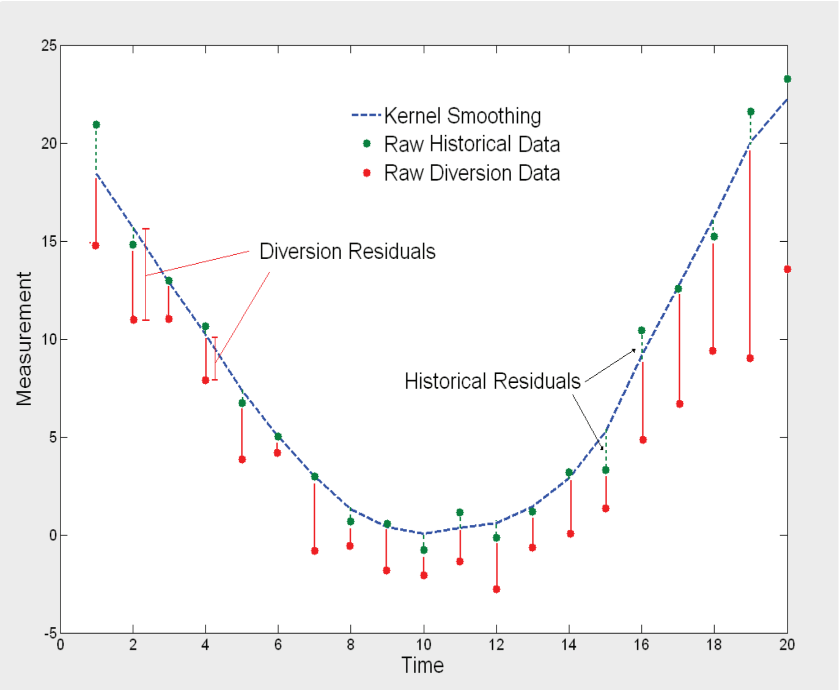


Figure 18. Diagram showing residual analysis with historical data and diversion data.

Z and Students-t Tests

Z tests and students-t tests are similar static mean differentiation tests. These tests are designed to identify whether the mean of two sets of data are different (i.e., determine the conclusion of differentiation between two sets at a threshold of evidence. These tests are very commonly used in statistical analysis because they are the most powerful tests for statistically normal data. Besides the assumption of normality, a Z test assumes a known variance and true mean for the population, while the student-t test does not. The students-t test will reduce to a Z test under large sample sizes (as the variance of the sample limits to the variance of the tested population. The Z test and students-t test are shown below as equations 32 and 33.

$$Z_{\bar{x}} = \frac{\bar{X}-\mu}{\sigma_{\bar{X}}} \qquad \sigma_{\bar{X}} = {}^{\sigma}\!/\!_{\sqrt{n}} \tag{32}$$

$$t_{n_1-n_2-2} = \sqrt{S\frac{2}{\bar{Y}_1} + S\frac{2}{\bar{Y}_2}} \qquad S_{\bar{Y}_1-\bar{Y}_2} = \sqrt{S\frac{2}{\bar{Y}_1} + S\frac{2}{\bar{Y}_2}} = \sqrt{\frac{s_1^2}{n} + \frac{s_2^2}{n}} \tag{33}$$

In these equations, $\bar{X}$ is the mean of the sample, μ is the true mean of the population against which the sample is being tested, $\sigma_{(\bar{X}}$) is the estimated variance of the limited sample, calculated from the true variance (σ) and the number of samples (n). Y is the mean of two independent samples, with S the combined normalized variance of the two independent samples. t and Z are both the test statistics which are inserted into the normal Gaussian equation to determine the power at which a conclusion can be drawn. The Z test statistics are provided into the integration of the normal Gaussian. The normal Gaussian is shown as equation 34, followed by its integration as equation 35.

$$\phi(x;\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{34}$$

$$\Phi(z) = \int_{-\infty}^{z} \phi(x)dx \tag{35}$$

This integration provides the p value. While it is commonly referred to as a probability value, the p value represents a likelihood based on the current level of evidence. There are two ways of using a Z or students-t test: "one-tailed" and "two-tailed." A one-tailed test only tests one side of the bell curve: the analyst must choose to test for above average or below average. A two-tailed test will provide information regarding both significantly above and significantly below, but has a higher threshold of evidence. This is seen most easily in

Figure 19; it is clear that if the same evidence threshold for the one-tailed test was used for the two-tailed test (i.e. the highlighted areas under the curve) then the "tails" would be thinner for the two-tailed test.

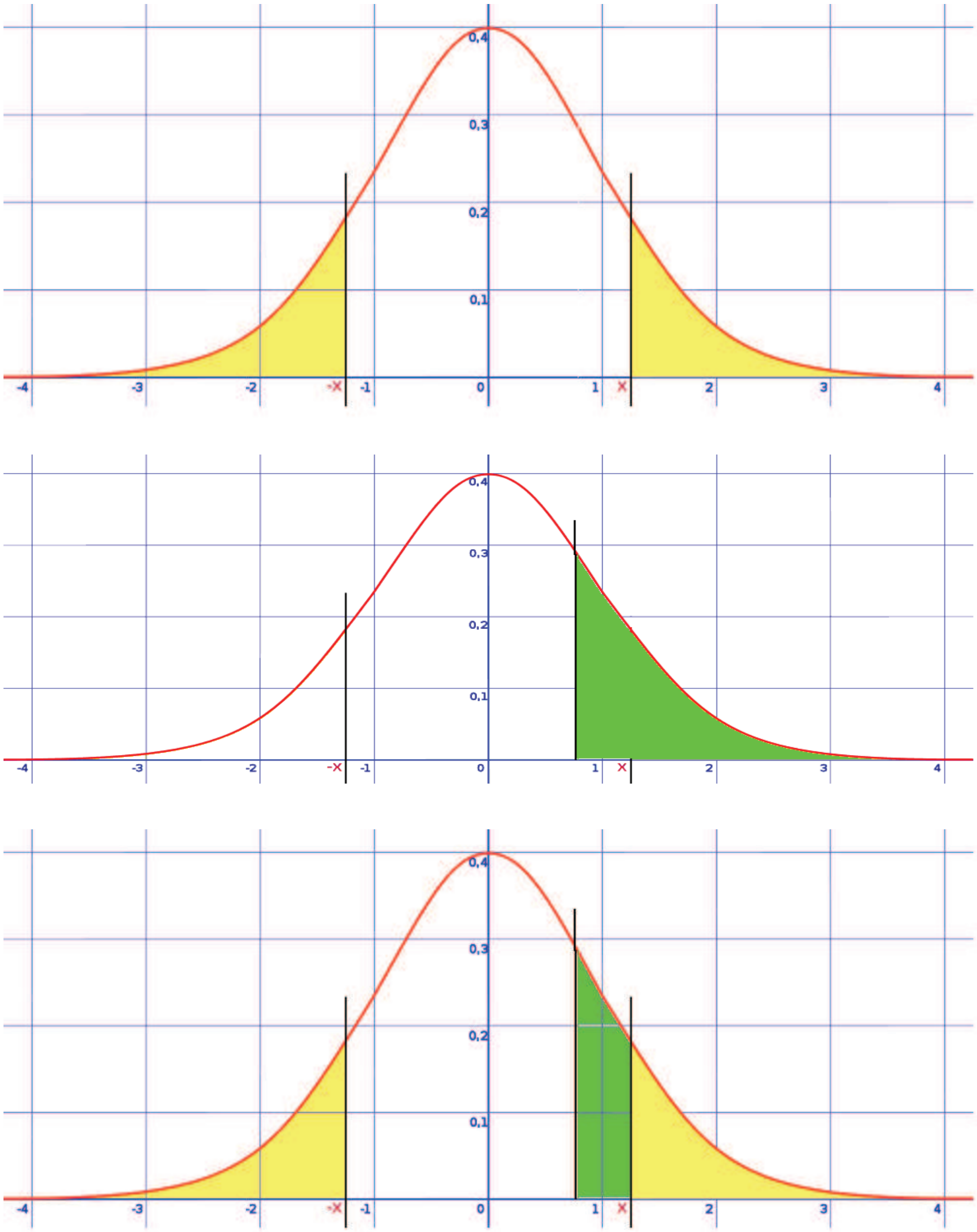


Figure 19. Comparison of one and two sided tests.

In application the *p* values for practically every value of *Z* have been calculated, and more often than not the *Z* value for a given test is simply compared to the *Z* value at a given threshold of likelihood at that level of evidence (data).

The student t statistic works very similarly, with the distinction that the “tails” are wider because the variance is not known. The test is effectively inferring the true variance as part of the test, which is why it has degrees of freedom in measurement of comparison to the two samples. As the likelihoods have been evaluated for each t value, the students-t test statistic is typically directly compared rather than integrating the function.

Chi-Square Test

A Chi-Square test has been used to replace the original Z testing of the cumulative sums to identify if the deviation from the “true” values has the appropriate variance. An unusually high variance could represent diversion, mechanical fatigue, or sensor failure. While the typical Chi-Square test is used to evaluate the performance of a system, the application of this test to the residuals can provide a second measure to determine if the residuals are away from normal.

Equation 1 shows a standard Chi-Square test. In this equation, x^2 is our test statistic, O_i is the individual observations (residuals), and E_i are the expected values.

$$x^2 = \sum_{i-1}^{r} \left[\frac{(O_i - E_i)^2}{E_i}\right] \tag{36}$$

The numerator term is a sum of the residuals, and the denominator term becomes the variance of the historical set. As with a student’s-t test, very little is assumed about the data that is available and, as a result, the Chi-Square test has differing thresholds for evidence based on the number of degrees of freedom. The degrees of freedom are one less than the number of observations in the set. This test becomes more powerful faster with more data than other test types because the data are being used two ways (note: this also means outliers can more easily impact the result). Seeking additional data in limited areas is promising in utilizing this test and therefore lower false alarms for the same probability of nondetection.

This test has been integrated with the student's-t as part of the standard suite for detecting diversions. Specifically, this test provides a mechanism for combining all residuals positively to address the diversion scenario of removal of material during a statistically high event.[iv]

The issue that arises from adding a Chi-Square test is the increased FAR that is to be expected from adding additional tests. As discussed previously, a union or intersection model can be created with the Chi-Square and cumulative sum test. Some diversion types would not typically be detected with the cumulative sum test, and so only a union model can be applied. This has an unfortunate disadvantage: the FAR must increase with the linearly with the FAR for each test, but the detection probability for some diversions is only derived from one test.

Croisier's CUSUM

Croisier's CUSUM is a cumulative sum method which updates the prior sum before moving to the next iteration. The update to the prior sum determines if the new sum will be moved towards zero (as given in Eqs. 2-7), or if the system will be reset to zero. This resetting to zero is expected to increase the PND but decrease the FAR and so may be preferred in applications where many measurements are taken in multiple locations. The reduction to FAR, which increases linearly to the number of measurements in the union model, is a crucial requirement for MBP and acceptance by operators.

$$C_t = \{(S_{t-1} + e_t)^T \Sigma^{-1} (S_{t-1} + e_t)\}^{(1/2)} \tag{37}$$

[iv] This diversion is outlined in a later section.

$$S_t = S_{t-1} + e_t - k \tag{38}$$

$$S_t = 0 \tag{39}$$

$$k = (S_{t-1} + e_t)\frac{\lambda}{C_t} \tag{40}$$

$$S_t = (S_{t-1} + e_t)\frac{1-\lambda}{C_t} \tag{41}$$

$$Y_t = \left(S_t^T \Sigma^{-1} S_t\right)^{(1/2)} \tag{42}$$

In equations 37-42, C_t is the existing and updating cumulative sum, S_{t-1} is the prior sum, the new S_t is the new sum added onto this group, k is a scalar (in the direction of S for the multivariate case), λ is a scaling parameter, and Y_t is the new test statistic.

The procedure for this analysis is very similar to other cumulative sum tests. The updated cumulative sum is used as a test statistic to determine if the root mean error is beyond a certain threshold with a given probability. Unique to this test is the parameter λ. λ is a scaling parameter for the impact of the most recent sum. In a students-t test, this factor is zero. However, if this parameter is nonzero, λ reduces the FAR, but increases the PND because it adds an additional threshold for divergence on a given measurement before it is added to the cumulative sum, as expected by a system which has thousands of measurements.

One of the issues associated with Croisier's cumulative sum is that a control parameter, λ, is required as well as the standard threshold. As with the Chi-Square test, this test has the potential to increase the optimization, but also synthetically increases the parameter space. In the event that Croiser's CUSUM's λ variable is highly sensitive, this test must be discarded.

Procedure Used

A Markov Monte Carlo chain was created for each set. In each trial, the errors were added randomly, as above, and then the historical set was smoothed by the use of Kernel regression. The cumulative residuals were used as the basis for testing, as their mean should be zero and this has historical success. 500,000 runs were used to evaluate the probabilities, but 100,000 runs were repeated as part of code-checking. As each data point was added, a cumulative residual test was used to determine if the event (at that point) had exceeded the threshold. This type of test does not require the exact stop time of the transient and was used as a Z or student-t test. Using the assumption that the exact stop time was used, a second final cumulative sum test was used with a students-t test. The thresholds for these tests were altered incrementally, to determine the optimal thresholds.

A multivariate test was also used, combining the density and level measurements to generate an effective volume. This test exceeded expectations of sufficient magnitude to require a second analysis. The FAR and PND were both significantly lower than 0.1%, allowing for several months MBP. This error took significant time to track down because the code associated with these tests had not been changed before running the analysis. It was believed that a heretofore unknown error within the code had produced a major bug in the reporting statistics.

Several techniques for debugging were applied, as well as external review by colleagues not associated with this research. Finally as the code was determined to be accurate, and the new test variables—a combination of level, density, and temperature—were checked to ensure no major data flaws.

An analysis for skewness on the density and level measurements provided no valuable results, even at the *p*=0.01 level. While, at a glance, the data are correct, a very careful examination shows that the density measurements begin later and end sooner than the level measurements. As a result, the error (which is most significant at the beginning and ending of the transient) was drastically misestimated, suggesting that process monitoring could perform much better than would be achievable in actual operations. This overlap is demonstrated in Figure 20.

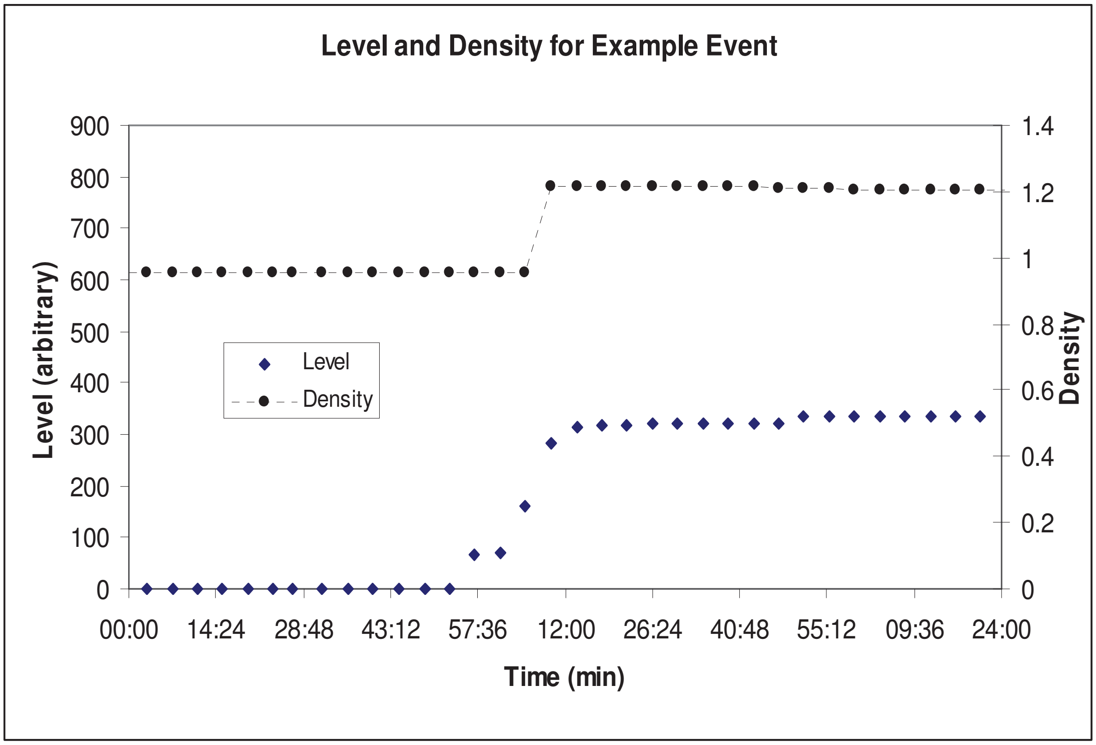


Figure 20. Level and density discrepancy.

The reason for the drastic increase in material balance period with the safeguards envelope operation was because of the synthetic increase in the number of points created within the area in which the error was driven to zero. This compounded the underestimation of the FAR and PND and led to the drastic overestimation of the MBP.

Several variables were still tested. Multiple case numbers were run to establish the uncertainty in the final results through the code. A test including level, density, and temperature with Kernel regression is the first test; density and temperature are not expected to contribute significantly to detection, but may contribute to false alarm rate. A second test, focusing only on level, is next, followed by a final test in which the Chi-square test is not applied for comparison.

Results of the Basic Process Monitoring

The results of the example basic process monitoring are below as Table 1 for three diversion percentages.

Table 1. Results of the example monitoring.

Diversion of 0.5% vs Error of 0.1%

Cases		FAR - Base	PND - Base	MBP - Base
10000	AllVariables	0.00%	0.99%	12.96
	Level	0.01%	0.13%	>30
	Level (No Chi2)	0.00%	0.19%	23.99
100000	AllVariables	0.00%	0.91%	13.19
	Level	0.30%	0.13%	>30
	Level (No Chi2)	0.05%	0.15%	>30
100000	AllVariables	0.00%	0.89%	13.24
	Level	0.00%	0.14%	>30
	Level (No Chi2)	0.01%	0.13%	>30
100000	AllVariables	0.00%	0.92%	13.21
	Level	0.01%	0.14%	>30
	Level (No Chi2)	0.30%	0.15%	>30
500000	AllVariables	0.00%	0.89%	13.24
	Level	0.00%	0.16%	28.74

Table 1 Continued

	Level (No Chi2)	0.00%	0.15%	>30

Diversion of 0.5% vs Error of 0.2%

		FAR -	PND -	MBP -
Cases		Base	Base	Base
10000	AllVariables	1.52%	10.23%	9.14
	Level	3.49%	5.54%	8.91
	Level (No Chi2)	3.58%	6.31%	8.76
100000	AllVariables	1.44%	10.36%	9.16
	Level	3.45%	6.17%	8.85
	Level (No Chi2)	3.93%	6.06%	8.89
100000	AllVariables	1.46%	10.28%	9.16
	Level	3.49%	6.24%	8.81
	Level (No Chi2)	3.51%	6.13%	8.82
100000	AllVariables	1.50%	10.35%	9.14
	Level	3.49%	6.24%	8.81
	Level (No Chi2)	3.40%	6.08%	8.88
500000	AllVariables	1.48%	10.30%	9.15
	Level	3.40%	6.14%	8.88
	Level (No Chi2)	3.48%	6.16%	8.83

Diversion of 0.5% vs Error of 0.3%

		FAR -	PND -	MBP -
Cases		Base	Base	Base
10000	AllVariables	11.09%	19.21%	8.00
	Level	16.40%	14.56%	8.00
	Level (No Chi2)	16.30%	14.65%	8.00
100000	AllVariables	10.85%	19.11%	8.00
	Level	10.16%	14.56%	8.00
	Level (No Chi2)	16.28%	14.33%	8.00
100000	AllVariables	10.78%	19.45%	8.00
	Level	16.37%	14.55%	8.00
	Level (No Chi2)	16.54%	14.59%	8.00
100000	AllVariables	10.88%	19.11%	8.00
	Level	16.32%	14.58%	8.00
	Level (No Chi2)	16.57%	14.57%	8.00
500000	AllVariables	10.91%	19.25%	8.00
	Level	16.42%	14.54%	8.00
	Level (No Chi2)	16.27%	14.53%	8.00

The results for basic process monitoring suggest that highly accurate online measurements (similar on-line to accountancy uncertainty) would greatly increase MBP; the current state of the art would provide a small benefit, but inferior equipment would not provide any benefit. There are additional insights from these data, but they are addressed in the results for the safeguards envelope, below.

In the case of the diversion and error required by domestic safeguards, and using the IAEA target values (Diversion of 0.5% vs Uncertainty of 0.2%), moderate benefit can be made from process monitoring. Using only level as the measurement and only the knowledge of the start of the transient, the increase in effective MBP is shorter than one day. Using the knowledge of the exact start and stop of the transients, a day of operating time can be gained. This increases the "uptime" to 9 of every 10 days, rather than 8 of every 9 days, a gain of roughly 1% in total efficiency in the facility. Note that while it may at first appear to be an increase of ~10% efficiency, it is assumed that the facility will operated quasicontinuously (i.e., as soon as one cycle is completed, it resumes operation). Flushout takes only one day, and return to equilibrium requires no time. With the assumptions that flushout takes a day, and the facility requires two days to equilibrate, the increase in efficiency is ~2.3%.

Safeguards Envelope Application

Clearly some benefits accrue from this rudimentary process-monitoring system, but the system could be optimized. Statistical process monitoring systems are limited by their fundamental data: no statistical test can make a certain conclusion on no data, and few can make any valuable conclusions on very limited data. Thus, the weakest points in the monitoring system must occur in the areas of the lowest data (hence the use of the transient Event #1 rather than a simple fill or simple flush operation). The expectation values of Equations 32 and 33 should still be zero (because this is more data that are distributed about zero, this make sense) but the variance should increase. Similarly, the likelihood of detection of a diverted case continues to have an expectation value of the diversion with an increase in variance, but the additional data are more likely to push the measured value to the expectation value.

An increase in data comes at a cost. Increasing the measurement points using the already existing equipment (presuming they are measuring as soon as they are cleared) requires that operations be executed slowly as compared to their original operating speed. Thus, there is a tradeoff: operations may be slower, but the plant would be able to operate longer. The amount of slow down in the process must be kept to an absolute minimum: that is, to the immediate fill-flush events (2.2% operating time). The idea of slowing a process down in order to increase throughput seems highly counterintuitive, but like the proverbial tortoise and hare, it is likely that the slower but longer operations complete more operations in the same amount of time.

This increase in operations also must be evaluated as part of the security and safety envelopes. A decrease in operating speed does not, at first glance, appear to cause a change to the security of the material, especially under the assumptions currently posited by the USDOE. Traditional wisdom also suggests that slowing operations down would not induce safety issues, as the pressures would decrease, material would have lower velocity (at least not increasing wear on the pipes), and less pumping power would be required. Therefore, a back-of-the-envelope calculation suggests that efficiency in reprocessing can be increased by reducing safeguards burden while maintaining the same levels of safety and security.

Illustration of the Safeguards Envelope Method

As an example of safeguards envelope, consider the case in which the fill-flush transient (Event #1) is reduced to half speed to allow for more data to be available to the process monitoring system. To simulate half speed operation, the “true” data sets were linearly interpolated to create an additional datapoint. While this can cause some issues with the smoothing at the very top of the curve, it should add error rather than reduce it with the Kernel smoothing and is a conservative assumption.[v] Using a similar procedure to that described above, a Markov Monte Carlo chain was created for each set. In each trial, the errors were added randomly as above, and then the historical set was smoothed by the use of Kernel regression. The cumulative residuals were used as the basis for testing as their mean should be zero and this has historical success. 500,000 runs were used to evaluate the probabilities but 100,000 runs were repeated as part of code-checking. As each data point was added, a cumulative residual test was used to determine if the event (at that point) had exceeded the threshold. This type of test does not require the exact stop time of the transient and was used as a Z or student-t test. Using the assumption that the exact stop time was used, a second final cumulative sum test was used with a students-t test. A multivariate test was also used, but the data were determined to be circumspect. The thresholds for these tests were altered incrementally, to determine the optimal thresholds.

Several variables were tested. Multiple case numbers were run to establish the uncertainty in the final results through the code. A test including level, density, and temperature with Kernel regression is the first test because density and temperature are not expected to contribute significantly to detection, but may contribute to false alarm rate. A

[v] Consider the case of two points opposite with the true maximum between them: linear interpolation will tend to suggest material removal, which is conservative in PND and nonconservative in FAR.

second test focusing only on level is next, followed by a final test in which the Chi-squared test is not applied for comparison.

Results of the Safeguards Envelope Operation

The results of the example basic process monitoring are below as Table 2 for three diversion percentages.

Table 2. The results of the safeguards envelope application.

Diversion of 0.5% vs Error of 0.1%

Cases		FAR – Base	PND - Base	MBP – Base	FAR - SE	PND- SE	MBP - SE
10000	AllVariables	0.00%	0.99%	12.96	0.43%	0.00%	>30
	Level	0.01%	0.13%	>30	0.58%	0.00%	>30
	Level (No Chi2)	0.00%	0.19%	23.99	0.00%	0.00%	>30
100000	AllVariables	0.00%	0.91%	13.19	0.52%	0.01%	>30
	Level	0.30%	0.13%	>30	0.55%	0.00%	>30
	Level (No Chi2)	0.05%	0.15%	>30	0.02%	0.00%	>30
100000	AllVariables	0.00%	0.89%	13.24	0.52%	0.00%	>30
	Level	0.00%	0.14%	>30	0.53%	0.00%	>30
	Level (No Chi2)	0.01%	0.13%	>30	0.02%	0.00%	>30
100000	AllVariables	0.00%	0.92%	13.21	0.53%	0.00%	>30
	Level	0.01%	0.14%	>30	0.54%	0.00%	>30
	Level (No Chi2)	0.30%	0.15%	>30	0.00%	0.00%	>30
500000	AllVariables	0.00%	0.89%	13.24	0.55%	0.00%	>30
	Level	0.00%	0.16%	28.74	0.53%	0.00%	>30
	Level (No Chi2)	0.00%	0.15%	>30	0.00%	0.00%	>30

Diversion of 0.5% vs Error of 0.2%

Cases		FAR - Base	PND - Base	MBP – Base	FAR - SE	PND- SE	MBP - SE
10000	AllVariables	1.52%	10.23%	9.14	1.19%	1.33%	11.82
	Level	3.49%	5.54%	8.91	2.74%	0.31%	15.45
	Level (No Chi2)	3.58%	6.31%	8.76	2.16%	0.36%	15.24
100000	AllVariables	1.44%	10.36%	9.16	1.19%	1.29%	11.88
	Level	3.45%	6.17%	8.85	2.81%	0.34%	14.90
	Level (No Chi2)	3.93%	6.06%	8.89	2.42%	0.42%	14.31
100000	AllVariables	1.46%	10.28%	9.16	1.18%	1.29%	11.89
	Level	3.49%	6.24%	8.81	2.79%	0.35%	14.82

Table 2 Continued

	Level (No Chi2)	3.51%	6.13%	8.82	2.42%	0.37%	14.88
100000	AllVariables	1.50%	10.35%	9.14	1.15%	1.34%	11.82
	Level	3.49%	6.24%	8.81	2.83%	0.38%	14.33
	Level (No Chi2)	3.40%	6.08%	8.88	2.42%	0.40%	14.50
500000	AllVariables	1.48%	10.30%	9.15	1.17%	1.26%	11.94
	Level	3.40%	6.14%	8.88	2.86%	0.35%	14.66
	Level (No Chi2)	3.48%	6.16%	8.83	2.42%	0.40%	14.47

Diversion of 0.5% vs Error of 0.3%

Cases		FAR – Base	PND - Base	MBP - Base	FAR - SE	PND- SE	MBP – SE
10000	AllVariables	11.09%	19.21%	8.00	10.10%	5.59%	8.00
	Level	16.40%	14.56%	8.00	12.67%	4.29%	8.00
	Level (No Chi2)	16.30%	14.65%	8.00	10.34%	4.51%	8.00
100000	AllVariables	10.85%	19.11%	8.00	0.97%	0.54%	8.00
	Level	0.16%	14.56%	8.00	12.75%	3.89%	8.00
	Level (No Chi2)	16.28%	14.33%	8.00	10.27%	4.89%	8.00
100000	AllVariables	10.78%	19.45%	8.00	9.78%	5.75%	8.00
	Level	16.37%	14.55%	8.00	12.66%	4.06%	8.00
	Level (No Chi2)	16.54%	14.59%	8.00	10.39%	5.01%	8.00
100000	AllVariables	10.88%	19.11%	8.00	9.79%	5.28%	8.00
	Level	16.32%	14.58%	8.00	12.26%	3.86%	8.00
	Level (No Chi2)	16.57%	14.57%	8.00	10.36%	4.86%	8.00
500000	AllVariables	10.91%	19.25%	8.00	9.80%	5.39%	8.00
	Level	16.42%	14.54%	8.00	12.57%	3.97%	8.00
	Level (No Chi2)	16.27%	14.53%	8.00	10.31%	5.06%	8.00

The results for Safeguards Envelope process monitoring suggest that highly accurate online measurements (similar on-line to accountancy uncertainty) would greatly increase MBP even over basic process monitoring. The reporting period for this type of material is one month. Envelope operation, applied to highly accurate measurements, could yield drastic increases in efficiency. In the case of basic process monitoring, the difference between all variables and only a limited subset (testing for an expected diversion) is very large. This suggests that, as additional nondestructive analysis techniques are brought online, envelope operation becomes even more relevant. This example case is not currently applicable, however, because the on-line measurements that are available do not have this level of accuracy.

In the case of the standard diversion against the state of the art for measurements, the basic process monitoring change in MBP between multiple variables and level is less pronounced in this diversion percentage than in the prior example. Basic process monitoring also shows that adding or removing a more advanced test (for example, the Chi-square) has only a limited impact on MBP. Safeguards Envelope operation did significantly increase MBP, and the difference between a known and unknown diversion was much more pronounced. The calculation for efficiency becomes more complicated, however. Because a subset of the operations of the facility are at half speed, the efficiency decrease through this choice of operation could be between 1.1% and 2.2%, depending whether the half-speed operations can be performed simultaneously or must be explicitly staggered (this is unrealistic, since tanks are connected). The increase in uptime, assuming a twelve day MBP using slightly more optimized thresholds and simultaneous half speed operations, would result in an efficiency increase of 1.2%. A perfectly staggered half-speed operation for two tanks would reduce this to roughly 0.1% efficiency increase. However, if it is assumed that flush-outs require three days, these efficiency impacts become 3.9% and 2.8% respectively, quite significant considering operational cost of ICPP was approximately $1 million/hr[vi].

The application of the safeguards envelope in the case of inferior equipment does not generate any efficiency increase. It is worth noting that the FAR and PND are both reduced significantly under SE operation, but in this regime, accountancy measurements clearly dominate process-monitoring applications.

Safety and Security Considerations in this Envelope Operation

Though there is proven benefit from a safeguards perspective in this relatively simple change of operation, the safety and security concerns that were only cursorily considered must be evaluated in more detail. The safety envelope within which the facility operated is not available in the public domain, nor are the exact security configurations and systems. Expert elicitation was used as a surrogate, in the framework of PRA for safety and the DOE Security Orders for Security.

The major classes of accident in the hypothetical PRA would have been those discussed in the prior chapters: irrecoverable damage, recoverable damage, and threat to the public. Because only one subsystem is altered in this example envelope, and there are only a few modes of failure for a tank, it is not an insurmountable problem to estimate the effects of the suggested changes. The impact of risk is broken down into probability of an event and its consequences. The change in risk as a result of slowing down operations initially appears very low. The tank is clearly designed to operate for long periods of time with material in it, and so an increase in material holding for short periods of time does not appear to increase the risk of either corrosive tank failure or plugging. Similarly, the material is no more dangerous as a result of residence time than the other materials.

However, consulting with prior employees reveals that the flushouts prior to tank fill had a major and minor purpose. The major purpose was to ensure that the tank was fully cleared of material, but the minor purpose was to reduce the amount of hydrofluoric acid (HF) resident in the accountancy tank. Because of the multiple-head-end structure of the facility (see Figure 1 in prior chapter), HF was used for some dissolutions. The accountancy tank was not made of the steels, very highly resistant to HF and HNO_3, that are available

[vi] ~5000 employees at $200/hr with overhead ~$1mil/hr.

today, but used the technology available in the 1950s. Some tanks were better able to handle HF, but would have been corroded by HNO_3, allowing for dissolution of material in HF and storage, but both HF and HNO_3 lines entered the accountancy tank. Counter to intuition, the envelope operation suggested may have actually increased risk because of increased residency of HF; a valve or pipes connected to the accountancy were more likely to be corroded.

There is a relatively simple solution to the corrosion problem: an increased maintenance of the valves that would be corroded by HF. Corrosion and replacement of valves was a common problem, but a major failure and subsequent leak of HF and spent fuel would have been extremely expensive in terms of time and money. An extremely large release would have been even more dangerous for humans because the facility was, at the time, pushing the boundaries for exposure to HF. HF causes irreversible heart damage and failure with relatively small chemical doses, and some former workers anecdotally mention that it was a major concern of the plant.

The security perspective also suggested little to no change at first calculation; the DOE Security Orders provide no benefits or drawbacks for material residence time. Work by Citpiti and Duran, however, suggests process monitoring models that adjust the alert status of the physical security force against the insider and insider–with-collusion threat.[28] In this case, the increased detection probability directly results in a more timely response from the physical security force. This work suggests that increases in detection and neutralization increase with a process monitoring detection as physical security forces are then placed on higher alert. The generalization of this method has not been publicly released, but this suggests that the example envelope would significantly increase the physical security against two of the three major threats.

This example shows that a thorough understanding of the plant is required and that the operating space must be designed from all aspects: safety, security, and safeguards.

Limitations of the Safeguards Envelope Application

This example envelope is not the fully optimized envelope and will not catch all possible diversions. Complexity in the number of variables and systems prevents an easy optimization. In a similar manner to the adjustments to load-cells required for relative humidity and air density, precise determination of the exact optimal parameters will require extensive start-up testing.

When simulations are available, and these parameters are being estimated through models, it becomes much easier to explore the parameter space and determine potential optimal operations. Unfortunately, the size and versatility of bulk processing nuclear facilities and the flexible requirements of detection and false alarm for each subsystem create an exceptionally large number of variables. An example set of variables this analysis: (1) L-norm level, (2) threshold for the student's-t test, (3) threshold for the Chi-Square test, (4) amount of slowing down over transients, (5) time-location of the slowdown, (6) kernel bandwidth for kernel regression, (7) weight per kernel residual, (8) acceptable confidence intervals, (9) number of intervals for the Chi-Square test, (10) number of tests per cumulative sum, and (11) amount of rebaselining per test. It must be assumed that:

1) Each variable contributes in at least a linear fashion,

2) Some variables contribute in nonlinear fashions, and

3) Independence is not expected from any variables.

Because the nonlinear nature of the interaction is unknown, this can be approximated by a series of exponentials or polynomials. For the sake of simplicity, this analysis will use polynomials. In this case, the final effect on the FAR, PND, and MBP are specific expressions of the generalized equation:

$$MBP_{(x_1,x_2,\cdots x_N)} = \sum_{i_1=0}^{\infty}\sum_{i_2=0}^{\infty}\cdots\sum_{i_N=0}^{\infty}\alpha_{i_1 i_2\cdots i_N} x_1^{i_1} x_2^{i_2}\cdots x_N^{i_N} \qquad (43)$$

In equation 43, the each □ is a determined coefficient of the factors, which is given by the various *x*. Determining the coefficients of the factors of the infinite sum is not feasible with modern computational methods as the amount of factors limit to infinity. The nonlinear character of the interaction makes standard regression analysis useless unless enough cases were run to isolate the interaction of each variable.

Previous analysis using Markov Monte-Carlo evaluated the PND and FAR with a running time of roughly an hour per analysis. Each adjustment to each variable required an entirely new run. Under a broad assumption that each variable requires ten settings to explore the entire parameter space, the time required for a complete exploration is 10^N hours.

This can be accelerated by deconstructing the analysis into group families, but this can ultimately only reduce the number of calculations to a loss of two degrees of freedom. While a reduction by two orders of magnitude may seem significant, this analytical method still cannot be pursued. The required time has led to the requirement of seeking secondary methods of evaluating the most relevant factors in the parameter space.

A method developed for exploring extremely large parameter spaces in operations analysis is the 2^k factorial analysis. In this analysis, an arbitrarily high and an arbitrarily low value is assigned for each one of the potential quantitative variables. Note that some variables, such as diversion-type, are qualitative, and so a subset of qualitative variables must be chosen.

This can reduce the number of independent tests to factors of two. There are several assumptions in this model, however:

1) Each variable has only first order interaction with each other variable,

2) Each variable has only first order impact into the final function, and

3) Choice of "high" and "low" values are not the absolute limit and represent "appropriate" values for the quantitative measure.

The third assumption is not difficult to overcome for most of the conditions listed. For example, *p* values for the statistical tests of the Chi-Square and the student's-t test are unlikely to 0.50, and are much more likely to be appropriate in the standard tests of p=0.05 or p=0.01. The first and second assumptions, however, are not appropriate for this model. It is reasonable to expect that a student's-t test on the residuals and a Chi-Square test on the absolute variance are poorly estimated by a “high” and a “low” variable test set. These functions should have multi-order impact, and would not even be linearly independent. As a result, the proposed approach of the 2^k factorial method was not applied.

The envelope suggested is based on process monitoring available in an example facility. No systems are added to detect diversions that the original configuration would not have detected, though some diversions do become harder to execute under envelope operation. Five of these diversions are provided below as examples:

1) A diversion which removes material between the penultimate and final points in a transient is strictly undetectable. The expected value of the last point is explicitly zero, and there is no knowledge of the intervening time. All statistical tests should

provide the same result of no diversion. Slower operations reduce the amount of material that can be removed by half, but only the inclusion of multi-tank analysis and rigorous testing of the systematic error drift of multiple tanks (which could be significant) could prevent this diversion.

2) A diversion which removed material during a statistically rare event, such as abnormally high reading due to systematic error or weather conditions would be similarly undetectable. Consider the far-fetched case of diversion during a tornado or tropical depression. The change in atmospheric pressure would suggest more material is present than actually is, allowing for removal. A second example: a diverter could wait for an event that is reading abnormally high through random occurrence, effectively turning what would have been an anomalously high event (which safeguards staff neither record nor regard) into a normal event. Multitank analysis would be required to attempt detection; the anomalous weather event would be detected as that tank presenting as a statistical outlier, but the high-to-normal event diversion would still not be detected.

3) A diversion which includes a synthetic control system reading through an insider cyberattack would render the entire system irrelevant. Comparison to normal historical cases is used, but there is no test to determine if an event is identical to a prior event. In fact, if the historical curves are known to the operator, as expected, and the operator simulates the facility for efficiency calculations, the tools likely already exist for this type of spoofing. Appropriate Design Information Verification (DIV), resilient control systems, and information security must be added.

4) A diversion which feeds material into a tank at the same rate as removal would be difficult to detect. In the example envelope presented, the density and temperature conditions were not used as part of the process monitoring suite. However, even if they were included, addition of iron dissolved in nitric acid at the appropriate temperature would spoof the system. Without additional process-monitoring variables, the process monitoring system simply cannot detect this advanced diversion.

5) A diversion which occurs during events external to the sensors, or for which there is no historical data set, would also defeat the monitoring system. First start ups, introduction of new additives, or major and uncommon maintenance would rely on (potentially) flawed simulations. This diversion is notable, however, for being external to the operating envelope explicitly, and so it is handled by the methodology.

Additionally, the suggested results assume that only the accountancy tank operation is changed. If fill and flush is very common in the rest of the plant, the effective efficiency increase from the provided envelope would not be as significant. From looking at the surrounding tanks in the head-end process, the fill/flush operation is much less common but the exact operations inside of the rest of the facility are not known.

CHAPTER IV

CONCLUSIONS AND FUTURE WORK

A new framework for safeguards is needed to increase the viability of the closed nuclear fuel cycle. Modern safeguards application is a defense in depth, layering barriers to prevent the loss of material, but with no integration with operations and often acting counter to the facility's efficiency. Significant prior works have developed the advanced tools and methods to include transparency measures such as process monitoring, as part of the safeguards suite, with only limited implementation. This Dissertation suggests a new paradigm to safeguards: operational integration instead of a layering of defense.

Through an example facility, using real recorded data, this work demonstrates the viability of this methodology. The example envelope for the head-end process of the Idaho Chemical Processing Plant showed significant efficiency increases, despite operating some areas of the facility more slowly, with minimal impact to the safety or security of the facility. The presented example was limited in computational power; even more significant increases in efficiency may have been established if the parameter space could have been explored more fully.

This methodology provides an opportunity to fully integrate safeguards into an as-built facility, but there are limitations in application currently. These limitations suggest significant future work: modern techniques previously unavailable to contribute to quantitative safeguards can be included as part of the safeguards suite, the expanse of the optimization variables requires significant research to determine efficient optimization techniques, new data processing and statistical tests may detect diversion more easily, and each facility type may have unique advantages or challenges to applying the methodology.

REFERENCES

1. AREVA. "Nuclear Power: Selective Separation and Recycling." http://www.areva.com/EN/operations-1370/nuclear-waste-recycling-and-treatment.html. (2010).

2. Bathke, C. et al. "The Attractiveness of Materials in Advanced NUclear Fuel Cycles for Various Proliferation and Theft Scenarios." LA-UR-09-02466. (2009).

3. DOE-M-470.4-6. http://www.hss.energy.gov/NMMSS/pdfs/m4704-6c1.pdf. Website accessed Aug (2011).

4. Ehinger, M. "Process Monitoring in International Safeguards for Reprocessing Plans - A Demonstration." ORNL/TM-10912. (1989).

5. Personal Conversation with Michael Ehinger. Contact Oak Ridge National Laboratory. (2009).

6. Wei, T, and J. Reifman. "PRODIAG Combined Expert System/Neural Network for Process Fault Diagnosis." ANL/RE/RP-89482. (1994).

7. Morman, J.A. et al. " IGENPRO Knowledge-based Digital System for Process-transient Diagnostics and Management." IAEA Meeting on Advanced Technologies for Improving Availability and Reliability of Current and Future Water Cooled Nuclear Power Plants. 8-11 September 1997, Argonne National Laboratory, Chicago, IL. (1997).

8. Wei, T. et al. "Signal Trend Identification with Fuzzy Methods." IEEE International Conference on Information, Intelligence, and Systems. Bethesda, MD. (1999).

9. Burr, T., Coulter, A., Howell, J., Wangen, L., "Solution Monitoring: Quantitative and Qualitative Benefits to Safeguards" *J. Nucl. Sci. and Tech.* **40**(4): 256-263, (2003).

10. Burr, T., Hamada, M., “Measurement Error Modelling and Simulation for Solution Monitoring” LAUR08-06399. (2008).

11. Burr, T., Hamada, M., Howell, J., “Multivariate Statistical Process Monitoring Options for Solution Monitoring” LAUR08-06290. (2008).

12. Burr, T., Ehinger, M., Howell, J., “A Review of Process Monitoring for Safeguards” 8th International Conference on Facility Operations - Safeguards Interface, Portland, OR, (2008).

13. Burr, T., Howell, J., Longo, C., Suzuki, M., “Change Detection in Solution Monitoring for Safeguards” Proc. INMM, (2009).

14. Howell J., Scothern, S., “An Explicit Model-Based Diagnostic Approach In A Plutonium Nitrate Tank Storage Facility” *J. Cont. Eng. Prac.*, **8**(6), pp 645-656, ISSN: 0967-0661, (2000).

15. Howell J., Miller, E., “Evaluation of Process Information to Obtain Additional Safeguards Assurances in Reprocessing Plants” UK R&D Programme in Support of IAEA Safeguards. SRDP-R279. (2001).

16. Howell, J., Binner, R. , Bevan, G., Sirajov, B., “Tank Monitoring Evaluation Systems: Methods and Algorithms” Proc. INMM, (2009).

17. Burr, T. and Wangen, L. "Process Fault Detection and Nonlinear Time Series Analysis for Anomaly Detection in Safeguards." LAUR-04-0171. (1994).

18. Ansolabehere, S., et al. “The Future of Nuclear Power” Massachusetts Institute of Technology. ISBN:0-615-12420-8. (2003).

19. Garcia, M.L., *Design and Evaluation of Physical Protection Systems: Second Edition*. Elsevier/Butterworth-Heinemann. Waltham, MA. (2001).

20. Garcia, M.L., *Vulnerability Assessment of Physical Protection Systems*. Elsevier/Butterworth-Heinemann. Waltham, MA. (2006).

21. Cipiti, B.B., Durán, F., Middleton, B., Ward R.,"Fully Integrated Safeguards and Security for Reprocessing Plant Monitoring" SAND2011-7292. (2011).

22. DeMott, D.L. "PRA as a Design Tool" Proceedings - Annual Reliability and Maintainability Symposium. San Jose, CA. (2011).

23. H. Aigner et al, "International Target Values 2000 for Measurement Uncertainties in Safeguarding Nuclear Materials", Intern. Atomic Energy Agency, STR-327. (2001).

24. Personal Email: John Howell. University Glasgow. (2011).

25. Binner, R., Howell, J., Janssens-Maenhout, G., Sellingshegg, D., Zhao, K., "Practical Issues Relating to Tank Volume Determination." *J. Ind. Eng. Chem. Res.*, **27**, 1533-1545. (2008).

26. Howell, J. "Towards the Re-verification of Process Tank Calibrations." *Trans. of the Inst. of Meas. and Cont.*, **31** (2). pp. 117-128. ISSN 0142-3312 (2009).

27. Teknomo, K., "Kernel Regression". Accessed July 2009. http://people.revoledu.com/kardi/tutorial/regression/kernelregression/ (2007).

28. Cipiti, B. B., Duran, F., Merkel, P., Tolk, K., "Data Validation and Security for Reprocessing" SAND20008-6458. (2008).

APPENDIX 1

DATA RECOVERY

A significant portion of this appendix is from Summary of Data Recovery Efforts to Date Available in the DOE Complex, INL-EXT-09-17374.

Data Retrieval

The data retrieval effort took on three parts: raw data, metadata, and open search. Raw process monitoring data files were transferred from magnetic tapes to an optical drive, where they were copied to a single database. Once that database was restored, the data were copied to flat files and entered into a new database.

Metadata, containing computed and applied ICPP process monitoring information, were in storage at the Idaho Nuclear Technology and Engineering Center (INTEC), formerly known as the ICPP. Of these data, only campaigns 38 and 40 were obtained, which consisted of approximately 2000 pages of information. These hard copy files were then scanned and stored in .PDF format, organized by campaign, month, and batch.

An open search conducted primarily through INL's Electronic Document Management System (EDMS) has produced details of plant operation, the process monitoring system and other manuals.

Description of the ICPP Facility

Completed in 1953, the ICPP was designed by Oak Ridge National Laboratory (ORNL) personnel to process several types of fuel: aluminum clad fuel from the Material Test Reactor, unclad Experimental Breeder Reactor I (EBR-I) fuel, and Hanford producing fuel. The amount and type of fuels processed at the ICPP expanded throughout its operational history. During forty years of operation, the facility reprocessed fuel from nearly 100 tests and research facilities around the world and ultimately recovered approximately 32 metric tons of uranium.

The ICPP was equipped with several head-end dissolution processes capable of dissolving the aluminum-, zirconium-, stainless steel-, and custom-clad fuels. The main extraction process separated uranium through a tributyl phosphate (TBP) extraction cycle followed by two methyl isobutyl ketone (MIBK) extraction cycles. The resulting uranyl nitrate entered a denitrator and was almost instantaneously converted to uranium trioxide. This solid product was then put into cans, measured for accountability, and shipped to the customer.

Operational Capacity

The processing complex consisted of five interconnected facilities: CPP-601, CPP-627, CPP-640, CPP-602 and CPP-630. The first three were dissolution and extraction facilities while the last two were denitration and support facilities. The extraction cycles were housed within 29 cells in CPP-601. These cells were assigned letters of the alphabet and had different capabilities. G Cell contained the aluminum dissolution process and initial accountability tanks. The TBP extraction took place in G and H Cells and the MIBK extractions were in P and Q Cells. Other cells like M and N were for intercycle sampling and storage. A process makeup area above the operating cells housed the acid and water makeup tanks.

Instruments, tanks, and pipes were named with the cell letter and a corresponding number depending on the type of equipment. For example, G-105 was a tank in G Cell and F-55 is a valve in F Cell. For further explanation of instrument nomenclature, see Appendix 1. The equipment within the cells was controlled within the operating corridor; a long hallway in the center of the building separated the two sets of operating cells.

Before processing, expended fuel was stored on site in four storage facilities. These irradiated and unirradiated fuels included uranium metal; uranium metal clad in aluminum, zirconium, stainless steel or other special metals; uranium alloyed with those metals; uranium oxide; and other uranium ceramics. The unirradiated fuels were stored in an aboveground building or buried-in-earth, caisson-type containers. Irradiated fuels were most often stored in water basins between 20 and 44 ft deep or within shielded air-cooled rooms encased in buried-in-earth, caisson-type containers. They were required to have at least 90 days of cooling before entering the dissolution process although the cooling period would often be for much longer than this in order to collect enough of the same type of fuel to run a specific dissolution process.

After the required cooling period was complete, the fuel was transferred from storage into a charging cell and subsequently entered the head-end dissolution process appropriate for its makeup. Aluminum fuels were dissolved in nitric acid with a mercuric sulfate as a catalyst. Zirconium fuels were dissolved in hydrofluoric acid and nitric acid with an electric current running through the solution. Stainless steel fuels were dissolved in nitric acid with an electric current running through the solution. Graphite fuels were burned in oxygen, and the leftover metals were also dissolved in hydrofluoric and nitric acids. The custom processing facility dissolved small quantities of uniquely clad fuels. After the dissolution was complete, any deficiencies that were found in the uranium solution were corrected, and it was sampled for uranium content in accountability tanks. Once all of the chemical analyses were completed and approved, the solution was sent to the first cycle extraction process.

The uranium was removed by aqueous-organic extraction. These chemical separations occurred in countercurrent pulse-plate or packed columns. Following the first cycle, the uranyl nitrate solution was sent to M Cell for intercycle accountability and then to N Cell for intercycle storage. The second and third cycle extractions were run to extract as much uranium as possible. After the three cycles were complete and the uranyl nitrate was sufficiently pure, it was again sent to M Cell for accountability and then to Z Cell where it was stored. The uranyl nitrate then entered the fluidized-bed denitrator, where it was converted to uranium oxide.

Radioactive waste from the uranium dissolution and extraction was also treated at the ICPP. The high level radioactive waste that was removed during the first extraction cycle and was stored indefinitely as a calcined solid similar to sand. The low-level radioactive waste produced from the second and third cycles were stored in one of three 300,000 gallon tanks.

Operational History

From the beginning, the ICPP was a dynamic facility where new technologies were implemented on a frequent basis. The first campaign at the ICPP began in February of 1953. The first seven fuel campaigns used methyl isobutyl ketone (MIBK) in all three extraction cycles. In 1955, the first extraction cycle changed from MIBK to tributyl phosphate (TBP) extraction. This upgrade was beneficial because it did not require the first-cycle dissolver product to be preconcentrated. TBP extraction also allowed the plant to operate on a more continuous basis because the first cycle could operate at the same time as the fuel dissolution. The treatment of high-level waste was altered in 1964 when the Waste Calcination Facility (CPP-633) began to calcinate liquid waste into granular solids. A year later, the ICPP integrated a custom fuel processing facility where less conventional fuels could be dissolved.

Up until 1971, the final-product uranyl nitrate was stored in 10 liter polyethylene bottles. At this time, the denitrator process was developed in CPP-602 to convert the liquid uranyl nitrate into solid uranium trioxide, increasing the total amount of final product able to be stored in a given volume. About 85% of the entire uranium product was shipped to Y-12 in Oak Ridge, Tennessee. Most of the remaining 15% was shipped to Portsmouth Gaseous Diffusion Plant in Ohio. Small amounts of fuel were sent to other national laboratories for research purposes. These shipments continued from 1953 to 1998.

In 1973 the electrolytic dissolution process was installed into CPP-640, allowing for the dissolution of the stainless steel fuel from Experimental Breeder Reactor II (EBR-II). In 1981, the ICPP was equipped with the Process Monitoring Computer System (PMCS), the main purpose of which was to provide high quality processing information to operations, safeguards, and support staffs. 1983 saw the development of the ROVER (Nuclear Rocket) fuel recovery. Three years later, in 1986, zirconium-alloyed fuel dissolution was added allowing for the processing of navy fuels.

The plant was temporarily shut down in 1988 to update the underground piping in compliance with Environmental Protection Agency regulations. This was a significant undertaking for the facility. No major uranium extractions were performed after this time because the Secretary of Energy stopped all spent nuclear fuel processing in the United States in 1992. The uranium solution left in the plant in 1992 was finally processed in 1996 and shipped in 1998.

In October of 1994 the Idaho National Engineering Laboratory released its plan for decommissioning the ICPP, identifying which facilities would be destroyed or have their efforts redirected. Due to all of the recent changes, the ICPP has been renamed Idaho Nuclear Technology and Engineering Center (INTEC).

Process Monitoring System

In order to decrease inadvertent transfers and operator error, and to test the utility of process monitoring for safeguards, the ICPP was retrofitted with monitoring instruments and a computer system. Information such as pressure, flow rate, and on/off status of valves and samplers was recorded. The instrumentation was updated as new technologies were developed throughout the next decade. By the end of the 1980’s, this retrofit was capable of monitoring 1500 variables from 125 different process vessels throughout the extraction process. A description of the PMCS and its accompanying instrumentation is discussed below.

The PMCS was a set of programs used to store, analyze and graph process information and was installed on multiple VAX 11/780 and MicroVAX II computers within buildings CPP-601 and CPP-602. Three hundred and ninety-five analog signals were gathered by scanivalve controllers and 4 analog multiplexers. Four Digital Controllers gathered 484 on/off signals for pumps, jets, airlifts and samplers. All of this information was scanned once per minute and stored in an on-line database for one year, which was made available to operating, security, and safeguards staff. After one year, data from every fourth minute were permanently stored on magnetic tapes. Further information concerning forms and procedures used can be fount in “The Users Guide to the PMCS Revision 3” .

Instrumentation

Scanivalves are pneumatic devices that convert analog signals, such as pressure, into digital signals usable by the PMCS. Three 64-bit scanivalves were installed in the ICPP in 1982. With an accuracy of 1%, the scanivalves were the best technology of the time. However, they often encountered electrical noise problems and occasionally reported false short-duration changes in their readings. Because of the nature of the nuclear material, the scanivalves had to be operated remotely. This was accomplished by using AMDUX-12 Recording Devices which also did on line pressure correction computations.

The Precision Level/Density Scanners (PLDS) recorded accurate measurements of the solution densities and tank levels throughout the process. There were four PLDS installed outside of E, G, J, and N Cells, and one inside of Z Cell. Through scanivalves, the pneumatic pressures were multiplexed into two Digiquartz high-precision differential-pressure transducers. For a given tank, three dip tubes measured pressure at various points within the tank. (R) measured the reference pressure, (D) measured the pressure at a given depth within the tank, and (L) measured the pressure at a specific height above the bottom of the tank, as is demonstrated in the figure below. These Digiquartz transducers output electrical signals representing pressure differences (LR and DR) and temperature that were later interpreted by a computer.

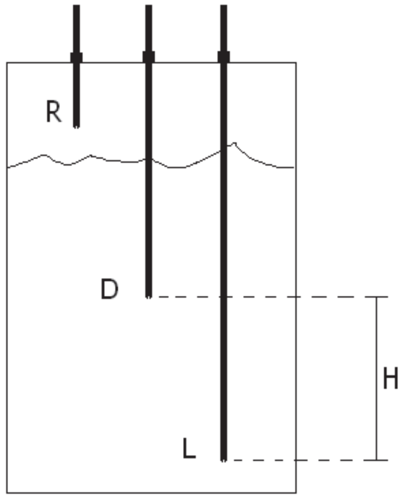


Figure 21. Crude diagram of the dip tube set-up within a tank.

The Liquid-in-Line sensors detected the presence of a fluid in air or instrument lines. They were placed in areas that would only have liquid in emergencies, mechanical failures, or diversion attempts. Three different types of sensors were tested between 1980 and 1981. The ultrasonic sensor could detect the presence of liquid in pipes smaller than 1/2 in. thick. The thermal sensor checked for temperature changes that would occur as liquid flowed through the pipe. Finally, the vacuum sensor was an invasive way of testing whether or not solution was siphoned out. The ultrasonic and thermal sensors were non-intrusive, whereas the vacuum sensor was, by nature, intrusive.

Pressure switches monitored steam jets, sample air jets, and remote-controlled valves. These were prone to provide false indications, however, when the control valves were leaking.

Process Liquid Flow Monitors were used to track fluid moving throughout the process. They were non-intrusive and detected temperature changes by moving fluid through a heated insulated section of pipe. Air-flow monitors were used for observing air sparge mixing, sampler air lifts and process air lifts where the flow rate exceeded 1.5 ft^3 per minute. However, nothing suitable was found for monitoring sample air lifts because the flow rates were too low.

Available Data Description

Raw Data

The raw data were obtained from magnetic tapes containing over six gigabytes of information. These span from October of 1986 through April 1996. Over this 10-year period, data were recorded from many tanks, centrifuges, evaporators, valves, jets and air lifts. Some of these data simply consisted of either a 1 or a 0, indicating whether a piece of equipment was activated or not. Only the centrifuges had speed indicators, and dissolvers only contained information for off-gas control signals or charge soot hydraulics.

The most valuable process monitoring data are associated with the accountability tanks, feed tanks, and sample pots, which consist of raw measured data obtained from Digiquartz transducers. These transducers measure pressure and temperature differences in the tanks or pots. These LR and DR pressure differences are used to calculate density/specific gravity, volume, and level of material in the tank.

Density is calculated by taking the difference between LR and DR and dividing that by the product of the acceleration due to gravity (g) and a known height (H) between dip tube D and dip tube L shown Equation A1. Volume and level are calculated with added constants and coefficients not described in detail here.

$$\rho = \frac{LR - DR}{gH} \tag{A1}$$

The raw data are currently accessible in either Microsoft Excel or text format. The pressure measurement error associated with the dip tubes is extremely small. With no noise, level calculations from pressure measurements reach less than 0.015%.

Metadata

The collected metadata were from campaigns 38 and 40 which covered September 1982 through January 1983 and September 1985 through January 1986, respectively. Included in these data are isotope concentrations, isotope ratios, chemical make-up of the fuel being reprocessed, shipper/receiver differences, campaign summaries, and product-can outputs. The metadata are currently organized in PDF format by campaign, month and batch number.

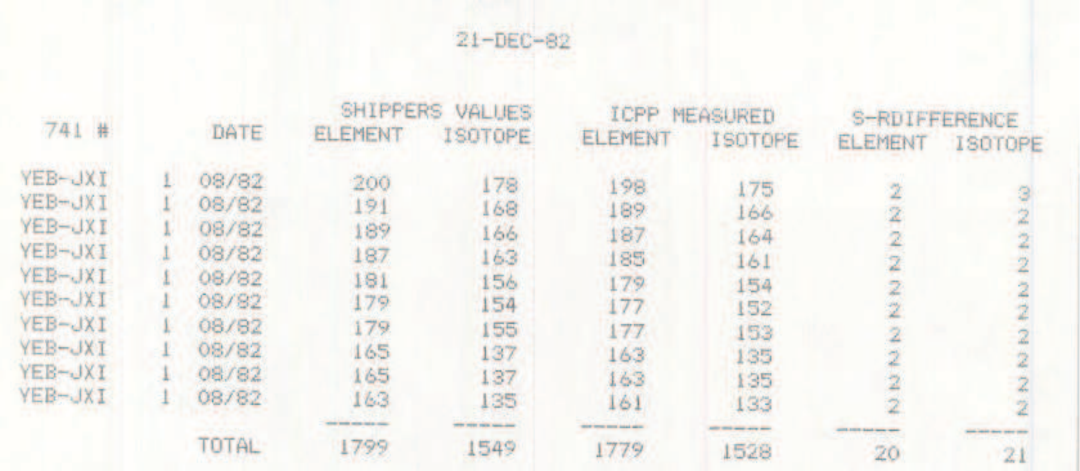
Several different types of forms have been recovered. Many of the measurements in the metadata are in milligrams per gram of uranium or grams per liter of solution. However, meanings of some of the acronyms and units are unknown. An attempt to describe the basic use of the forms and other necessary clarifications will be presented. The goal is to provide the interested researcher with enough information to deduce the meanings of those things that are not explained.

Form 751 recorded who shipped the spent nuclear fuel, who received it, and when it was received by the ICPP. In order for the ICPP to receive spent nuclear fuel, the shipper was required to account for the amount U^{235} and U^{238} the fuel. Since this is a very difficult measurement to make, the best accuracy achievable was about 20%. These values declared by the shipper were recorded on the 741 and were legal until the product was dissolved and accounted for in the plant. Once the accounting analysis was completed, these values became the official value for the amounts of uranium present in the fuel assemblies.

Copies of this form are not included in the Data Package due to legalities. However, the Transfer to Process forms included are summaries of the 741's.

Shipper/Receiver Differences

Several different versions of this form exist in the data package, but all follow a similar format. This form verified that what the shipper sent to the ICPP was received. Usually the type of fuel and the date that it was received were recorded in the first two columns, followed by the amounts of U^{238} and U^{235} claimed by the shipper and what was measured by the ICPP. The first column of values (ELEMENT) is the amount of U^{238} in grams and ISOTOPE, the second column of values is the amount of U^{235} in grams (see figure 22). The final columns were the differences between the declared amounts and the measured amounts. They are generally within a few grams of each other. Some of the forms list the difference measurements by fuel element, by batches or by fuel type (see Figure 22).



21-DEC-82

			SHIPPERS VALUES		ICPP MEASURED		S-RDIFFERENCE	
741 #		DATE	ELEMENT	ISOTOPE	ELEMENT	ISOTOPE	ELEMENT	ISOTOPE
YEB-JXI	1	08/82	200	178	198	175	2	3
YEB-JXI	1	08/82	191	168	189	166	2	2
YEB-JXI	1	08/82	189	166	187	164	2	2
YEB-JXI	1	08/82	187	163	185	161	2	2
YEB-JXI	1	08/82	181	156	179	154	2	2
YEB-JXI	1	08/82	179	154	177	152	2	2
YEB-JXI	1	08/82	179	155	177	153	2	2
YEB-JXI	1	08/82	165	137	163	135	2	2
YEB-JXI	1	08/82	165	137	163	135	2	2
YEB-JXI	1	08/82	163	135	161	133	2	2
			------	------	------	------	------	------
		TOTAL	1799	1549	1779	1528	20	21

Figure 22. Example of a sender/receiver form in grams of U^{235}.

First Cycle Extraction (FCE) and 1-FU-AL Forms

These were the forms that accounted for the amount and nature of material that entered the process. They specifically accounted for each batch of aluminum clad material before it entered the first cycle extraction. The left-most digit in the batch number distinguished which route the fuel would take in the dissolution process. For example, during campaign 38 a batch number of 1009 meant that batch 9 of material dissolved in G-101 and was accounted for in tank E-103. A batch number of 2010 meant that batch 10 of material dissolved in G-151 and was accounted for in tank E-153. For campaign 40, a batch number of 1126 meant that batch 126 started in dissolver G-101 and was sampled in tank G-105. A batch number of 2127 meant that batch 127 went from G-151 to G-155 to be sampled.

Included on these forms are various chemical-analysis results. Using three independent samples of solution, they record the uranium concentration, specific gravities, undissolved-solid concentration, and nitric-acid content. If the results of two samples were within specifications and met the accountability requirements, then the process continued. If the first two disagreed then the third sample was analyzed. If the third sample agreed with one of the other two then the process continued. However, if they could not obtain a satisfactory sample measurement they would stop the process and research the problem. The results of these forms are summarized in the RUSCA/RUSKA Measurement Data forms.

As part of the final batch report, maximum flow rates, upper and lower limits and atom percentages were calculated. Some of the batch reports have gamma analyses which were required to verify the properties of the material.

Document Change Requests

Document Change Requests stated why the operators deviated from the original run plan. Such reasons range from decreasing isotope concentration to correcting a dissolution error. They can be found in the processing run summaries.

Product Denitrator System (PDS) Reports

After the uranium completed the three extraction cycles, it was stored as uranyl nitrate in the Z-Cell tanks. When a sufficient amount of uranyl nitrate was collected, the denitrator was run to convert the uranyl nitrate to uranium trioxide (UO_3) in a heated fluidized bed. The UO_3 was stored in cans in a vault until it was shipped to Y-12 or other facilities. Every can was measured for its uranium content and radioactive activity. Additionally, the cans' net and gross weights were also recorded. All of this information is found in the product can reports for runs 38 and 40.

For accountability purposes, the data collected from the denitrator are not particularly helpful, because the denitrator was only run once every one or two years. It is very difficult to assign a specific product can to a specific batch since the uranyl nitrates from different runs were intermixed. In an attempt to resolve this issue, Ernest Laible of the Idaho National Laboratory determined which cans are most likely related to which types of fuel based on the cans' uranium enrichment content. His work is summarized in Table 3. The 741 identifiers are used in the fuel type column: 623-643 has 78% enrichment; some 78% some 91%.

Table 3. The product cans are associated with their respective fuel types.

Fuel Type	Date	Run Number	Inclusive Can Numbers	# of Cans	Enrichment
JXI-FZB	3/21/1983	5	226-277	21	85.24
JXI-FZB	7/9/1983	6	233-278	30	84.26
JXI-FZB	1/9/1984	7	285-295	10	87.25
JXI-FZF	9/4/1986	10	573-622	50	82.3
JXI-FZF	9/4/1986	11	623-690	50	86.22*
JXI-FZF	9/24/1986	12	644-658	12	82.17

Batch Processing Schedules

The Batch Processing Schedules for campaign 40 are very similar to the sender\receiver difference reports. These also include the uranium enrichment of the fuel as it was built. It is interesting to note that the batch numbers on the batch processing schedules do not match up with the batch numbers of the actual extraction process.

PMCS Photographs

Fifty-six photographs were taken in 1984 of the PMCS instrumentation in CPP-601. They show the pressure, temperature, and density analog recorders, valves, hallways, switches, and pipes that were used during this time period. Photographs can be associated with individual cells and processes. See Figure 23.

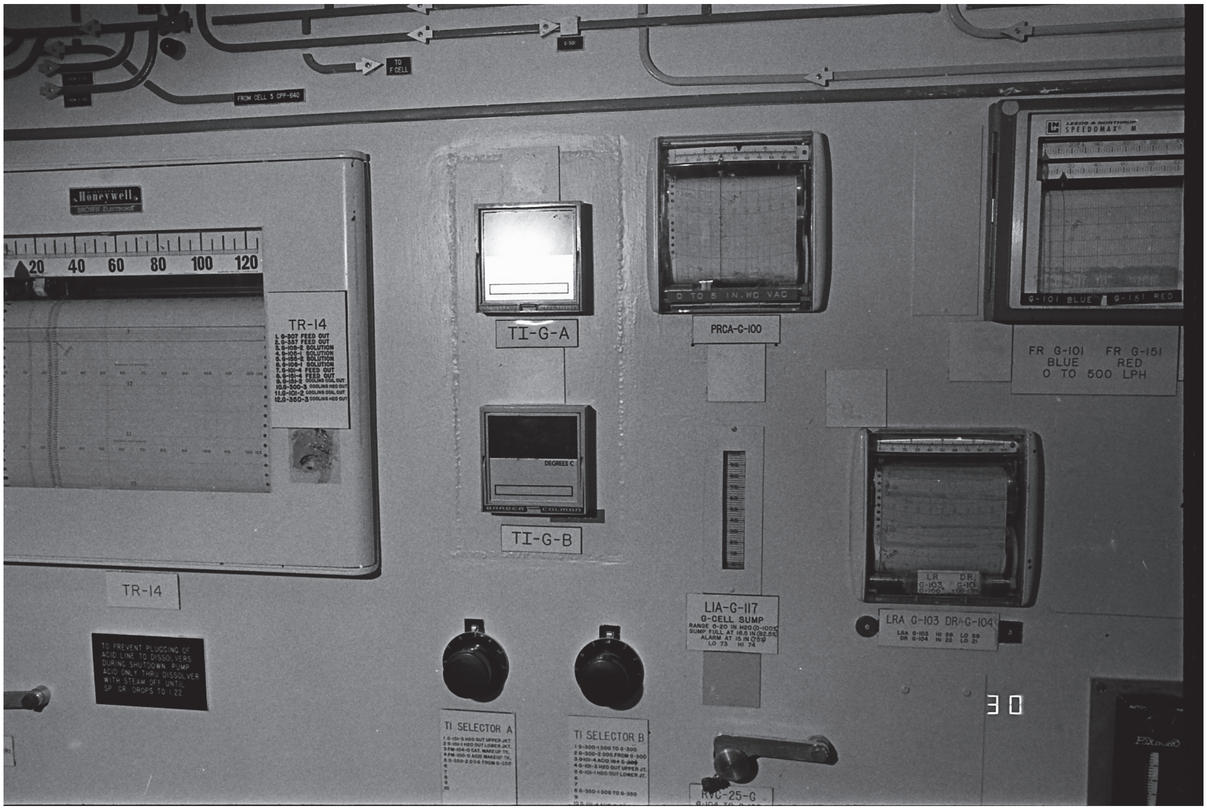


Figure 23. 1984 photograph of the PMCS equipment.

Operational Reports

A Hexone Extraction System Flush, a Flush and Sample of G-116, and a G-Cell Vessel Flush were recovered with the help of Phil Winston. These three operational reports explain clean-out operations which occurred in 1993 and 1994. They give detailed process information, such as how the fluid moved throughout the process, what valves were to be opened and in what sequence. This information can be used with the raw computer data to verify that the material was in the correct place at the correct time. Unfortunately, there is little information describing what type of material was in the tanks at that time.

Strip Charts

Strip charts recorded analog readings of many tanks, valves and other operating vessels. Charts relating to campaigns 38 and 40 are available in hard copy at the INL's record storage facility. A discussion of the difficulty of working with these charts is presented below under expected challenges.

Process Manuals

Several manuals and reports describing the ICPP and its operations in detail have also been found, which, although they will not be fully included in the data package, are useful in describing key areas of interest within the plant. Among these include the Precision Level/Density Scanner report, several annual reports and fuel campaign reviews, a Failure Rate Database, the Users Guide to the PMCS and manuals for plant operators.

Other Data

More data are available to be collected at a later time, such as 1986 Fuel Reprocessing Data Sheets, Fuel Process Logs, R.C. Maurer's 1982 log book, INTEC Analytical Lab logbooks, Batch Transfer Records and other miscellaneous run plans.

Operator Use

The most important use of the PMCS data was interactive analysis of process information. Safeguards, operating, and support staffs had access to this retrievable information in the form of tables, graphs, calculations and pre-printed forms. Digital process data were significant improvements over the analog strip charts previously used to do statistical testing and process monitoring.

From an operating standpoint, the PMCS helped to reduce the number of inadvertent transfers in the ICPP. The system would calculate the amount of headroom available in the next vessel in the process in order to ensure that there was enough room for the additional fluid. It would also calculate target values that would inform the operator when the transfer from one vessel to another was completed. Transfer routes were checked to ensure that there were no conflicts in the process, such as a closed valve when it should be open. To flag conflicting requirements in plant operation, a conflict report was printed describing the problem and possible correctional procedures. Operators also printed pre and post-transfer forms to ensure that the material was sent and received correctly. Of the 12,000 transfers that occurred in the plant up to 1989, there were only three inadvertent transfers of material. Of these three, none of them were attributable to a failure by the PMCS. All three were a result of equipment or other failures in the facility. This fact is a strong proponent of how a similar process monitoring system can both help with nuclear safeguards and facility efficiency.

The ICPP Safeguards staff had 5 main material balance areas in the ICPP called Sub-Material Balance Areas (Sub-MBAs): Dissolution Headends, First Cycle Extraction, Second and Third Cycle Extraction, Product Denitration and Salvage/Low-Level Waste. Using a special subset of PMCS data, Safeguards personnel could monitor the movement of solution into and out of each Sub-MBA, movement of solution within a Sub-MBA, or any mixing or sampling that would occur in the Sub-MBA. They were responsible for ensuring operating procedures were being followed. Forms provided on a daily basis reported process events, instruments that lost connection with the computer and summaries of the status of the data acquisition devices.

Data Congruity Issues

The current metadata cover campaigns 38 and 40, which spans September 1982 through January 1983 and September 1985 through January 1986 respectively. Any metadata after January 1986 are currently unattainable. The raw digital data on the other hand, cover October 1986 through April 1996. Because of the infeasibility of storing that amount of information in the early 1980's, computerized data do not exist before October 1986. Therefore, the only available PMCS data before October of 1986 are in strip chart form.

The information that these strip charts contain is undeniably valuable; however, converting them from lines on charts to digital information would require an accurate strip chart reader. Once digital readouts were obtained, still more problems ensue. There seems to be a different nomenclature on these strip charts than the raw data. So, not only would the strip charts require deciphering the nomenclature, but also deciphering units of measurement and time intervals between measurements. These charts have little to no labels describing these aspects. Possibly the most deterring factor is the observation that the lines on these charts are thick enough that when digitized, the data will have a much larger margin of error than the raw data already in digital format.

VITA

Name: Richard Royce Metcalf

Education: B.S., Nuclear Engineering, Texas A&M University, 2007
M.S., Nuclear Engineering, Texas A&M University, 2009
Ph.D., Nuclear Engineering, Texas A&M University, 2011

Address: Department of Nuclear Engineering
c/o Dr. Pavel Tsvetkov
Texas A&M University
College Station, TX 77843-3133