RELIABILITY ENGINEERING APPROACH TO PROBABILISTIC PROLIFERATION RESISTANCE ANALYSIS OF THE EXAMPLE SODIUM FAST REACTOR FUEL CYCLE FACILITY

A Thesis

by

LILLIAN MARIE CRONHOLM

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

MASTER OF SCIENCE

August 2011

Major Subject: Health Physics

RELIABILITY ENGINEERING APPROACH TO PROBABILISTIC PROLIFERATION RESISTANCE ANALYSIS OF THE EXAMPLE SODIUM FAST REACTOR FUEL CYCLE FACILITY

A Thesis

by

LILLIAN MARIE CRONHOLM

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

MASTER OF SCIENCE

Approved by:

Chair of Committee,	John W. Poston
Committee Members,	John R. Ford
	William S. Charlton
	Sergiy Butenko
Head of Department,	Raymond J. Juzaitis

August 2011

Major Subject: Health Physics

ABSTRACT

Reliability Engineering Approach to Probabilistic Proliferation Resistance Analysis of the Example Sodium Fast Reactor Fuel Cycle Facility. (August 2011)

Lillian Marie Cronholm, B.S., Texas A&M University

Chair of Advisory Committee: Dr. John Poston

International Atomic Energy Agency (IAEA) safeguards are one method of proliferation resistance which is applied at most nuclear facilities worldwide. IAEA safeguards act to prevent the diversion of nuclear materials from a facility through the deterrence of detection. However, even with IAEA safeguards present at a facility, the country where the facility is located may still attempt to proliferate nuclear material by exploiting weaknesses in the safeguards system. The IAEA's mission is to detect the diversion of nuclear materials as soon as possible and ideally before it can be weaponized. Modern IAEA safeguards utilize unattended monitoring systems (UMS) to perform nuclear material accountancy and maintain the continuity of knowledge with regards to the position of nuclear material at a facility. This research focuses on evaluating the reliability of unattended monitoring systems and integrating the probabilistic failure of these systems into the comprehensive probabilistic proliferation resistance model of a facility.

To accomplish this, this research applies reliability engineering analysis methods to probabilistic proliferation resistance modeling. This approach is demonstrated through the analysis of a safeguards design for the Example Sodium Fast Reactor Fuel Cycle Facility (ESFR FCF).

The ESFR FCF UMS were analyzed to demonstrate the analysis and design processes that an analyst or designer would go through when evaluating/designing the proliferation resistance component of a safeguards system. When comparing the mean time to failure (MTTF) for the system without redundancies versus one with redundancies, it is apparent that redundancies are necessary to achieve a design without routine failures.

A reliability engineering approach to probabilistic safeguards system analysis and design can be used to reach meaningful conclusions regarding the proliferation resistance of a UMS. The methods developed in this research provide analysts and designers alike a process to follow to evaluate the reliability of a UMS.

DEDICATION

To my family:

Rita Cronholm, Greg Cronholm, and Catherine Cronholm

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. John Poston for his support, insight and guidance. I would also like to thank my committee members, Dr. Ford, Dr. Charlton, and Dr. Butenko, for their support during the course of this research.

I am very grateful to Mike Zentner and Garill Coles at Pacific Northwest National Laboratory for their mentorship and introducing me to proliferation resistance assessment.

Many thanks go to T. Pochet, E. Smith, and M. Frankl for their time and expertise.

I would also like to express thanks to Adam Shephard for his unwavering support, friendship and assistance through this process.

Additional thanks go to Kim Ania Kaminski, Adam Hetzler, John Creasy, and Tomasz Styblinski for their editorial assistance and continuous support.

NOMENCLATURE

AD	Assembly Disassembly
AF	Assembly Fabrication
AFCI	Advanced Fuel Cycle Initiative
AMS	Attended Monitoring System
BU	Burnup
CDF	Cumulative Distribution Function
Cm-Pu	Curium-Plutonium
CoK	Continuity of Knowledge
C/S	Containment and Surveillance
CW	Ceramic Waste Processing
DAQ	Data Acquisition
DIV	Design Information Verification
EC	Element Chopper
ER	Electro-Refiner
ESFR	Example Sodium Fast Reactor
FCF	Fuel Cycle Facility
FP	Fission Product
GenIV	Generation IV
He3	^{3}He or Helium-3
HEU	Highly Enriched Uranium
HM	Heavy Metal
IAEA	International Atomic Energy Agency
IC	Product Prep Injection Caster Furnace
IS&NP	International Safeguards and Nonproliferation
KMP	Key Measurement Point
MBA	Material Balance Area
MCNP	Monte Carlo n-Particle

MTBF	Mean Time between Failures
MTTD	Mean Time to Detection
MTTF	Mean Time to Failure ($1/\lambda$)
MTTR	Mean Time to Repair
MW	Metal Waste Processing
NMA	Nuclear Material Accountancy
NPT	Nuclear Non-Proliferation Treaty
OP	Oxidant Production
PBMR	Pebble Bed Modular Reactor
PDF	Probability Distribution Function
PIV	Physical Inventory Verification
PP	Pin Fabrication/Pin Processing
PR	Proliferation Resistance
PR&PP	Proliferation Resistance & Physical Protection
PUREX	Plutonium and Uranium Recovery by Extraction
PWR	Pressurized Water Reactor
RM	Remote Monitor
RMS	Remote Monitoring System
SQ	Significant Quantity
TP	U/TRU Product Processing
TR	U/TRU Extraction/Recovery
TRU	Transuranic
UMS	Unattended Monitoring System
UP	Uranium Product Processing
WS	Waste Form Temporary Storage

TABLE OF CONTENTS

Page

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER I
INTRODUCTION

Probabilistic analysis of the proliferation resistance of nuclear energy systems and facilities is an active area of research in the field of international safeguards and non-proliferation. Methodologies and tools that support both the qualitative and/or quantitative analysis are continually being developed and improved. At present, no single approach, model, or method has emerged as a standard for either general or specific systems or facilities.

Previous studies on the topic of probabilistic approaches to proliferation resistance focus on the identification, analysis, and mitigation of proliferation pathways by the assignment of probabilities to each proliferation pathway. This research develops a method to model the proliferation pathway segment associated with the hardware failure of the International Atomic Energy Agency's (IAEA) unattended monitoring systems (UMS). This method applies probabilistic reliability engineering modeling to IAEA UMS installed at a facility and relates the probability of individual component failures to the probability of a system failure. A UMS failure would represent an opportunity for proliferation.

In general, probabilistic approaches to analyze diversion or misuse pathways are very difficult to analyze because they rely on the assignment of probabilities to the series of events that must happen to divert material from a nuclear facility or misuse of a nuclear facility. With no past data on successful covert or clandestine attempts at nuclear material diversion (because we would not know of the attempt if it was successful) and very little data on unsuccessful attempts, the probabilities would have to be estimated

---

This thesis follows the style of Health Physics.

based on best available information and/or expert judgment. The objective of this research is to offer a reliability engineering approach for incorporation into overall probabilistic proliferation resistance modeling. Reliability engineering is the area of study concerned with a system or component to perform satisfactorily over a given period of time.

International Atomic Energy Agency (IAEA) Safeguards is one method of proliferation resistance, which is applied at most nuclear facilities worldwide. IAEA safeguards act to prevent the diversion of nuclear materials from a facility through the deterrence of detection. However, even with IAEA Safeguards present at a facility, the country where the facility is located may still attempt to proliferate nuclear material by exploiting weaknesses in the safeguards system. The IAEA's mission is to detect the diversion of nuclear materials as soon as possible and ideally before it can be weaponized. Modern IAEA safeguards utilize unattended monitoring systems (UMS) to perform nuclear material accountancy and maintain the continuity of knowledge with regards to the position of nuclear material at a facility. This research focuses on evaluating the reliability of unattended monitoring systems and integrating the probabilistic failure of these systems into the comprehensive probabilistic proliferation resistance model of a facility.

To accomplish this, the research applies reliability engineering analysis methods to probabilistic proliferation resistance modeling. This approach is demonstrated through the analysis of a safeguards design for the Example Sodium Fast Reactor Fuel Cycle Facility (ESFR FCF). The analysis demonstrates the probability of safeguards system failure which would result in the loss of the continuity of knowledge of nuclear material at this facility. This failure probability of the UMS is then integrated into an overall proliferation resistance model of the facility. A detailed proliferation resistance model of the ESFR FCF is outside the scope of this research.

A UMS design for the ESFR FCF is presented in this research to facilitate demonstration of the reliability analysis process; the design itself is not emphasized. This UMS design for the ESFR FCF is in contrast to other designs which are proposed in the literature. Many of the safeguard designs proposed assume infinite financial resources, manpower, legal authorities, and futuristic technologies not currently available or in use by the IAEA. This research presents a UMS design for the ESFR FCF using currently available technology and a reasonable number of systems to safeguard the facility.

1.1 SCOPE OF WORK

This research applies quality engineering concepts to safeguards system analysis and design. A process is developed to calculate the probability of safeguards system failure from a probabilistic model of a network of unattended monitoring systems. This process is then applied to the design of a safeguards system for the ESFR FCF.

In Chapter II, the reader is introduced to IAEA Safeguards with an emphasis on the role of Unattended Monitoring Systems and the ESFR facility. In Chapter III, a general process for the analysis and/or design of the reliability of a safeguards system is developed. In Chapter IV, this process is applied to the ESFR FCF. In Chapter V, the reliability process how it relates to proliferation resistance analysis is discussed.

The beneficiaries of this research are the IAEA, international safeguards and non-proliferation (IS&NP) community and the proliferation resistance and physical protection (PR&PP) community. This research demonstrates a process that the IAEA and the IS&NP community can use to analyze existing safeguards systems and design future safeguards systems. Researchers in the area of PR&PP will be able to utilize the probabilistic modeling developed and apply it in a broader sense to more facilities and integrate it into broader probabilistic proliferation resistance methods and models.

CHAPTER II
BACKGROUND AND LITERATURE REVIEW

This chapter discusses modern approaches to IS&NP with references to governing documents and IAEA safeguards. This is followed by a literature review which includes previous work in proliferation resistance approaches. Finally, the IS&NP and PR&PP literature specific to the ESFR is discussed.

2.1 IAEA INTERNATIONAL SAFEGUARDS

The International Atomic Energy Agency (IAEA) is the intergovernmental body which administers international safeguards in accordance with the Non-Proliferation Treaty (NPT). The IAEA is an independent United Nations (UN) Organization; it draws independent conclusions and reports these conclusions to the UN Security Council. Every country in the world with the exception of Israel, Pakistan, India and North Korea participates in the NPT.

2.1.1 OBJECTIVES

The objective of IAEA Safeguards is defined to be, "the timely detection of diversion of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons or of other nuclear explosive devices or for purposes unknown, and deterrence of such diversion by the risk of early detection." (International Atomic Energy Agency 1972)

The timeliness criteria is defined to be, “where there is no additional protocol in force or where the IAEA has not drawn and maintained a conclusion of the absence of undeclared nuclear material and activities in a State, the timeliness detection goals are as follows:

- One month for unirradiated direct use material,
- Three months for irradiated direct use material,
- One year for indirect use material.

Longer timeliness detection goals may be applied in a State where the IAEA has drawn and maintained a conclusion of the absence of undeclared nuclear material and activities in that State” (International Atomic Energy Agency 2001).

A significant quantity is defined to be, “the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded. Significant quantities take into account unavoidable losses due to conversion and manufacturing processes and should not be confused with critical masses. Significant quantities are used in establishing the quantity component of the IAEA inspection goal” (International Atomic Energy Agency 2001). Significant quantity values currently in use are given in Table 1.

Table 1. Significant quantities

Material	**Significant Quantity (SQ)**
Direct use nuclear material	
Pu[a]	8 kg
^{233}U	8 kg
HEU ($^{235}U \geq 20\%$)	25 kg
Indirect use nuclear material	
U ($^{235}U < 20\%$)[b]	75 kg ^{235}U (or 10 ton natural U or 20 ton depleted U)
Th	20 tons

[a] For Pu containing less than 80% ^{238}Pu.
[b] Including low enriched, natural and depleted uranium.

2.1.2 APPROACHES

As part of the treaty verification regime, the IAEA must determine that the facility has not been altered for the purpose of misuse and nuclear material has not been diverted. The design information verification (DIV) is performed for each facility as necessary to verify that the facility design has not been altered such to perform undeclared activities. A physical inventory verification (PIV) is performed as necessary to verify the presence of declared materials and the absence of undeclared materials.

One safeguards method to verifying the presence of material is through "nuclear material accountancy" (NMA). This method establishes "Material Balance Areas" (MBAs) through which nuclear material flows. General mass balance equations are applied to the special nuclear materials which flow in and out of a MBA as well as materials which

are created or destroyed. In general, MBAs are selected based on the design characteristics of the facility and the points in the process area which permit the optimal balance between the maximization of materials verification (i.e., minimization of measurement uncertainties) and the minimization of inspection resource requirements. The locations that the nuclear material is in a form that can be measured for material flow or inventory are called key measurement points (KMP). KMPs are, but not limited to, the inputs and outputs of MBAs (International Atomic Energy Agency 2001). Other methods of NMA include item counting and item balances for situations which are not suitable for mass balances. For some facilities, significant amounts of materials may be in the process lines inside the MBA. Additionally, some "hold up" may occur where materials are permanently deposited in the process lines. During an inspection, it may be necessary for the facility operator to clear the process lines in order for the inspector to perform the material balance. For the occasions where there is more than a significant quantity of material in the hold up, the inspector will directly measure the material deposited in the process lines in the process area. A material balance period is established for each MBA and/or facility based on the uncertainties inherent in the safeguards measurement techniques as well as the timeliness criteria.

The nuclear material measured at KMPs can either be in bulk form or item form. Materials in item form are items that are easy to identify and account for. Examples of item form material includes fuel assemblies and fuel pins. Bulk material is liquids, gas or powder. Bulk material also includes pellets or pebbles that cannot be individually identified for NMA (International Atomic Energy Agency 2001).

Another verification method is Containment and Surveillance (C/S). This method utilizes the continuous monitoring or "continuity of knowledge" (CoK) of items or materials to verify their presence. Specifically, surveillance cameras are used to monitor the presence of material until it can be placed in an IAEA sealed container. IAEA seals can be generally understood as a tamper indicating locks. The C/S method is usually

applied to safeguarded materials which are difficult to verify by quantitative measurements, such as irradiated nuclear fuel assemblies.

Attended, Unattended, and Remote Monitoring Systems (AMS/UMS/RMS) are deployed at facilities to assist the inspectors carrying out their mission. AMS are either portable or resident at a facility and require an IAEA inspector to operate them. These are devices such as handheld radiation detectors and physical seals. UMS are resident at a facility and do not require an inspector to operate them. These include devices such as detectors, cameras, and electronic seals in process and transport areas. Data are collected by these systems continuously. Conditions regarding the inspector's authorities to review, collect, and remove data from a facility depend upon individual agreements between the IAEA and the facility established through the Comprehensive Safeguards Agreement (International Atomic Energy Agency 1972) and the Model Additional Protocol (International Atomic Energy Agency 1997). Data restricted to the facility must be evaluated during an inspection by an inspector at the facility and either erased after use or left behind at the facility. Data released from the facility may be retrieved physically by an inspector via a data storage device. RMS are UMS using a remote monitor (RM) which can collect data remotely via the internet and are used to reduce the burden of inspection for both the IAEA inspector and the facility operator.

2.1.3 UNATTENDED AND REMOTE MONITORING SYSTEMS

UMS generally consist of a detector, detector electronics, data acquisition system, data storage system, and backup power supply. RMS includes all these with the addition of a remote monitor (RM) such as a modem or other connectivity devices. Redundancies of components are required to ensure that there are no system failures or loss of data. Individual component failures occur and must be anticipated in the system design stages. For UMS/RMS systems which focus on maintaining the CoK, a system failure may result in the loss of the CoK, if there is data loss. If loss of the CoK occurs, inspectors must perform a PIV to be performed to regain the CoK. A UMS/RMS failure also triggers an unscheduled maintenance where a technician is dispatched immediately to

replace/repair the failed system. Both the PIV and maintenance are manpower intensive and consume significant IAEA and operator resources. Thus, UMS/RMS reliability is very important to the optimization of safeguards.

2.1.4 CURIUM-PLUTONIUM RATIO (Cm-Pu Ratio)

The Cm-Pu ratio technique is where the Cm-Pu ratio is multiplied by either the singles or doubles neutron count rate to obtain the concentration of plutonium in the measured material. The neutrons from ^{244}Cm are a dominant source of neutrons in spent fuel and fresh fuel that still contains major actinides. Once the ^{244}Cm is measured by neutron detectors the concentration of plutonium in the spent fuel or fresh fuel can be calculated based on the ratio (Rinard et al. 1996). The fresh fuel from the ESFR pyroprocessing facility leaves the actinides, including ^{244}Cm, in the fuel.

2.2 RELIABILITY ENGINEERING

The proliferation weaknesses of a system with respect to UMS reliability can be determined by identifying the least reliable component or subsystem in the system.

Reliability engineering is the analysis of the reliability and failure characteristics of individual components or a system of components. Reliability is defined to be "the probability of a product performing its intended function for a stated period of time under certain specified conditions" (Mitra 1998). The reliability of a component can be modeled statistically using time-independent or time-dependent failure probability distributions and measurable parameters, such as the component mean-time-to-failure (MTTF). Time-independent models, such as the exponential distribution, are used to model random chance-failures with a constant, time-independent failure-rate. Time-dependent models, such as the Weibull distribution, are used to model random chance-failures with a variable, time-dependent failure-rate (Mitra 1998). Time-dependent models are particularly useful for modeling the debugging or wear-out of components while the time-independent models are useful for modeling normal operation. System reliability can be calculated from the reliability models for each of the individual system

components. These reliability engineering models must be applied to a problem to produce results. For this work, the ESFR has been adopted as the model to demonstrate these methods.

2.3 EXAMPLE SODIUM FAST REACTOR (ESFR)

The Example Sodium Fast Reactor (ESFR) is a hypothetical Generation IV (GenIV) nuclear reactor; it is not an operating facility and will presumably never be built. This hypothetical sodium-cooled fast reactor and pyroprocessing facility were designed by Argonne National Laboratory (ANL) for the purpose of facilitating discussion on the subject of fast reactor and pyroprocessing safeguards in the absence of a safeguards confidential design and processing information from an operating facility.

Sodium fast reactors are one of the GenIV facilities that would possibly have a co-located nuclear fuel reprocessing facility included in the design. Nuclear material pyroprocessing is a type of dry reprocessing that uses molten salts as solvents as opposed to aqueous reprocessing e.g. PUREX process (Plutonium and Uranium Recovery by Extraction) that uses water and organic compounds. The ESFR pyroprocessing facility never separates the plutonium from the actinides; therefore the fresh fuel contains actinides. Nuclear fuel reprocessing facilities are of particular concern when it comes to proliferation resistance. Having the co-located facility increases the attractiveness of the site to potential proliferators due to the presence of bulk nuclear material and the ability to acquire plutonium in a form easier to convert to a weapon.

The ESFR design includes four 800 MWth (300 MWe) reactors (Argonne National Laboratory 2006) and an on-site pyroprocessing fuel cycle facility (FCF), which includes fuel fabrication, as shown in Fig. 1 (Argonne National Laboratory 2006). The fuel used at the ESFR is metallic fuel containing U and Pu.

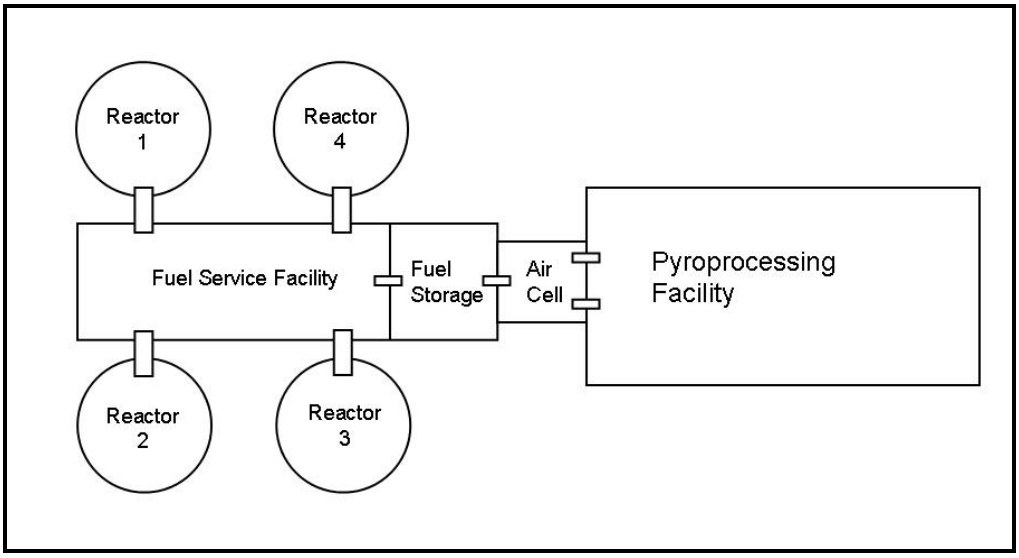

Figure 1. Example Sodium Fast Reactor (ESFR) layout

The pyroprocessing facility layout is shown in Fig. 2 (Argonne National Laboratory 2006). The basic, high-level materials flow for the pyroprocessing facility is described below. More information on the pyroprocessing facility and the material flow can be found in Appendix A. The material in the pyroprocessing facility is processed in batches and does not flow through pipes.

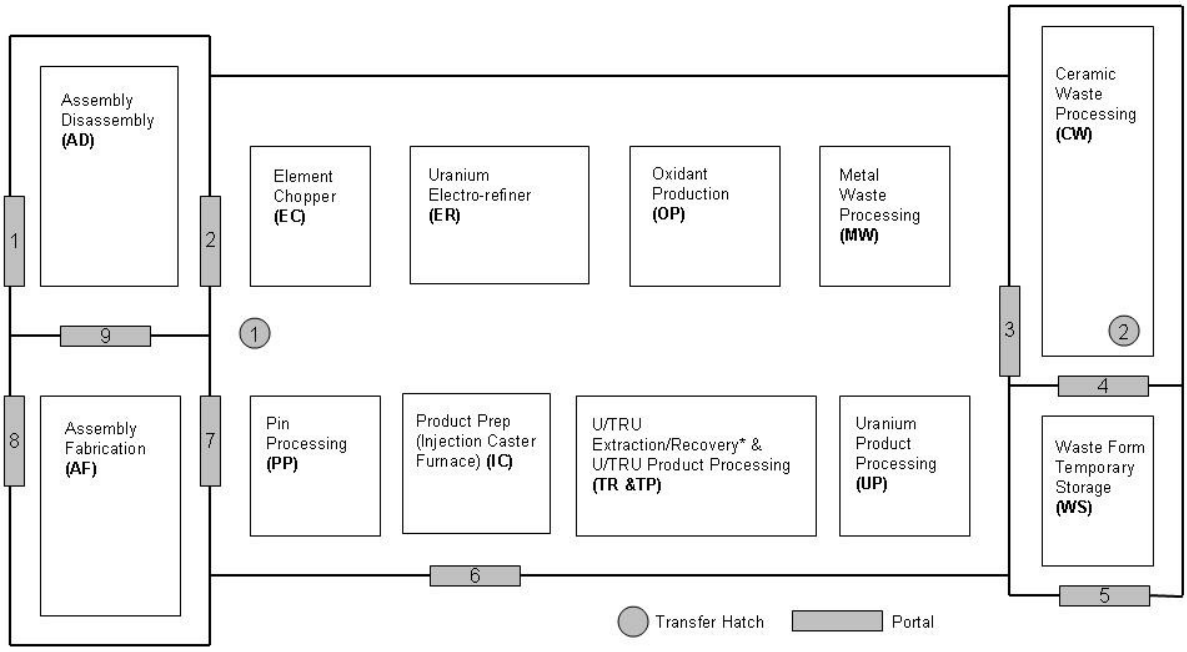

Figure 2. ESFR pyroprocessing facility layout

The below process areas are seen in Fig. 2.

- Assembly Disassembling (AD)

  The irradiated fuel assemblies are received from the fuel storage pit and disassembled. The fuel pins are passed into the argon filled process cell to be chopped. Assembly hardware that does not contain nuclear material is disposed. On average 0.57 fuel assemblies are processed per day over the entire year. The nuclear fuel being processed is from the co-located fast reactor which uses metallic fuel. Additionally, the fuel has been cooled for 7-8 years before it is sent to the pyroprocessing facility.

- Element Chopper (EC)

  The element chopper converts the irradiated fuel pins into ¼-inch long pieces. One hundred and fifty four pins are chopped each day. The chopped fuel pins are moved to the electro-Refiner (ER) in an anode basket. Four anode baskets are sent to the ER per day. Each anode basket contains about 10 kg of Pu within the irradiated fuel pieces.

- Electro-Refiner (ER)

  The purpose of the ER unit is to electrochemically separate uranium from other spent fuel constituents. During normal ER operation, essentially all of the uranium dissolves in the medium and electrochemically transports and deposits on the cathode as uranium metal. The uranium metal on the cathode is transferred to the uranium product processing (UP) unit. Undissolved cladding pieces, known as hulls, and noble metal fission products remain in the anode basket and are transferred to metal waste processing (MW). During normal ER operation, effectively all of the plutonium and other transuranic (TRU) elements dissolve in the salt phase. The salt from the ER containing dissolved U, TRU and fission products (FP) is sent to U/TRU Extraction/Recovery (TR).

  Two cathodes containing uranium metal are sent to uranium product processing (UP) per day. One container per day of salt is sent to the U/TRU Extraction/Recovery (TR).

- Uranium Product Processing (UP)

  The cathode from the ER is sent to the UP. The uranium metal from the ER is cast into ingots. The ingots are sent to the product prep injection caster furnace (IC). One container every three days is sent to the IC with twenty four 3.7 kg uranium (and small amounts of TRU) ingots. The adhering salt is recycled back to the ER.

- U/TRU Extraction/Recovery (TR) and U/TRU Product Processing (TP) – Two-Stage Electrolysis Option

  One container of salt per day from the ER is sent to the U/TRU Extraction/Recovery (TR). Each container has 260 kg of salt. The salt from the ER contains dissolved TRU (about 10.4 kg of Pu per container), reactive fission products, small amounts of cladding and small amounts of uranium. The U/TRU is removed from the salt in a two-stage process by electrochemical reduction. During the first stage, 100% of the U and 86% of the TRU is assumed to be removed. During the second stage, 86% of the

TRU is again extracted from what is left. This results in approximately 98% TRU extraction from the salt via the two electrolysis stages.

In the U/TRU product processing the U/TRU metal is formed into ingots. The ingots are sent to the product prep injection caster furnace (IC).

- Product Prep Injection Caster (IC)

  In the product prep unit, metal ingots from UP and TRU/U product processing are melted above 1200 ºC to serve as feed for fuel fabrication. Metal ingots are melted, mixed, and cast into TRU/U metal slugs.

- Pin Fabrication/Pin Processing (PP)

  TRU/U metal slugs from the IC are sent to the pin fabrication/pin processing (PP). The slugs are put into metal cladding with bond sodium to fill the gap between the TRU/U and the cladding. Each fuel pin is sealed, tested for leaks and sent to assembly fabrication (AF).

- Assembly Fabrication (AF)

  The 154 fuel pins per day from PP are sent to the assembly fabrication (AF). In the air-filled shipping and receiving cell, the pins are assembled into fuel assemblies. On average 4 assemblies per week are assembled.

2.4 PREVIOUS WORK

2.4.1 APPROACHES TO PROLIFERATION RESISTANCE

Success Tree Model Approach

Golay (2001) used the success tree representation as the framework to assess proliferation success probability. By determining an overall proliferation success

probability for an assessed facility design, comparisons between facility design concepts could be made.

Sentell (2002) did a study following the work of Golay that tested the concepts presented in Golay's study. Sentell used the same success tree model that was developed by Golay to compare a typical UO_2 fuelled pressurized water reactor (PWR), a PWR with thorium-oxide fuel, and a pebble bed modular reactor (PBMR). The probabilities used by Sentell for his success tree were based on his expert judgment.

Integrated Methodology for Quantitative Assessment of Proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods

This study used a probabilistic approach with event-trees and fault-trees to model diversion from the spent fuel storage of a modular pebble bed reactor system (MPBR). An integrated evaluation methodology was used. The methodology includes proliferation competition model development, model input evaluation, and pathway assessment. Expert elicitation was used for evaluation of key model inputs. The results of the study demonstrate the probabilistic approach to assessing the proliferation resistance of an advanced nuclear energy system (Ham 2005).

Safeguards Logic-Trees

Cojazzi, Renda and Contini (2004) elaborated on the safeguards logic-trees developed by Hill (1998). This investigation demonstrated the application of the fault-tree technique to the assessment of the proliferation resistance. The study identified possible acquisition pathways in a given nuclear fuel cycle and their quantification in terms of non-detection probability.

Multi-Attribute Utility (MAU) Analysis

MAU analysis has been used since the late 1970's to rank the attractiveness and risk factors associated with different proliferation pathways. In 2000, Ko, Kim, Yang and Park used MAU theory and an electrical circuit representation to model proliferation

resistance in a quantifiable way (Ko et al. 2000). In 2007, Charlton and his colleagues developed an additive, multi-attribute utility analysis (MAUA) method for proliferation resistance assessment for the U.S. Department of Energy's Advanced Fuel Cycle Initiative (AFCI) program (Charlton et al. 2007).

MAU analysis is applicable to a wide variety of nuclear energy systems and can identify strengths and weaknesses in a system. MAU analysis uses attributes (e.g., weight fraction of Pu in target material) that are weighted by importance to determine a proliferation resistance measure for each step. Each attribute is assigned a utility function via expert knowledge or a physical characteristic of the attribute. MAU allows ranking of various options and non-technical components can be considered. The values given to the attributes and weighting factors use objective (measurable) and/or subjective types of determinations.

A Practical Tool to Assess the Proliferation Resistance of Nuclear Systems: the SAPRA Methodology

A "simplified approach for proliferation resistance assessment" (SAPRA) was developed by AREVA for analysis of proliferation resistance of their reactor designs. It is based on an evaluation of the efficiency of material-related, technical, or institutional barriers against diversion or misuse by a country possessing civilian nuclear material or having developed technologies on its own territory or abroad. It was not a sophisticated method but rather a crude quantitative attempt to index or "measure" the proliferation resistance of a civilian nuclear fuel cycle at each of its steps (Greneche 2008).

2.4.2 PROLIFERATION RESISTANCE APPROACHES APPLIED TO THE ESFR

PR&PP Evaluation: ESFR Full System Case Study Final Report

This study applies the proliferation resistance and physical protection (PR&PP) methodology to the ESFR pyroprocessing fuel cycle facility (Generation IV International Forum Proliferation Resistance and Physical Protection Evaluation

Methodology Working Group 2009). Targets, target material, and potential proliferation pathways of the material in the pyroprocessing facility are outlined for the ESFR. Proliferation pathways for each material balance area (MBA) were analyzed qualitatively based on technical difficulty, cost, time, detection probability, fissile material type, and detection resource efficiency. The analysis focused on diversion (vs. misuse and abrogation/break-out). This study was an overview of the pathway as a whole. Further study would open up the possibility of analyzing the specific pathway segments (or steps the proliferators would take). Expert elicitation was used for the qualitative analysis in this case study.

Application of the Event-Tree/Fault-Tree Modeling Approach to the Evaluation of Proliferation Resistance

This study by Coles and Zentner (2007) used the PR&PP methodology to perform a fault-tree analysis of an attempted diversion scenario from the pyroprocessing facility at the ESFR. This diversion would result in the diversion of one significant quantity (SQ) of material in one year. The study focused on pathway analysis of a protracted diversion from the external uranium container.

Markov Model Approach to Proliferation-Resistance Assessment of Nuclear Energy Systems

Scientists at Brookhaven National Laboratory used a Markov model approach to assess the proliferation resistance of the ESFR for a protracted diversion (Yue et al. 2008). Their quantitative assessment modeled uncertainty, false alarms, concealment, and human performance. The PR&PP methodology also was incorporated into the model framework.

CHAPTER III
RELIABILITY DESIGN PROCESS

For existing safeguards systems, the proposed method can be used to determine the reliability (or probability of failure) of installed systems. For future systems, it would be used to design a safeguards system to a specified reliability.

System reliability is related to the probability of system failure. An analyst/designer can integrate this failure probability into more comprehensive probabilistic PR&PP models. Both the analysis and design processes are proposed in this chapter and demonstrated in the next chapter.

3.1 ANALYSIS AND DESIGN PROCESS – OVERVIEW

Fig. 3 shows the reliability design process. First, the reliability criteria for a system or facility are chosen and the initial safeguards design is laid out. The safeguards design reliability is analyzed to determine if it meets the reliability criteria. If it does the safeguards can be finalized and installed; otherwise, the safeguards design is revised and redundancies are added.

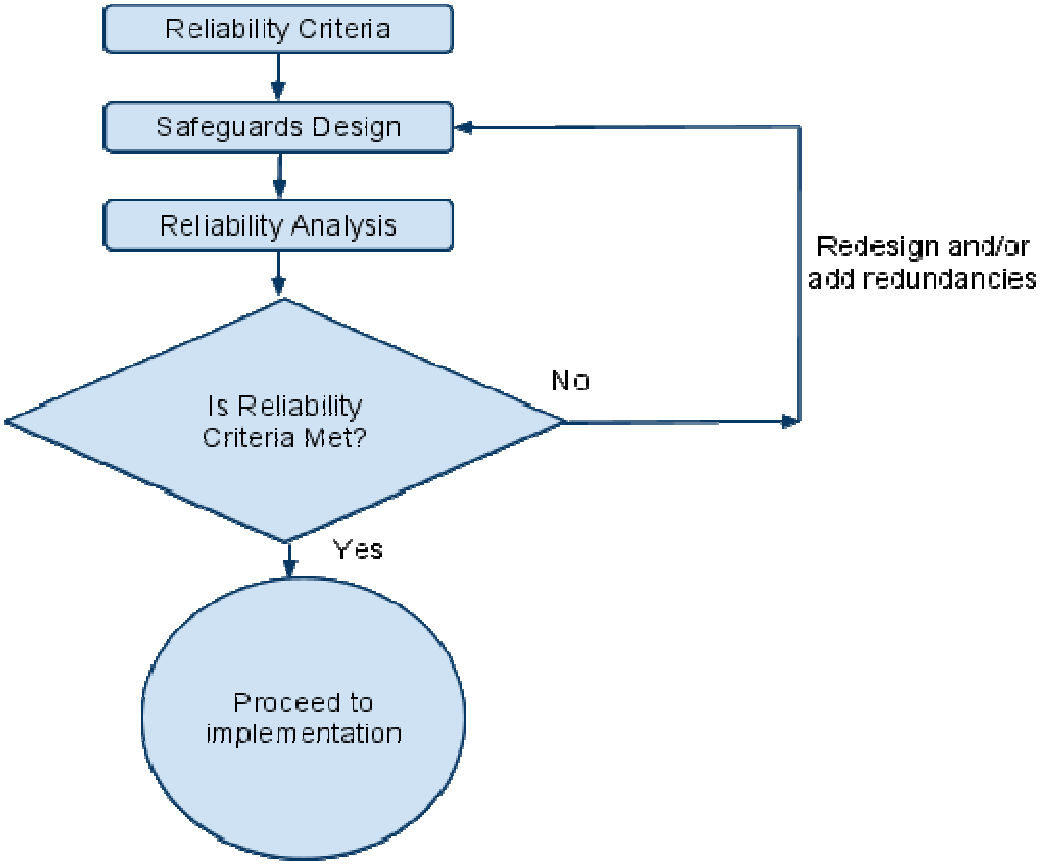

Figure 3. Design process for safeguards systems with respect to reliability criteria

3.2 RELIABILITY CRITERIA

The reliability criteria are user defined. The goal is to have the highest reasonable reliability criteria for a system.

Unattended systems which maintain the continuity-of-knowledge (CoK) require a high-level of reliability as system failure would result in the loss of the CoK. The cost associated with regaining the continuity-of-knowledge (if it is possible at all) is generally very high.

3.3 SAFEGUARDS DESIGN

The safeguards design consists of an overarching conceptual design of how the safeguards system will work at a given facility. The safeguards approach is generalized by facility type but varies significantly from facility to facility. A detailed discussion of safeguards system design is outside the scope of the current research.

3.4 RELIABILITY ANALYSIS

The reliability analysis focuses on determining the reliability of a safeguards system design. From the system analyst's and designer's prospective - there are two methods to acquiring appropriate reliability model parameters:

(1) Estimate system reliability from the data generated by past experience.
(2) Estimate system reliability from the individual component reliabilities stated by the manufacturer.

For method (1), the IAEA would be able to collect data on component failures and replacements over time. Proper failure reporting and archiving generates the reliability data necessary to determine the best model (either exponential or Weibull) and to estimate model parameters. For method (2), as previously discussed, system reliabilities can be estimated from individual component reliabilities.

Most products go through three distinct phases from product inception to wear-out. Fig. 4 shows a typical life-cycle curve for which the failure rate (λ) is plotted as a function of time (Mitra 1998). This curve consists of the debugging phase, chance-failure phase, and wear-out phases. The debugging phase represents the initial problems identified and corrected during prototyping and exhibits a decrease in the failure rate. The chance-failure phase represents the useful life of the product and exhibits failures which occur randomly and independently. The wear out phase represents the end of the product's useful life as parts age, wear out and exhibit an increase in the failure rate.

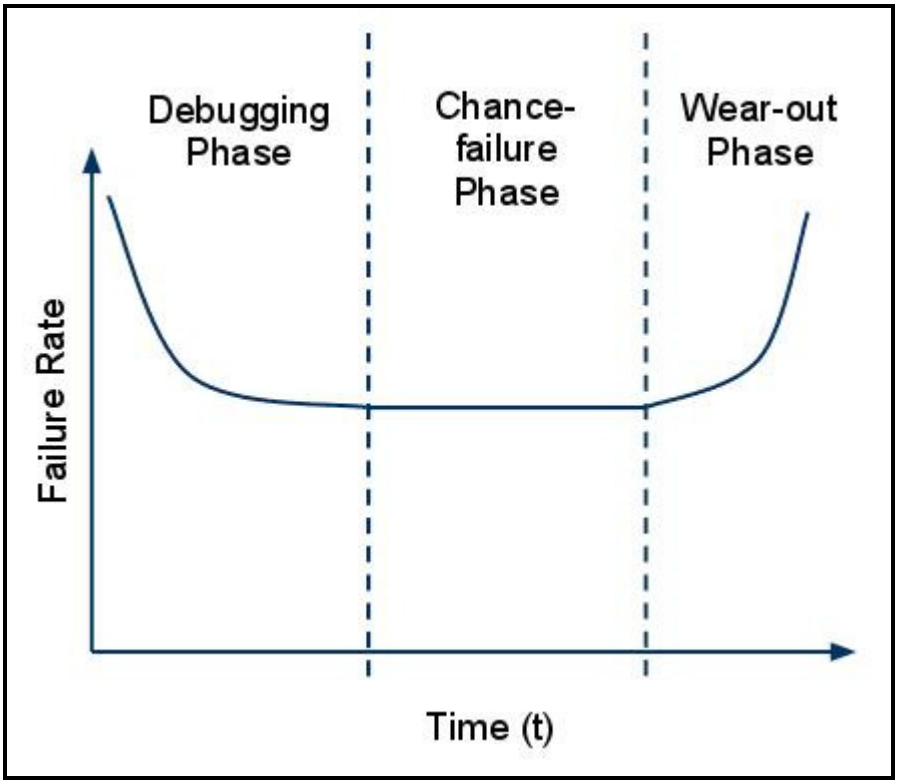

Figure 4. General equipment failure rate over the equipment lifetime

Some basic concepts in reliability engineering are the mean time to failure (*MTTF*), the mean time to detection (*MTTD*), the mean time to repair (*MTTR)*, and the mean time between failures (*MTBF*). The *MTTF* is the average (or expected) time interval between when a product is initially functional until it fails. The *MTTD* is the average (or expected) time interval between when a product failure occurs and is detected. The *MTTR* is the average (or expected) time interval between when a product failure is detected until it is repaired. The *MTBF* is the average (or expected) time between failures. The relationship between the these concepts is

$$MTBF = MTTF + MTTD + MTTR. \tag{3.1}$$

If time to detection is instantaneous or minimal (e.g., through remote monitoring) then *MTBF* is

$$MTBF = MTTF + MTTR \ \ where \ MTTD \approx 0. \tag{3.2}$$

If the time to detection is minimal and time to repair is short or minimal compared to the time to failure, then:

$$MTBF \approx MTTF \ \text{where} \ MTTD + MMTR \ll MTTF. \tag{3.3}$$

3.4.1 MODELING COMPONENT RELIABILITY

A component's reliability is represented by a distribution. Described below are two common distributions used to model reliability.

Exponential Distribution

For components with a failure rate that is constant and independent of time, failures are exponentially distributed. As seen in Fig. 4, the exponential distribution would be applied to the chance-failure phase of the component's lifetime. For example, if you had some number of identical components, N, and each began operating at time t = 0, and each component is expected to fail to fail randomly over time, the probability that a component will fail by time t will be exponentially distributed as shown in Fig. 5.

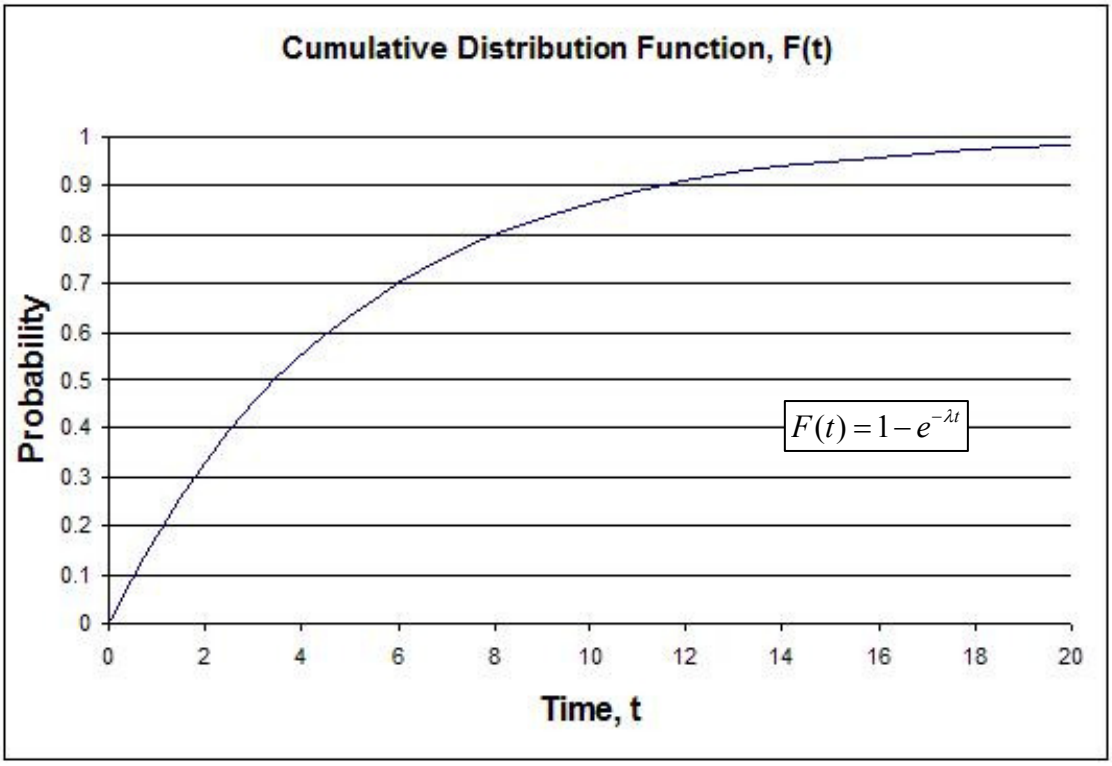

Figure 5. Failure function *F(t)* or CDF for the exponential distribution, $\lambda = 0.2$

For the chance-failure phase of a component's life (Fig. 4), the time until failure of a component with a constant failure rate can be modeled by the exponential distribution. These are in contrast to the debugging and wear out phases of a component discussed in the next sublevel. These phases have decreasing and increasing failure rates, respectively, which may be modeled by the Weibull family of distributions (Mitra 1998).

For exponentially distributed failures, the probability that a component fails at or before time, t, given a constant failure rate, λ, is represented by *F(t)*, the failure function or the cumulative distribution function (CDF) for the exponential distribution:

$$F(t) = \int_0^t \lambda e^{-\lambda t'} dt' = 1 - e^{-\lambda t}, \quad t \geq 0. \tag{3.4}$$

The failure function F(t) is related to the probability density function (PDF), *f(t)*:

$$f(t) = \frac{dF(t)}{dt}, \quad t \geq 0. \tag{3.5}$$

For the exponential distribution, the PDF is:

$$f(t) = \lambda e^{-\lambda t}, \; t \geq 0. \tag{3.6}$$

The *MTTF* for the exponential distribution is constant and is the reciprocal of the failure function and equal to the expected value *E(T)*:

$$E(T) = \int_0^\infty [1 - F(t)]\, dt = \int_0^\infty R(t)\, dt = MTTF. \tag{3.7}$$

For repairable equipment where the failure detection and component repair times are short relative to the *MTTF*, the *MTTF* is also equal to the mean time between failures (*MTBF*).

The probability that failure does not occur at or before time t is represented by $R(t)$, the reliability function, and is the compliment of the CDF:

$$R(t) = 1 - F(t). \tag{3.8}$$

For the exponential distribution, the reliability function is:

$$R(t) = e^{-\lambda t} \tag{3.9}$$

and is shown in Fig. 6.

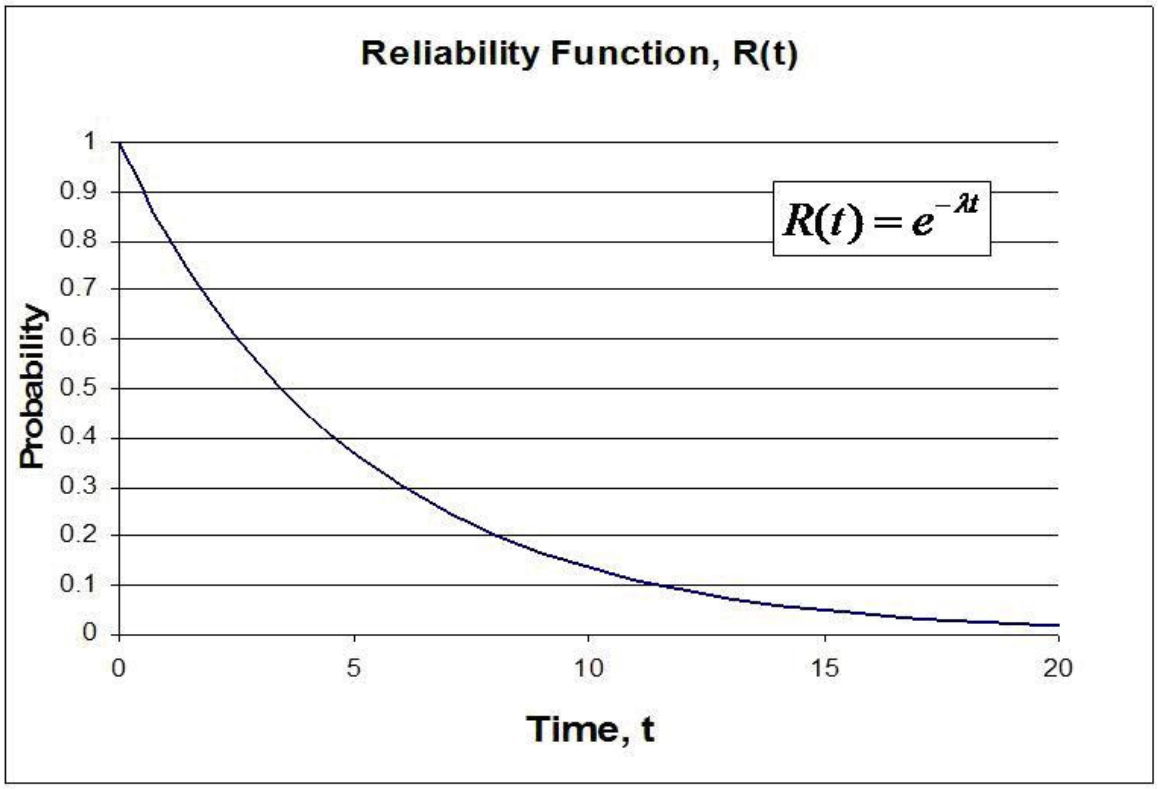

Figure 6. Reliability function *R(t)* for the exponential distribution, $\lambda = 0.2$

In general, the failure-rate function, *r(t)*, is given by the ratio of the PDF, *f(t)*, to the reliability function, *R(t)*;

$$r(t) = \frac{f(t)}{R(t)}. \tag{3.10}$$

For the exponential failure distribution:

$$r(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda, \tag{3.11}$$

which implies a constant failure rate, which is consistent with the earlier statement.

Weibull Distribution

For components with a variable failure rate, i.e., time-dependent, failures can often be modeled by the Weibull distribution. This is a three-parameter distribution whose PDF, *f(t)*, is given by:

$$f(t) = \frac{\beta}{\alpha} \times \left[\frac{(t-\gamma)}{\alpha} \right]^{\beta-1} \times e^{-\left[\frac{(t-\gamma)}{\alpha}\right]^{\beta}}, \quad t \geq \gamma \tag{3.12}$$

and the CDF or failure function, *F(t)*, is:

$$F(t) = 1 - e^{-\left[\frac{(t-\gamma)}{\alpha}\right]^{\beta}}, \quad t \geq \gamma. \tag{3.13}$$

The parameters are a location parameter $\gamma(-\infty < \gamma < \infty)$, a scale parameter $\alpha(\alpha > 0)$, and a shape parameter $\beta(\beta > 0)$, however, the γ parameter always equals zero when applied to reliability modeling (Mitra 1998). The location parameter determines the location or shift of the distribution. The scale parameter determines the spread of the distribution. The shape parameter affects the shape of the distribution (e.g. normal distribution, exponential distribution, etc). The PDFs for $\gamma = 0$, $\alpha = 1$ and several values of $\beta(\beta = 0.5, 1, 2, 4)$ are shown in Fig. 7 (Mitra 1998).

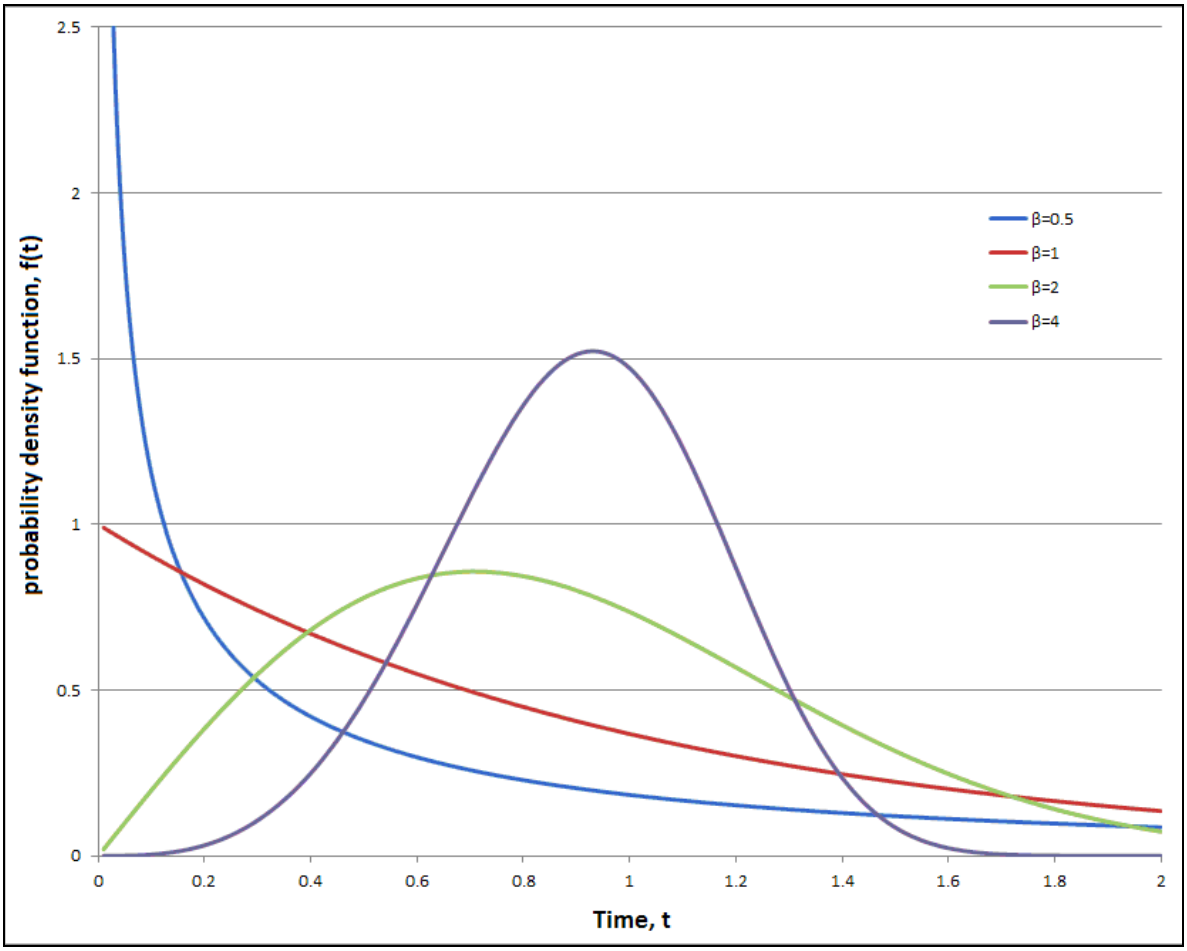

Figure 7. Weibull probability density functions (PDF) for $\gamma = 0$, $\alpha = 1$, $\beta = 0.5, 1, 2, 4$

The reliability function, *R(t)*, for the Weibull distribution is given by:

$$R(t) = e^{\left(-t/\alpha\right)^{\beta}} \tag{3.14}$$

and the MTTF is:

$$MTTF = \alpha \times \Gamma\left(\frac{1}{\beta + 1}\right), \tag{3.15}$$

where Γ is the gamma function which is expressed by

$$\Gamma(t) = \int_0^{\infty} e^{-x} \times x^{t-1} dx. \tag{3.16}$$

The failure-rate function, *r(t)*, for the Weibull time-to-failure probability distribution is

$$r(t) = \frac{f(t)}{R(t)} = \frac{\beta t^{\beta-1}}{\alpha^{\beta}}. \tag{3.17}$$

Fig. 8 shows the shape of the failure rate function for the Weibull distribution, for values $\beta(\beta = 0.5, 1, 3.5)$ and $\alpha = 1$.

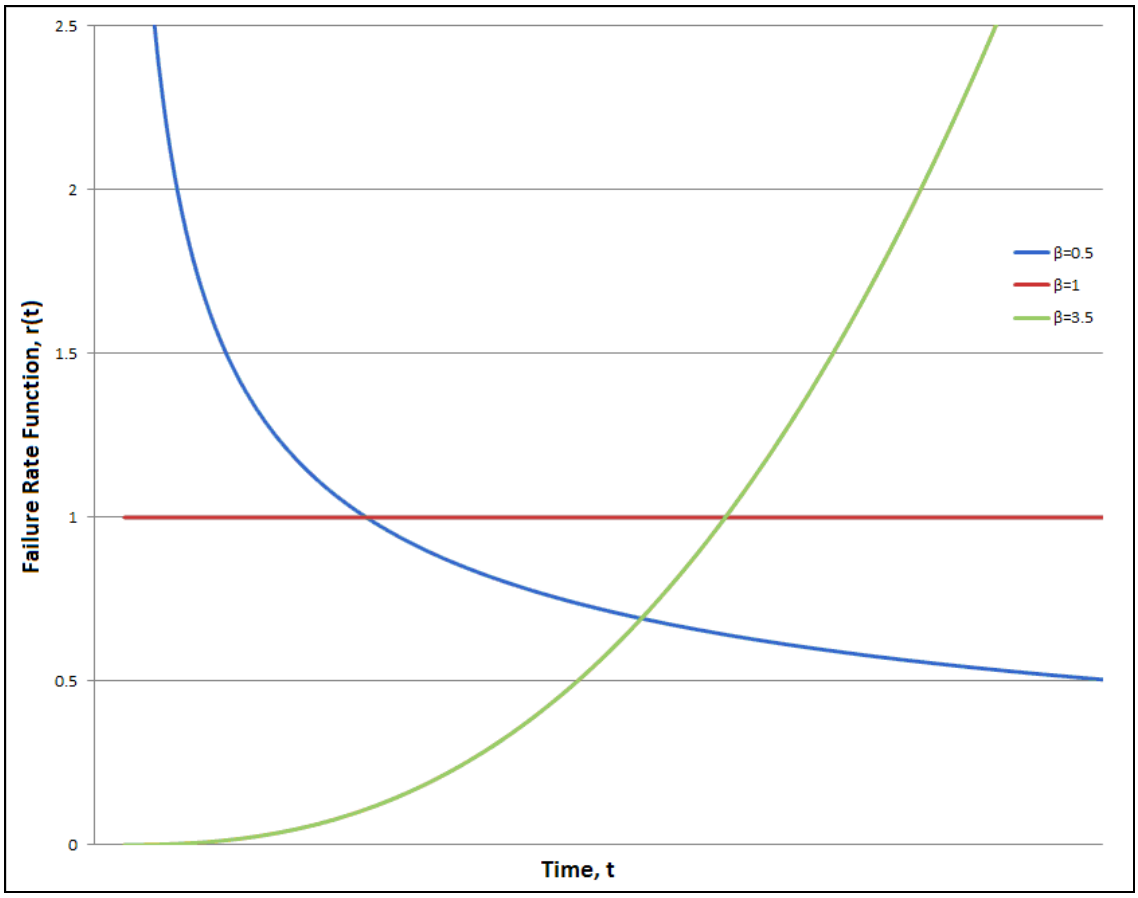

Figure 8. Failure-rate functions *r(t)* for the Weibull distribution for $\gamma = 0$, $\alpha = 1$ and $\beta = 0.5, 1, 3.5$

For $\gamma = 0$, $\alpha = 1$, $\beta = 1$, the failure rate is constant with time and the Weibull distribution becomes the exponential distribution (Fig. 8). If $\gamma = 0$, $\alpha = 1$ and $\beta = 0.5$, the failure rate decreases with time and can be used to model components in the debugging phase (Fig. 8). And if $\gamma = 0$, $\alpha = 1$ and $\beta = 3.5$, the failure rate increases with time and can be used to model components in the wear-out phase. In this case, the Weibull function approximates the normal distribution (Fig. 8).

3.4.2 MODELING SYSTEM RELIABILITY

Most systems are made up of a number of components. The reliability of each component and the configuration of the components which make up the system determine the system reliability. To increase the reliability of a system, redundancies can be added by placing components in parallel. As long as one of the parallel components operates, the system operates. Described here are the methods to determine a system's reliability based on the reliability of the individual system components for systems with components configured in series, parallel, and a combination of the two. In Chapter IV these will be used to calculate the system reliability of unattended monitoring systems which consist of a detector, data collect computer, and modem in series with redundancies in parallel. The exponential distribution will be used to model the components.

Systems with Components in Series

Fig. 9 shows a system with three components (A, B, and C) in series.

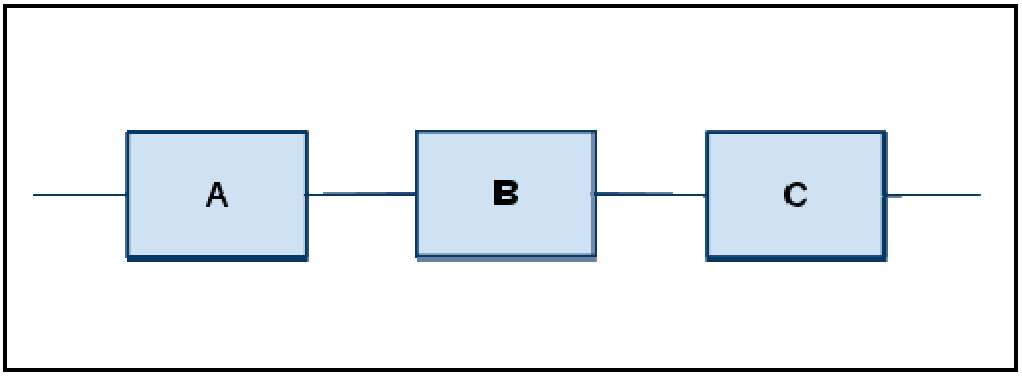

Figure 9. System with components A, B and C in series

For the system to operate, each component must operate. If one component fails, the entire system will fail. It is assumed that the components operate independently of each other (that is, the failure of one component has no influence on the failure of any other component). In general, if there are n components in series, where the reliability of the ith component is denoted by R_i, the system reliability, R_S is

$$R_S = R_1 \times R_2 \times \ldots \times R_n. \tag{3.18}$$

For the components in Fig. 9 the system reliability is

$$R_S = R_A \times R_B \times R_C \tag{3.19}$$

where R_A, R_B, R_C are the reliability of components A, B, and C, respectively.

The system reliability decreases as the number of components in series increases. Although over-design in each component improves reliability, its impact would be offset by the number of components in series. Manufacturing capabilities and resource limitations restrict the maximum reliability of any given component. Product redesign that reduces the number of components is a viable alternative.

If the system components can all be assumed to have a time-to-failure given by the exponential distribution, i.e., each component has a constant failure rate; we can compute the system reliability, failure rate, and mean time to failure. As noted earlier, when the components are in the chance-failure phase, the assumption of a constant failure rate could be justified. Suppose the system has n components in series, each with an exponentially distributed time-to-failure with failure rates $\lambda_1, \lambda_2, ..., \lambda_n$. The system reliability, R_S, is found as the product of the component reliabilities:

$$R_S = e^{-\lambda_1 t} \times e^{-\lambda_2 t} \times \ldots \times e^{-\lambda_n t} = e^{-\left(\sum_{i=1}^{n} \lambda_i\right) t}. \tag{3.20}$$

This implies that the time-to-failure of the system is exponentially distributed with an equivalent failure rate, λ_S, of

$$\lambda_S = \sum_{i=1}^{n} \lambda_i. \tag{3.21}$$

Therefore, if each component that fails is replaced immediately with another that has the same failure rate, the mean-time-to-failure for the system, $MTTF_S$, is given by

$$MTTF_S = \frac{1}{\lambda_S} = \frac{1}{\sum_{i=1}^{n} \lambda_i}. \tag{3.22}$$

Systems with Components in Parallel

System reliability can be improved by placing components in parallel. Since components are redundant and independent of each other; the system operates as long as

at least one of the components operates. The only time the system fails is when all the parallel components fail. Fig. 10 shows an example for a system with three components (A, B, and C) in parallel. All components are assumed to operate simultaneously.

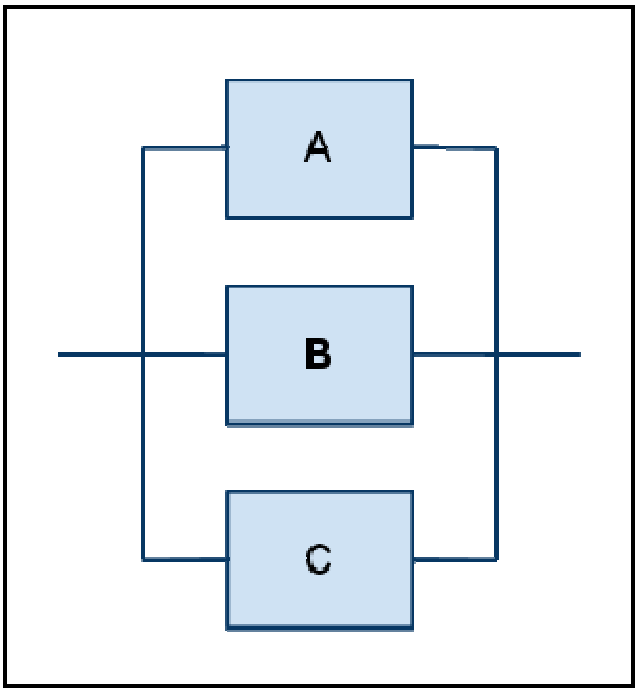

Figure 10. System with components A, B and C in parallel

Suppose we have n components in parallel, with the reliability of the *ith* component denoted by R_i, $i = 1, 2, ..., n$. Assuming that the components operate randomly and independently of each other, the probability of failure of each component is given by $F_i = 1 - R_i$. Now, the system fails only if all the components fail. Thus, the probability of system failure, F_S, is

$$F_S = (1 - R_1) \times (1 - R_2) \times ... \times (1 - R_n) = \prod_{i=1}^{n} (1 - R_i). \tag{3.23}$$

For the components in Fig. 10 the system failure, F_S, is

$$F_S = (1 - R_A) \times (1 - R_B) \times (1 - R_C) \tag{3.24}$$

where R_A, R_B, R_C is the reliability of component A, B, and C, respectively.

The reliability of the system, R_S, is the complement of F_S and is given by

$$R_S = (1 - F_S) = 1 - \prod_{i=1}^{n} (1 - R_i). \tag{3.25}$$

If the time-to-failure of each component can be modeled by the exponential distribution, each with a constant failure rate λ_i, $i = 1, 2, ..., n$, the system reliability (R_S), assuming independence of component operation, is given by

$$R_S = 1 - \prod_{i=1}^{n} (1 - R_i) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t}). \tag{3.26}$$

The time-to-failure distribution of the system is not exponentially distributed. Therefore, the mean time to failure (*MTTF*) for the system with n identical components in parallel, assuming that each component is immediately replaced by an identical component, is given by

$$MTTF = 1/\lambda \,(1 + 1/2 + 1/3 + ... + 1/n). \tag{3.27}$$

Systems with Components in Series and in Parallel

Complex systems often consist of components that are both in series and in parallel. Reliability calculations are based on the previously discussed concepts, assuming that components operate independently. For the complex system shown in Fig. 11

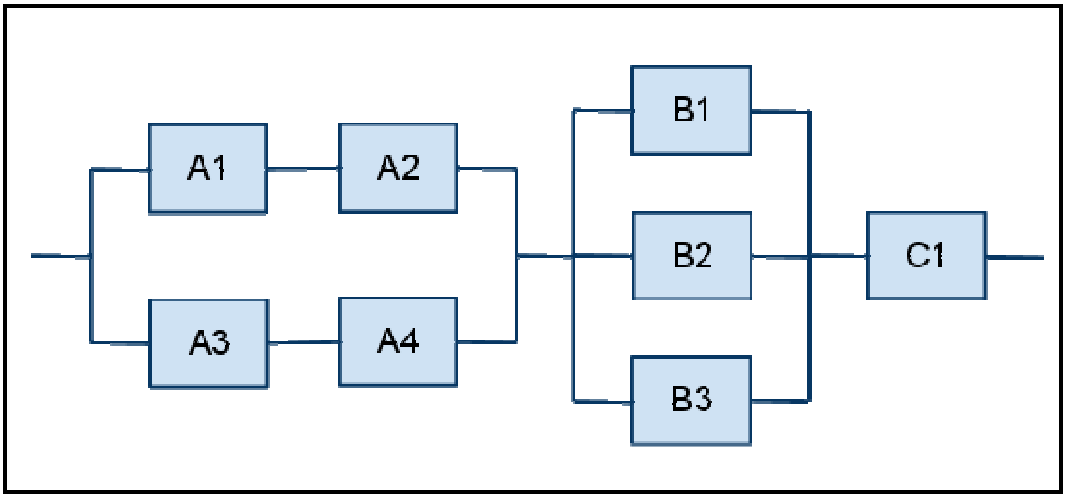

Figure 11. Complex system with components in series and in parallel

$$R_S = R_A \times R_B \times R_{C1} \tag{3.28}$$

where

$$\begin{aligned} R_A &= 1-(1-R_{A1}\times R_{A2})(1-R_{A3}\times R_{A4}) \text{ and} \\ R_B &= (1-R_{B1})(1-R_{B2})(1-R_{B3}). \end{aligned} \tag{3.29}$$

R_A is the reliability of components A1, A2, A3, and A4. The same applies for R_B. R_{A1} is the reliability of component A1, etc. If the time to failure for each component can be assumed to be exponentially distributed, the system reliability and mean time to failure can be calculated under certain conditions using the previously discussed procedures.

Systems with Standby Components

In a standby configuration, one or more parallel components wait to take over operation upon failure of the currently operating component. Here, it is assumed that only one component in the parallel configuration is operating at any given time. Because of this the system reliability is higher than for comparable systems with components in parallel.

In parallel systems discussed previously, all components are assumed to operate simultaneously. Fig. 12 shows a standby system with a basic component and two standby components in parallel. Typically a failure-sensing mechanism triggers the operation of a standby component when the currently operating component fails.

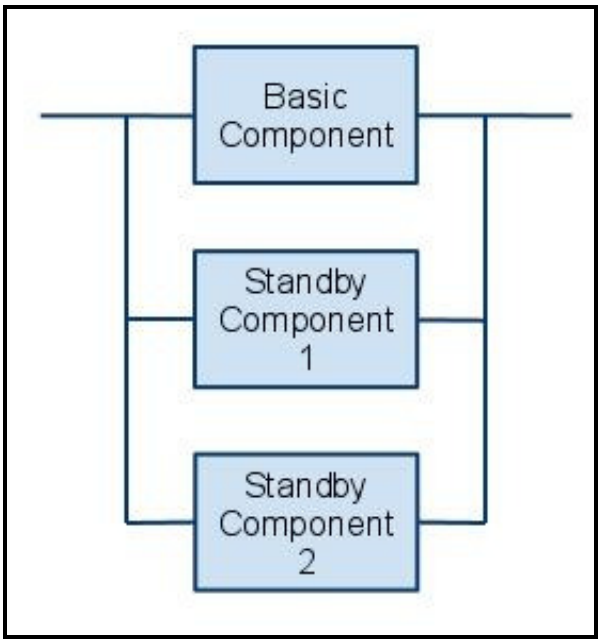

Figure 12. System with one main component and two standby components

If the time to failure of the components is assumed to be exponential with failure rate λ, the number of failures in a certain time t adheres to a Poisson distribution with the parameter λt. Using the Poisson distribution, the probability of x failures, *P(x)*, in time t is given by

$$P(x) = \frac{e^{-\lambda t} \times (\lambda t)^x}{x!}. \tag{3.30}$$

For a system that has a basic component in parallel with one standby component, the system will be operational at time t, as long as there is no more than one failure. In this situation the system reliability, *R(t)*, is

$$R(t) = e^{-\lambda t} + e^{-\lambda t} \times \lambda t. \tag{3.31}$$

For a system that has a basic component and two standby components (Fig. 12) the system will be operational if the number of failures is less than or equal to 2. The system reliability is

$$R(t) = e^{-\lambda t} + e^{-\lambda t} \times \lambda t + e^{-\lambda t} \times \frac{(\lambda t)^2}{2!}. \tag{3.32}$$

In general, if there are n components on standby along with the basic component (for a total of n+1 components in the system), the system reliability is given by

$$R_s(t) = e^{-\lambda t}\left[1 + \lambda t + \frac{(\lambda t)^2}{2!} + \frac{(\lambda t)^3}{3!} + \ldots + \frac{(\lambda t)^n}{n!}\right]. \tag{3.33}$$

The mean time to failure for such a system is

$$MTTF_s = \frac{(n+1)}{\lambda_i}. \tag{3.34}$$

3.4.3 SIMULATION

Direct calculations can be performed to determine the reliability of simple systems. However, simulations are better suited for the analysis of complex systems with various component models and/or complex distributions. Simulations are relatively simple to understand and easy to implement. A random number generator is used to simulate random failures given a representative failure distribution for each component. First, a random number, *T*, is generated uniformly between 0 and 1. Second, the reliability

function is set equal to *T*. Third, the equation is inverted for the time, t_f, which represents the time of the random failure.

$$R(t_f) = T \geq t_f = R^{-1}(T). \tag{3.35}$$

For the exponential distribution,

$$R(t) = T = e^{-\lambda t_f} \tag{3.36}$$

where

$$t_f = \frac{-\ln(T)}{\lambda}, \tag{3.37}$$

which is shown in Fig. 13.

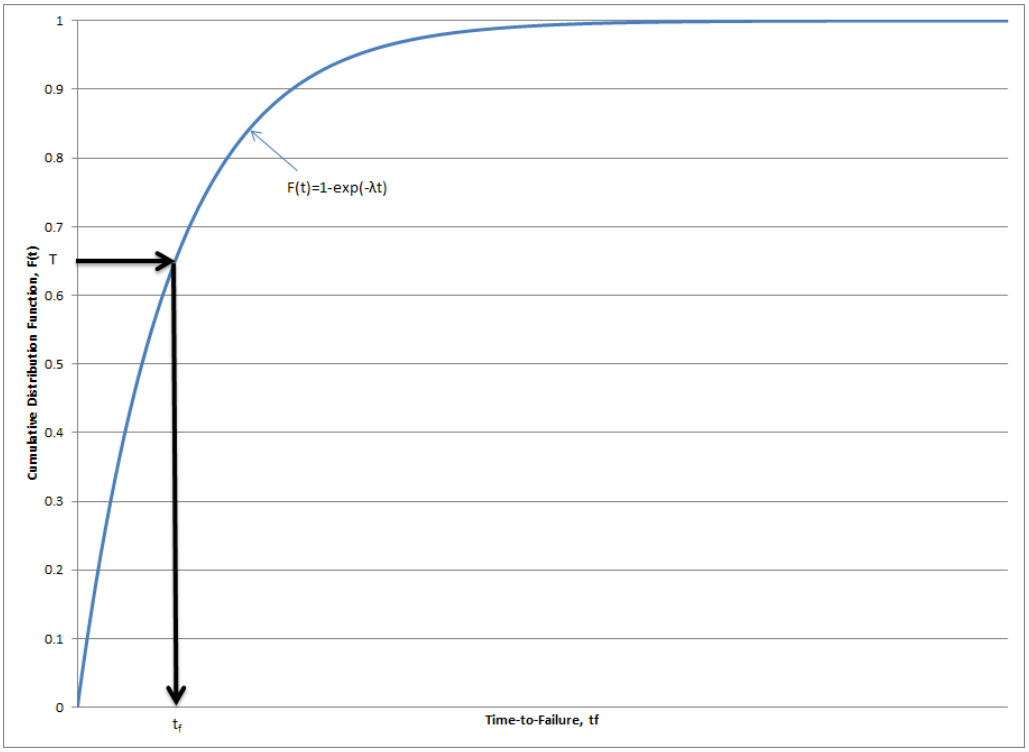

Figure 13. Simulation example for failure function exponential distribution

For the Weibull distribution,

$$R(t) = T = e^{-\left(\frac{t_f}{\alpha}\right)^{\beta}}, \text{ and} \tag{3.38}$$

$$t_f = -\alpha \times \ln(T)^{1/\beta}. \tag{3.39}$$

The repair distribution is coupled to the failure distribution to complete the simulation model. The simulation should be run a sufficient number of times to reduce the variance of the MTTF of the system. Alternatively, the model can be run for the lifetime of the facility to include scheduled maintenance, upgrades, etc.

3.5 RELIABILITY DESIGN

A system designer iteratively improves the reliability of the components most likely to fail the fastest in the system one at a time while minimizing costs. After the addition of each component, the designer should repeat the reliability analysis of the updated design and compare the updated *MTTF* for the system with the value stated in the reliability criteria. If the updated *MTTF* is greater than the specified reliability criteria, the design has acceptable reliability. If the *MTTF* is less than the specified value, additional redundancies or more reliability components are necessary in the design and the design process is iterated again.

The approach to adding redundancies varies depending on additional design constraints, such as cost. For example, on each iteration of the design process a component is added. Without consideration of the cost of the added component, the designer would simply add a redundancy with the goal of minimizing components. Therefore, the design is optimized to maximize the improvement-per-component-added. However, if cost is considered, the designer would add a redundancy in the most cost efficient manner. Thus, the design is optimized to maximize the improvement-per-cost-added.

In Fig. 14, a designer with the choice of system A, B or C would choose system B because it meets the minimum reliability criteria and does not exceed the maximum cost for the system.

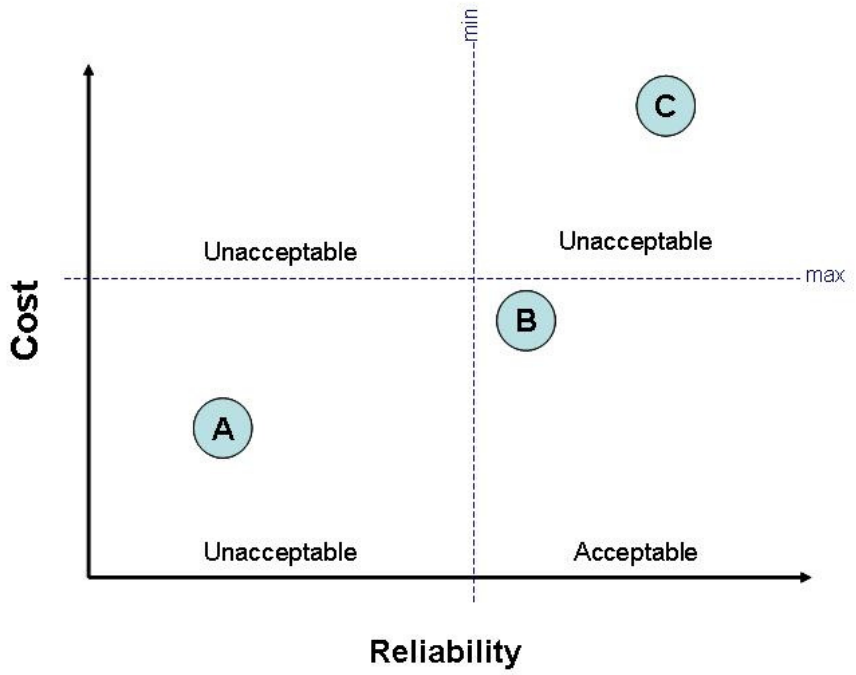

Figure 14. Reliability vs. cost

3.6 SUMMARY

This chapter discussed the methods and distributions used to analyze the reliability of systems and design systems with target reliabilities. The modeling of components in series, parallel and in complex systems was additionally reviewed.

CHAPTER IV
ANALYSIS

4.1 OBJECTIVE

Chapter IV demonstrates the safeguards reliability decision process using the ESFR pyroprocessing facility. Basic unattended monitoring components with associated failure rates will be applied to the ESFR fuel cycle facility (FCF) and analyzed for overall reliability.

4.2 SAFEGUARDS DESIGN FOR ESFR PYROPROCESSING FACILITY

A hypothetical and basic safeguards system design for an ESFR pyroprocessing facility is presented here. The "hypothetical" refers to the fact that an actual facility of this type does not exist, thus the custom attended and unattended monitoring systems which would be used by the IAEA to safeguard this facility also do not exist. The "basic" refers to the fact that the presented design only considers the basic UMS component of the safeguards system design and therefore does not include the detail of a complete safeguards design for this facility. A complete safeguards design would include directional monitoring of the fuel, in-process monitoring of the pyroprocessing, containment and surveillance, and in-core operational monitoring.

Many of the UMS systems proposed in the literature for use at the ESFR FCF suggest using technology that is either not available or not approved for use by the IAEA. Since the purpose of this design is to facilitate the demonstration of the reliability analysis, the design presented here only includes currently available technology in use by the IAEA; the design itself is not emphasized.

The UMS used in the current design are discussed in terms of the UMS technologies used to measure the particular nuclear material form because, as mentioned previously, the exact UMS equipment would be of a custom design using technology available to the

IAEA. The UMS technology used at each measurement point is described in the design and not a specific system. The appropriate reliability models and parameters associated with each UMS technology is estimated from information available in the literature for similar UMS equipment or a reasonable parameter is approximated. Clearly, it is not appropriate to publish actual IAEA UMS reliability values for confidentiality reasons and, consequently, the values used here are not meant to imply accuracy but to be reasonable estimates. Again, the objective is demonstration of the reliability analysis process.

4.2.1 MATERIAL BALANCE AREAS AND PORTALS

Nuclear material accountancy (NMA) is performed by applying material balance areas (MBA) to the fuel cycle facility (FCF) of the ESFR and monitoring the flow of materials in and out of the MBAs. These MBAs are shown in Fig. 15. MBAs are based on the convenience of the measurement of the nuclear material at the entrances and exits of these areas. The primary movement of materials is through Portal 1, to Portal 2, to Portal 7, and through Portal 8 last. At these locations the materials are in the form of spent fuel assemblies, spent fuel elements, fresh U/TRU elements, and fresh U/TRU fuel assemblies, respectively. Potentially there are additional convenient measurement points inside the process area, such as the U/TRU ingots, but without specific details, such as ingot size and shape, no meaningful assumptions about measurements will be made in this exercise.

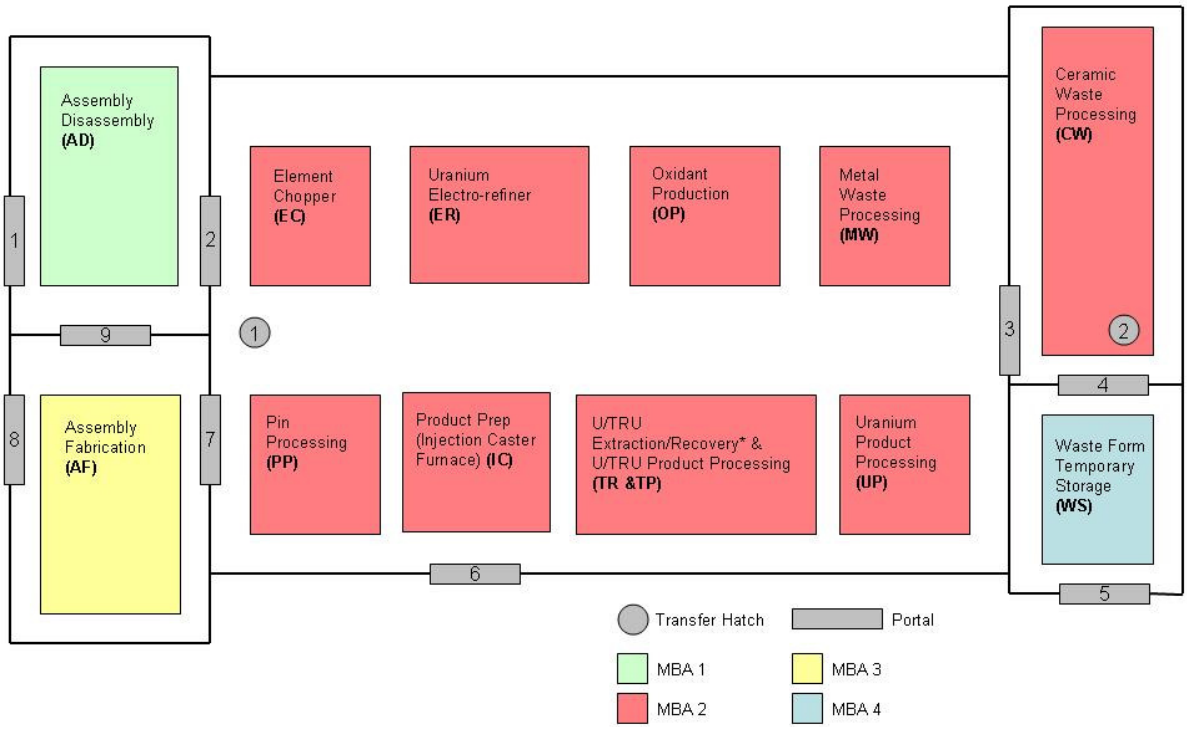

Figure 15. MBAs, for ESFR pyroprocessing facility

MBA 1 contains the assembly disassembly (AD) area. Spent fuel assemblies pass through Portal 1 from the spent fuel storage to AD. Spent fuel pins exit the AD through Portal 2 to the element chopper (EC). Portal 9 is used to move fuel handling equipment between MBA 1 and MBA 3.

MBA 2 includes the element chopper, electro-refiner (ER), uranium product processing (UP), U/TRU extraction/recovery (TR), U/TRU product processing (UP), injection caster furnace (IC), pin processing (PP), oxidant production (OP) and metal waste processing (MW). MBA 2 is also referred to as the process cell (PC) and is a hot cell and filled with argon.

MBA 3 contains only the assembly fabrication. Fresh fuel pins enter the MBA through portal 7 and fresh fuel assemblies exit MBA 3 through portal 8.

MBA 4 contains the ceramic waste processing (CW) and waste form temporary storage (WS). Salt waste enters MBA 4 through Portal 3. The vitrified waste canisters exit the CW through Portal 4 into the WS. Portal 5 is used when the vitrified waste will be removed from the site.

Portal 1. The spent fuel assemblies are passed through multiple, ring-type neutron counters upon entering MBA1. The measured total neutron and gamma counts should be consistent with Monte Carlo n-Particle (MCNP) and burn-up calculations which utilize operator declarations and in-core monitoring, if any.

Portal 2. Spent fuel pins pass through Portal 2 from the assembly disassembly (AD) area to the element chopper (EC).

Portal 3. Spent salt passes through Portal 3 from the process cell to MBA 4. This portal will not be considered in the safeguards design due to its infrequent use.

Portal 4. Vitrified waste canisters pass through Portal 4 from ceramic waste processing (CW). This portal will not be considered in the safeguards design due to its infrequent use.

Portal 5. Vitrified waste canisters pass through Portal 5 from the waste form temporary storage.

Portal 6. Make-up TRU and uranium pass through Portal 6 from an external source.

Portal 7. Fresh fuel pins pass through Portal 7 from pin processing (PP) in the process cell to assembly fabrication (AF).

Portal 8. Fresh fuel assemblies pass through Portal 8 from assembly fabrication (AF) to fresh fuel storage.

Portal 9. Fuel handling equipment passes through Portal 9 back and forth between assembly disassembly and assembly fabrication.

4.2.2 SIMPLIFYING ASSUMPTIONS FOR ANALYSIS

To facilitate the analysis of the ESFR FCF, some simplifying assumptions were made.

- MBA 4, Portal 4 and Portal 5 were not considered in this analysis since the waste portion of the facility would be in use much less often than MBA 1, MBA 2 and MBA 3. MBA 4 is where waste is processed and it is assumed it will only operate once a large quantity of waste has accumulated to be vitrified.
- Portal 3 was not considered in the analysis. It is assumed Portal 3 is under IAEA safeguards seal and not used unless an inspector is present with attended monitoring. This is because the waste transferred through Portal 3 is assumed to be infrequent.
- Portal 6 was not considered in the analysis. Portal 6 is under IAEA safeguards seal and is not used unless an inspector is present with attended monitoring. This portal is to add makeup material to the fuel as needed and the portal will not need to be used frequently.
- Portal 9 was not considered in the analysis as a simplifying assumption and because nuclear material does not pass through this portal.
- Transfer hatches 1 and 2 were not considered in the analysis. They are used to move equipment into a hot area for repair and will be assumed to also be used infrequently and under IAEA safeguards seal.

After the above assumptions are applied, only MBA 1, MBA2, MBA 3, Portal 1, Portal 2, Portal 7 and Portal 8 in will be considered for analysis (see Fig. 16).

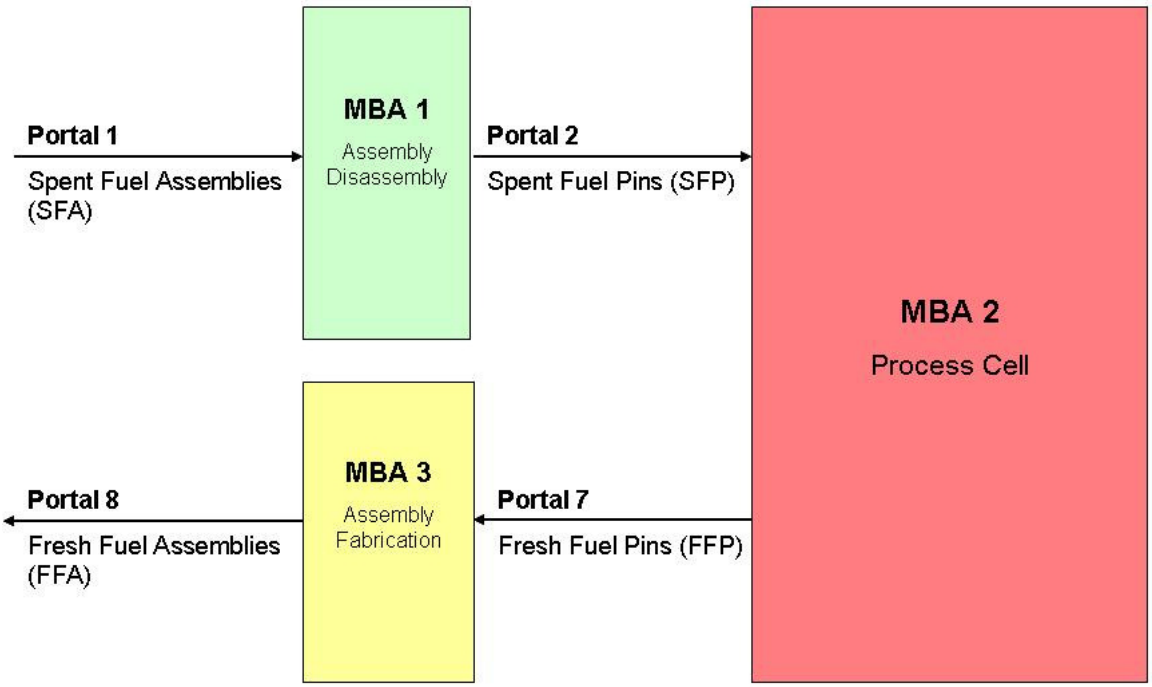

Figure 16. Simplified MBAs and portals for ESFR pyroprocessing facility

4.2.3 UNATTENDED MONITORING SYSTEM TECHNOLOGIES

The following assumptions were made for unattended monitoring systems:

1. No dual-use equipment where the facility and the IAEA share equipment.
2. Integrated safeguards, where the equipment and data collected are both utilized by the IAEA and the operator, was not considered.
3. Only technologies currently in use by the IAEA or similar was considered.
4. Only the key equipment needed for the Cm-Pu balance was considered. Peripherals such as directional flow monitoring were not considered in this analysis.
5. No components will be modeled as stand-by components. The IAEA currently does not implement stand-by for UMS.

At each portal there are certain data to be collected. Below in Table 2 are the basic systems that would be needed to implement Cm-Pu accountancy. This is based on the ESFR safeguards in Option 1 of Budlong Sylvester et al. (2003).

Table 2. Safeguards equipment for ESFR simplified design layout

Measurement Point	Nuclear Material Form	Measurement Technique	Measurement Technology
Portal 1	Spent Fuel Assembly	Gamma + Neutron Gross Counts → Burnup → Cm → Pu	1 Fission Chambers 1 Ionization Chambers
Portal 2	Spent Fuel Element	Gross Neutron → Cm → Pu	He-3 Collar, Passive
Portal 7	Fresh U/TRU Fuel Element	Gross Neutron → Cm → Pu	He-3 Collar, Passive
Portal 8	Fresh U/TRU Fuel Assembly	Gross Neutron → Cm → Pu	He-3 Collar, Passive

At Portal 1 the burnup (BU) of the spent fuel assembly is determined. One fission chamber and the one ionization chamber are used to count total neutrons and total gammas. These measurements are used to confirm the declared burnup of the spent fuel assembly. At Portal 2 the neutron activity is measured to determine the ^{244}Cm in the spent fuel pin which is used to determine the concentration of plutonium using the Cm-Pu ratio. Similarly at Portals 7 and 8 the ^{244}Cm is being counted using a He-3 Collar. The recycled fuel exiting Portals 7 and 8 still has ^{244}Cm and long-lived actinides in the fuel.

4.3 RELIABILITY CRITERIA

Safeguards components have a goal of being designed with a minimum *MTBF* of 150 months (Doyle 2008). Assuming *MTTR* is very small compared to *MTTF* and *MTTD* is instant, a *MTBF* of 150 months can be assumed to be equal to a *MTTF* of 150 months. When a *MTTF* for a component is not available a 150 month *MTTF* will be assumed.

For the overall system, a goal of 2 years or 24 months *MTTF* will be the user defined reliability criteria. The overall system consists of Portal 1, Portal 2, Portal 7, and Portal 8 as depicted in Fig. 16.

4.4 RELIABILITY ANALYSIS

The overall system reliability is modeled by assuming the probabilistic reliability of each system is independent of the probabilistic reliability of every other system, as if the subsystems for Portals 1, 2, 7, and 8 are in series. If any one subsystem fails, then the whole system fails. This is calculated using Eq. 4.1 where $R_T(t)$ is the reliability for all portal subsystems, $R_1(t)$ is the reliability for Portal 1 subsystem, $R_2(t)$ is the reliability for Portal 2 subsystem, $R_7(t)$ is the reliability for Portal 7 subsystem, and $R_8(t)$ is the reliability for Portal 8 subsystem. The reliability of the system is

$$R_T(t) = R_1(t) \times R_2(t) \times R_7(t) \times R_8(t). \tag{4.1}$$

The individual subsystems are first modeled with the minimum equipment needed and without redundancies in equipment. The *MTTF* for each component and each "link" in the chain are analyzed to identify the weakest points in the "chain". To demonstrate the design process, the reliability is improved by adding redundancies until the overall system reliability meets the specified reliability criteria.

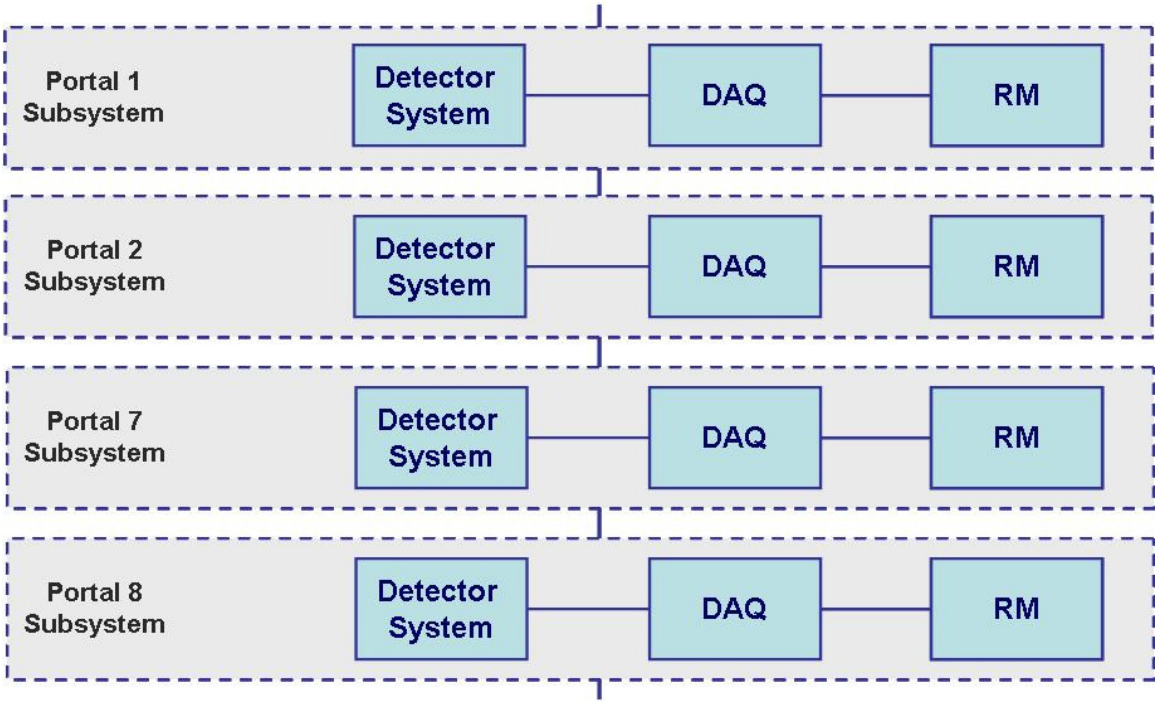

Figure 17. Overall system -- portal subsystems in series

Fig. 17 represents the overall safeguards system considered in this analysis. The remote monitor (RM) is pictured for completeness but is not considered a critical component and therefore is not included in the reliability analysis of each subsystem. The data acquisition (DAQ) component would continue to receive and store information even if the RM was inoperable.

4.4.1 PORTAL 1 SUBSYSTEM

To calculate and confirm the reported burnup, total neutrons and total gammas are counted for the spent fuel assemblies entering Portal 1. A minimum subsystem for Portal 1 consists of one fission chamber, one ionization chamber and one DAQ unit in series.

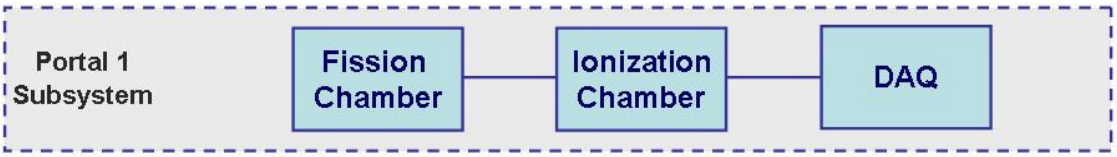

Figure 18. Portal 1 subsystem -- no redundancies

Fig. 18 does not represent the physical arrangement of the detectors; rather it illustrates that the failure of one detector or DAQ unit would constitute a failure or loss of knowledge for the subsystem. The MTTF for a fission chamber is 2556.75 days or 84 months, which equates to a λ_{FC} of 0.000391122 chance of failure per day. This number is based on a 7 year lifetime of fission chambers as reported by PHOTONIS (2007). The MTTF of an ionization chamber is 2435 days or 80 months, which also equates to a λ_{IC} of 0.000410678 chance of failure per day based on a 15% failure rate per year reported in (Emel'yanov et al. 1977). The MTTF for a DAQ unit is reasonably estimated to be 4565.625 days or 150 months as discussed in 4.3. The λ_{DAQ} for a 150-month MTTF of the DAQ unit is 0.000219028 chance of failure per day. Eq. 4.2 is used to calculate the reliability of the Portal 1 subsystem, $R(t)_{Portal1}$:

$$R(t)_{Portal1} = R(t)_{FC} \times R(t)_{IC} \times R(t)_{DAQ} = e^{-\lambda_{FC}*t} \times e^{-\lambda_{IC}*t} \times e^{-\lambda_{DAQ}*t}; \quad (4.2)$$

$$MTTF_{Portal1} = \int_0^\infty R(t)_{Portal1}\, dt. \quad (4.3)$$

$R(t)_{FC}$ is the reliability of the fission chamber, the $R(t)_{IC}$ is the reliability of the ionization chamber and the $R(t)_{DAQ}$ is the reliability of the DAQ unit. The MTTF for Portal 1 subsystem is 979.60 days or 32.18 months and is calculated by Eq. 4.3.

4.4.2 PORTAL 2, PORTAL 7, PORTAL 8 SUBSYSTEMS

Portals 2, 7, and 8 subsystems all use the same technology; a neutron detector using He-3 tubes and a DAQ unit. The He-3 collar and DAQ unit are set up in series as shown in Fig. 19. An He-3 collar has one complete ring of He-3 tubes and is represented by the "He-3 Collar" box in Fig. 19.

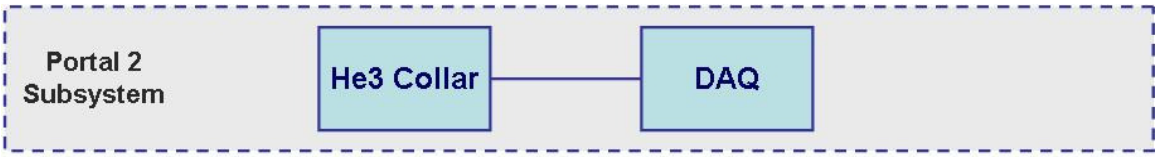

Figure 19. Portal 2 subsystem -- no redundancies

Eq. 4.4 shows the $R(t)_{Portal2}$ for the Portal 2 subsystem and also is equivalent to the Portal 7 and 8 subsystems. In future equations results for Portal 2 subsystem will only be calculated but are equivalent to the results for Portal 7 and Portal 8. The MTTF for a He-3 collar is assumed to be 150 months, which equates to a λ_{He3} of 0.000219028 chance of failure per day. The *MTTF* for a DAQ unit is estimated to be 150 months or 4565.625 days. The λ_{DAQ} for a 150-month MTTF of the DAQ unit is 0.000219028 chance of failure per day. The reliability of Portal 2 is:

$$R(t)_{Portal\ 2} = R(t)_{He3} \times R(t)_{DAQ} = e^{-\lambda_{He3}*t} \times e^{-\lambda_{DAQ}*t}, \tag{4.4}$$

and

$$MTTF_{Portal2} = \int_0^\infty R(t)_{Portal2}\, dt. \tag{4.5}$$

$R(t)_{He3}$ is the reliability of the He-3 collar. The *MTTF* for Portal 2 (also Portal 7 and Portal 8) subsystems is 2282.81 days or 75 months and is calculated using Eq. 4.5**.**

4.4.3 SUMMARY OF INITIAL ANALYSIS

Each subsystem must function for the entire system to function; thus, the reliability of the entire system is modeled as the probability of occurrence of four independent events in series.

The entire system (Fig. 20) reliability, $R_T(t)$, can be calculated as

$$R_T(t) = R_1(t) \times R_2(t) \times R_7(t) \times R_8(t). \tag{4.6}$$

As before, the reliability of the system is determined by

$$MTTF_{system} = \int_0^\infty R(t)_{system}\, dt. \tag{4.7}$$

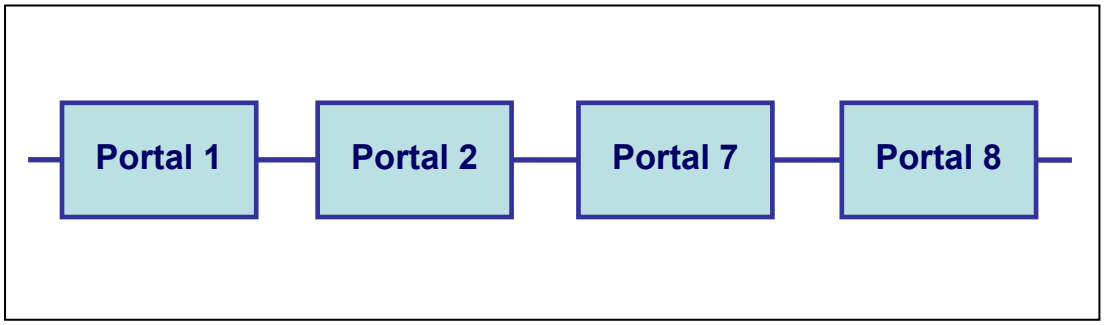

Figure 20. Entire system in series

For the values previously presented, the overall MTTF for all the entire system is 428.27 days or 14.07 months. This combines Portal 1, 2, 7 and 8 in series as seen in Fig. 17 and Fig. 20. The overall MTTF does not meet the goal of 24 months for the entire system. Following the process outlined in Sublevel 3.1, redundancies must be added to meet the reliability criteria.

4.5 RELIABILITY DESIGN – EQUIPMENT REDUNDANCIES

To meet the overall reliability criteria goal of 24 months for the system, redundancies in equipment must be added. In the absence of cost information, redundancies are added so that the number of overall components in a system is minimized, as opposed to the highest improvement-per-cost added. This cycle is iterated until the desired system reliability is met.

4.5.1 PORTAL 1 SUBSYSTEM

The Portal 1 subsystem consists of four redundant subsystems (Fig. 21).

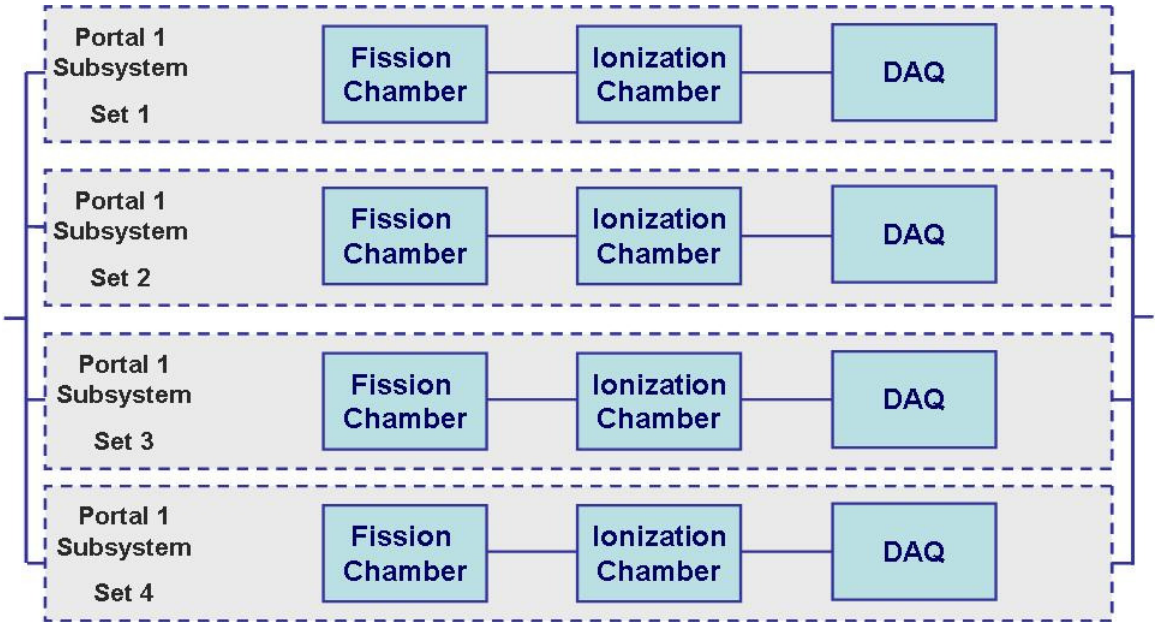

Figure 21. Portal 1 with four redundant subsystems in parallel

Eqs. 4.8 and 4.9 are used to calculate the reliability of the four subsystems in parallel:

$$R(t)_{Portal\ 1} = 1-\left[1-R(t)_{Set1}\right]\times\left[1-R(t)_{Set2}\right]\times\left[1-R(t)_{Set3}\right]\times\left[1-R(t)_{Set4}\right], \quad (4.8)$$

and

$$R(t) = 1 - \left(1 - e^{-\lambda_{Set1} * t}\right) \times \left(1 - e^{-\lambda_{Set2} * t}\right) \times \left(1 - e^{-\lambda_{Set3} * t}\right) \times \left(1 - e^{-\lambda_{Set4} * t}\right). \quad (4.9)$$

The reliability of Set 1, $R(t)_{Set1}$, is equal to the reliability of the Portal 1 subsystem calculated in Sublevel 4.4.1. $R(t)_{Set1}$ and $R(t)_{Set2}$,$R(t)_{Set3}$ and $R(t)_{Set4}$ are identical and the reliability calculated in Sublevel 4.4.1 can be used for all subsystem sets:

$$MTTF_{Portal1} = \int_0^\infty R(t)_{Portal1}\, dt. \quad (4.10)$$

The *MTTF* for Portal 1 subsystem is 2040.83 days or 67.05 months and is calculated using Eq. 4.10. The *MTTF* of Portal 1 with four redundant subsystems is about double the previous *MTTF* of 32.18 months.

4.5.2 PORTAL 2, PORTAL 7, PORTAL 8 SUBSYSTEMS

Portal 2, 7, and 8 subsystems consist of two redundant subsystems. Portal 2 is pictured in Fig. 22.

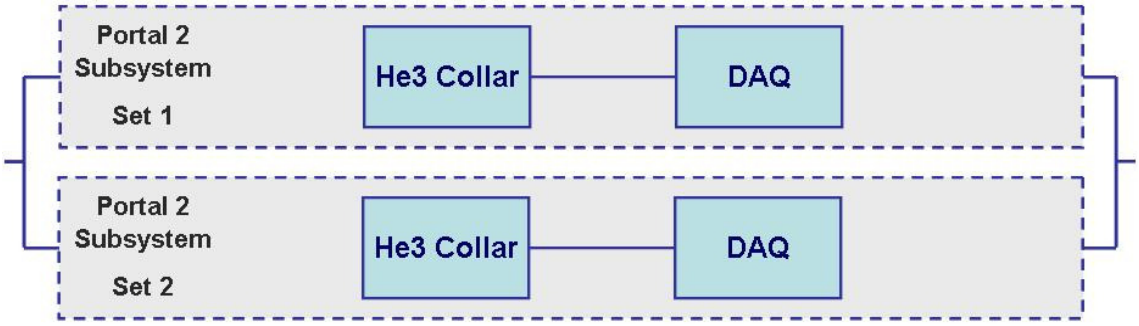

Figure 22. Portal 2 with two redundant subsystems in parallel

Eq. 4.11 and 4.12 are used to calculate the reliability of two subsystems in parallel for Portal 2, $R(t)_{Portal2}$:

$$R(t)_{Portal\ 2} = 1 - \left[1 - R(t)_{Set1}\right] \times \left[1 - R(t)_{Set2}\right]; \quad (4.11)$$

$$R(t)_{Portal2} = 1-\left(1-e^{-\lambda_{Set1}*t}\right)\times\left(1-e^{-\lambda_{Set2}*t}\right); \quad (4.12)$$

$$MTTF_{Portal2} = \int_0^\infty R(t)_{Portal2}\, dt. \quad (4.13)$$

The *MTTF* for Portal 2, 7 and 8 subsystems is 3424.22 days or 112.5 months and is calculated using Eq. 4.13. The *MTTF* of Portal 2, 7 and 8 with two redundant subsystems is 1.5 times the previous *MTTF* of 75 months.

4.5.3 SUMMARY OF ANALYSIS WITH EQUIPMENT REDUNDANCIES

Again, each subsystem must function for the entire system to function; thus, the reliability of the entire system is modeled as the probability of occurrence of four independent events in series:

$$R_T(t) = R_1(t)\times R_2(t)\times R_7(t)\times R_8(t). \quad (4.14)$$

As before, the reliability of the system is determined by:

$$MTTF_{system} = \int_0^\infty R(t)_{system}\, dt. \quad (4.15)$$

For the values previously presented, the overall *MTTF* for the entire system is 732.01 days or 24.05 months. This combines Portals 1, 2, 7 and 8 in series as originally seen in Fig. 17. The *MTTF* of 24.05 months meets the design goal of 24 months *MTTF* for the entire system.

4.6 EVALUATION

Table 3 summarizes the calculation results for the designs with and without redundancies.

Table 3. Results summary

Subsystem	Component Group	MTTF without Redundancies (months)	MTTF with Redundancies (months)
Portal 1	Fission Chamber	84	84
	Ionization Chamber	80	80
	DAQ	150	150
	Overall	*32.18*	*67.05*
Portal 2/7/8	He3 Detector	150	150
	DAQ	150	150
	Overall	*75*	*112.5*
Overall System		**14.07 months**	**24.05 months**

From Table 3, it is clear that Portal 1 represents the least reliable link in the system and hence, in the proliferation resistance model, a weakness. By adding a redundancy of four subsystems to Portal 1, this subsystem is made more reliable by a factor of approximately 2. By adding a redundancy of two subsystems to Portal 2, 7 and 8, each portal is made more reliable by a factor of 1.5. The entire system is made more reliable by a factor of 1.7. After adding sufficient redundancies, the design criteria of 24 months *MTTF* was met and the design accepted.

Obviously cost, space and other constraints limit the number of redundancies which can be installed; hence, an actual system would be designed to achieve the desired system reliability at the minimum cost. Instead, the approach used here, in the absence of cost information, was simply to minimize the number of components. This is only one safeguards design that meets the reliability criteria but was the design that had the fewest

components and met the reliability criteria. Appendix B shows other possible combinations of redundancies for the overall system.

4.7 DISCUSSION

This reliability process only considers reliability and not other considerations such as cost. It is clear that the system has doubled the number of components and therefore doubles the cost of the components but did not double the reliability. This is a consideration safeguards designers will need to make as they design a system.

Also, designs that focus safeguards on main material entrances and exits could be part of the design criteria. For the ESFR, a designer could add more redundancies to Portal 1 and Portal 8. While every portal presents an opportunity for proliferation, it is up to the safeguards designer to decide if one portal would require more redundancy than another.

During analysis it may be determined that component cost becomes a dominating factor. Additionally, it may be discovered that spending more money for a more reliable part (or cost-benefit) would reduce the number of redundancies needed in a system.

4.8 SUMMARY

The UMS for the ESFR FCF was initially designed with no redundancies. Upon performing the reliability analysis of that design, it was identified that the reliability criteria were not met. The design process used here was to iteratively add a redundancy to minimize components but reach the reliability criteria and then repeat the analysis to identify the new *MTTF* for the system. Eventually, when the desired *MTTF* was met by the design, the iteration was stopped and the design accepted. This approach does not consider the cost of components. Alternatively, a system designer with cost information may choose to add redundancies based on an improvement-per-unit-cost basis as opposed to simply the improvement-per-component basis used here.

CHAPTER V
USE OF THE RELIABILITY PROCESS IN PROLIFERATION RESISTANCE ASSESSMENT

Proliferation resistance studies as discussed in Sublevel 2.4 can be qualitative and/or quantitative. Many proliferation resistance studies and methods rely on expert judgment. The proliferation resistance assessments that use fault-tree, logic-tree or success-tree analysis (e.g. Golay 2001; Cojazzi et al. 2004; Coles and Zentner 2007) attempt to move away from qualitative analysis and toward quantitative analysis.

As demonstrated in Chapter IV, the reliability process yields a quantitative result in the form of a *MTTF* for the system. In the fault-tree modeling the different proliferation pathways for specific diversions are modeled (Coles and Zentner 2007). One of the basic events in fault-tree models for proliferation pathways is the chance that the IAEA safeguards (e.g. detectors) are not operating and have failed due to random chance during the nuclear material diversion. This reliability process provides a way for analysts to find a quantitative answer to this basic event. The reliability process also offers a way to do a time-dependent fault-tree analysis.

The reliability process was demonstrated on the ESFR for detectors and DAQ units. This process could additionally be applied to containment and surveillance (C/S). For various proliferation pathways the chance that different IAEA safeguards are not operating need to be known for the analysis. The quantitative result from the reliability process would be an improvement versus an expert judgment derived number.

Many proliferation resistance studies look at a Nation or State covertly diverting material from an IAEA safeguarded facility. Another consideration is for a State to prevent other States or individuals from diverting or stealing nuclear material from their facility. To detect and deter this, States use their own detectors, surveillance and physical protection of the facility. The reliability process demonstrated in this research can be applied to the equipment and sensors used for the physical protection of a facility. This equipment is important to a facility and analyzing its reliability would help a nuclear facility improve its protection.

Overall there are many areas the reliability process demonstrated in this research can be applied to proliferation resistance studies.

CHAPTER VI
CONCLUSIONS AND RECOMMENDATIONS

6.1 CONCLUSIONS

A reliability engineering approach to probabilistic safeguards system analysis and design can be used to reach meaningful conclusions regarding the proliferation resistance of a UMS. The methods developed in this research provide analysts and designers alike a process to follow to evaluate the reliability of a UMS.

A UMS was created for the ESFR FCF to facilitate demonstration of the new approach. The UMS emphasized the technologies and generalized hardware expected to be present at key measurement points but exact hardware specification was outside the scope of this study.

The ESFR FCF UMS was analyzed to demonstrate the analysis and design processes that an analyst or designer would go through when evaluating/designing the proliferation resistance component of a safeguards system. When comparing the *MTTF* for the system without redundancies, it is apparent that redundancies were necessary to achieve a design without routine failures.

6.2 RECOMMENDATIONS

Quality engineering concepts and the approach developed here should be integrated into broader probabilistic proliferation resistance models for facilities utilizing UMS and RMS.

Specific safeguards system reliability data are not and should not be published in the open literature but should be available to the IAEA for reliability analysis. Approximations or publicly available failure rates should be used in published research instead.

6.3 FUTURE WORK

Extensions to this work could include additional detail in the reliability modeling, improvement on the safeguards design considered for the ESFR FCF, and the discussion of the method with respect to additional facilities to be built or already operating and using UMS.

The IAEA and the international safeguards and non-proliferation (IS&NP) community could incorporate the reliability engineering approach to UMS design for upcoming fast reactor safeguards system designs. The approach developed here suffices as a primer for an IAEA engineer designing UMS in general and for pyroprocessing.

REFERENCES

Argonne National Laboratory. ESFR pyroprocessing facility description and preliminary safeguards approach for PR&PP demonstration study. Argonne, IL: ANL; 2006.

Budlong Sylvester K, Eller P, Veal K, Thomas K, Lee TK, Menlove H, Longmire V, Russo P. International safeguards for pyroprocessing: options for evaluation. LA-UR-03-0986. Los Alamos, NM: Los Alamos National Laboratory; 2003.

Charlton WS, LeBouf RF, Gariazzo C, Ford DG, Beard C, Landsberger S, Whitaker M. Proliferation resistance assessment methodology for nuclear fuel cycles. Nuclear Technology 157:143-56; 2007.

Cojazzi GGM, Renda G, Contini S. Probabilistic safety assessment and management. In: Spitzer C, Schmocker U, Dang VN, eds. Qualitative and quantitative analysis of safeguards logic trees. New York: Springer; 2004: 1083-1088.

Coles G, Zentner M. Application of the event tree/fault tree modeling approach to the evaluation of proliferation resistance. Proceedings of the ASME International Mechanical Engineering Congress and Exposition. New York: Amerian Society of Mechanical Engineers; 14:139-147; 2007.

Doyle, JE. Nuclear safeguards, security, and nonproliferation. Oxford, UK: Butterworth-Heinmann; 2008.

Emel'yanov IY, Alekseev VI, Lipin VF, Ol'shevskii VP, Postnikov VV, Rybakov YV, Steklov VO. Small in-reactor high-temperature ionization chamber. Atomnaya Energiya 43:41-43; 1977.

Generation IV International Forum Proliferation Resistance and Physical Protection Evaluation Methodology Working Group. PR&PP evaluation: ESFR full system case study final report GIF/PRPPWG/2009/002. Paris, France: GIF; 2009.

Golay M. Measures of safeguards, barriers and nuclear reactor concept/fuel cycle resistance to nuclear weapons proliferation. Trans. American Nuclear Society 85:83-84; 2001.

Greneche D. A practical tool to assess the proliferation resistance of nuclear systems: The SAPRA methodology. European Safeguards Research and Development Association Bulletin 39:41-49; 2008.

Ham H. An integrated methodology for quantitative assessment of proliferation resistance of advanced nuclear systems using probabilistic methods. Boston, MA: MIT; 2005.

Hill J. Logic trees and integrated safeguards. ASAP-9802, Barton: Australian Safeguards and Non-Proliferation Office; 1998.

International Atomic Energy Agency. IAEA safeguards glossary. IAEA International Nuclear Verification Series No. 3, Vienna: IAEA; 2001.

International Atomic Energy Agency. Model protocol additional to the agreement(s) between state(s) and the IAEA for the application of safeguards. Information Circular INFCIRC/540, Vienna, Austria: IAEA; 1997.

International Atomic Energy Agency. The structure and content of agreements between the agency and states required in connection with the treaty on the non-proliferation of nuclear weapons. Information Circular INFCIRC/153, Vienna, Austria: IAEA; 1972.

Ko WI, Kim HD, Yang MS, Park HS. Electrical circuit model for quantifying the proliferation resistance of nuclear fuel cycles. Annals of Nuclear Energy 27:1399-425; 2000.

Mitra A. Fundamentals of quality control and improvement, 2nd ed. Upper Saddle River, NJ: Prentice Hall; 1998.

PHOTONIS. PHOTONIS Neutron & Gamma Detectors Catalog [online]. Available at: http://www.photonis.com/upload/industryscience/pdf/neutrongamma/D-DNG-CAT2007_web.pdf; 2007. Accessed 1 February 2011.

Rinard PM, Menlove HO. Application of Curium Measurements for safeguarding at reprocessing plants, study 1: High-level liquid waste and study 2: Spent fuel assemblies and leached hulls. LA-13134-MS, Los Alomos, NM: Los Alamos National Laboratory; 1996.

Sentell DS Jr. A quantitative assessment of nuclear weapons proliferation risk utilizing probabilistic methods. Boston, MA: MIT; 2002.

Yue M, Cheng L, Bari R. A markov model approach to proliferation-resistance assessment of nuclear energy systems. Nuclear Technology 162:26-44; 2008.

APPENDIX A

In Fig. 23 on the next page, is a detailed material flow sheet for the ESFR pyroprocessing facility. In the figure HM refers to heavy metal and refers to U and TRU combined.

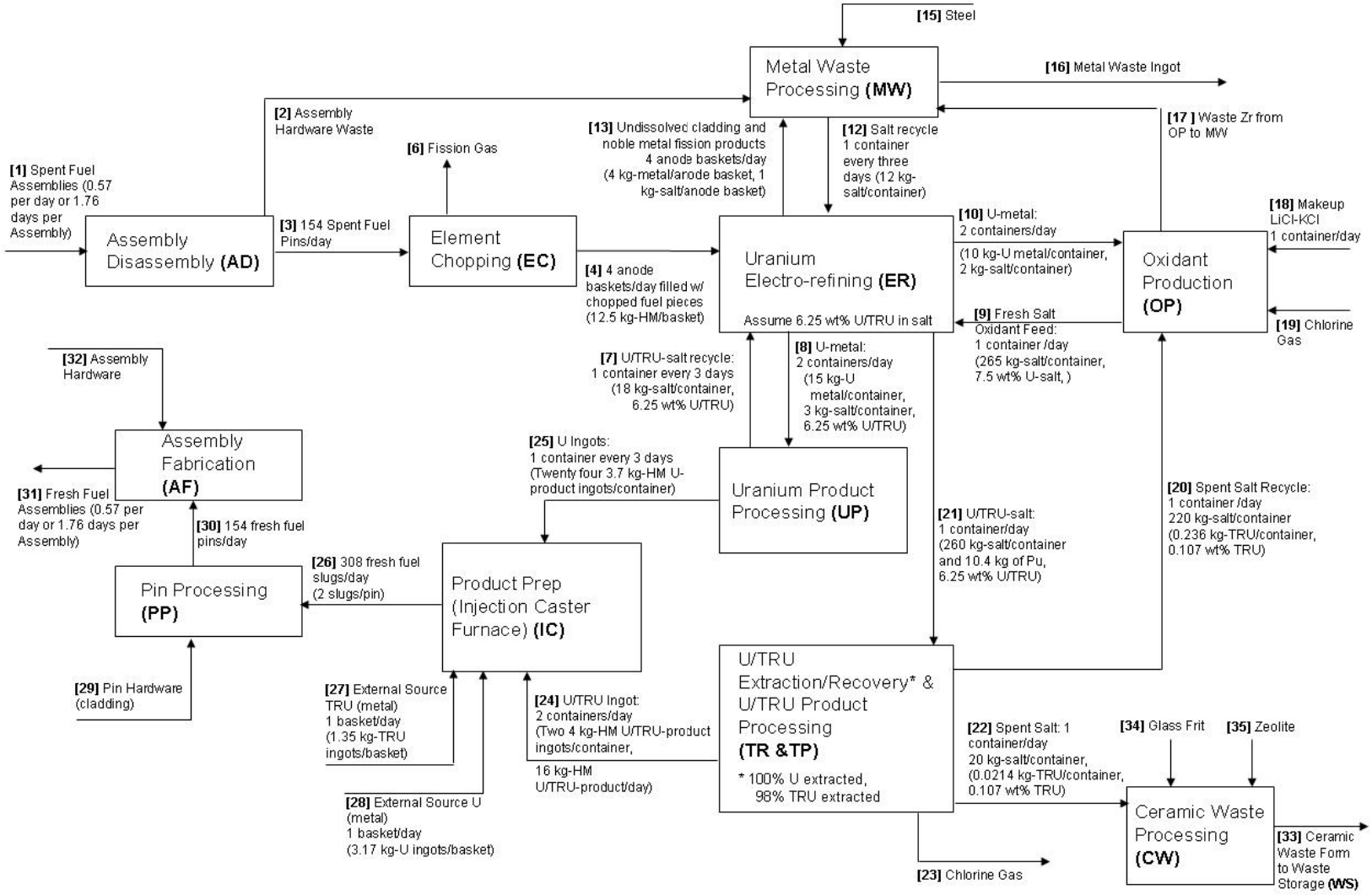

Figure 23. ESFR pyroprocessing facility material flow

APPENDIX B

The table below gives all possible combinations of redundancies for the overall system. Each portal has the minimum of one subsystem up to a maximum of four redundant subsystems. P1 is Portal 1; P2 is Portal 2, etc. Tot# is the total number of components for that particular system. Highlighted in yellow are systems that meet the 24 month reliability criteria goal. The system used in this research has a box around it signifying it has the least number of components while still meeting the reliability criteria goal.

Table 4. Number of redundancies at each portal

P1	P2	P3	P4	Tot#	MTTF (months)
1	1	1	1	9	14.07035176
1	1	1	2	11	15.00893389
1	1	1	3	13	15.38205427
1	1	1	4	15	15.59135793
1	1	2	1	11	15.00893389
1	1	2	2	13	16.08168475
1	1	2	3	15	16.51081065
1	1	2	4	17	16.75220039
1	1	3	1	13	15.38205427
1	1	3	2	15	16.51081065
1	1	3	3	17	16.96346613
1	1	3	4	19	17.21837521
1	1	4	1	15	15.59135793
1	1	4	2	17	16.75220039
1	1	4	3	19	17.21837521
1	1	4	4	21	17.48106218
1	2	1	1	11	15.00893389
1	2	1	2	13	16.08168475
1	2	1	3	15	16.51081065
1	2	1	4	17	16.75220039
1	2	2	1	13	16.08168475
1	2	2	2	15	17.31958763
1	2	2	3	17	17.81834544
1	2	2	4	19	18.09980751
1	2	3	1	15	16.51081065
1	2	3	2	17	17.81834544
1	2	3	3	19	18.34668079
1	2	3	4	21	18.64522152
1	2	4	1	17	16.75220039
1	2	4	2	19	18.09980751
1	2	4	3	21	18.64522152
1	2	4	4	23	18.9536388
1	3	1	1	13	15.38205427
1	3	1	2	15	16.51081065
1	3	1	3	17	16.96346613
1	3	1	4	19	17.21837521

P1	P2	P3	P4	Tot#	MTTF (months)
1	3	2	1	15	16.51081065
1	3	2	2	17	17.81834544
1	3	2	3	19	18.34668079
1	3	2	4	21	18.64522152
1	3	3	1	17	16.96346613
1	3	3	2	19	18.34668079
1	3	3	3	21	18.9073051
1	3	3	4	23	19.2245275
1	3	4	1	19	17.21837521
1	3	4	2	21	18.64522152
1	3	4	3	23	19.2245275
1	3	4	4	25	19.55257612
1	4	1	1	15	15.59135793
1	4	1	2	17	16.75220039
1	4	1	3	19	17.21837521
1	4	1	4	21	17.48106218
1	4	2	1	17	16.75220039
1	4	2	2	19	18.09980751
1	4	2	3	21	18.64522152
1	4	2	4	23	18.9536388
1	4	3	1	19	17.21837521
1	4	3	2	21	18.64522152
1	4	3	3	23	19.2245275
1	4	3	4	25	19.55257612
1	4	4	1	21	17.48106218
1	4	4	2	23	18.9536388
1	4	4	3	25	19.55257612
1	4	4	4	27	19.89201478
2	1	1	1	12	16.47058824
2	1	1	2	14	17.77150917
2	1	1	3	16	18.2970297
2	1	1	4	18	18.59394369
2	1	2	1	14	17.77150917
2	1	2	2	16	19.29555896
2	1	2	3	18	19.91665469
2	1	2	4	20	20.26896596
2	1	3	1	16	18.2970297
2	1	3	2	18	19.91665469
2	1	3	3	20	20.57906459
2	1	3	4	22	20.9554221
2	1	4	1	18	18.59394369
2	1	4	2	20	20.26896596
2	1	4	3	22	20.9554221
2	1	4	4	24	21.34580199
2	2	1	1	14	17.77150917
2	2	1	2	16	19.29555896
2	2	1	3	18	19.91665469
2	2	1	4	20	20.26896596
2	2	2	1	16	19.29555896
2	2	2	2	18	21.10552764
2	2	2	3	20	21.85085921

P1	P2	P3	P4	Tot#	MTTF (months)
2	2	2	4	22	22.27565236
2	2	3	1	18	19.91665469
2	2	3	2	20	21.85085921
2	2	3	3	22	22.65075993
2	2	3	4	24	23.10754847
2	2	4	1	20	20.26896596
2	2	4	2	22	22.27565236
2	2	4	3	24	23.10754847
2	2	4	4	26	23.58313993
2	3	1	1	16	18.2970297
2	3	1	2	18	19.91665469
2	3	1	3	20	20.57906459
2	3	1	4	22	20.9554221
2	3	2	1	18	19.91665469
2	3	2	2	20	21.85085921
2	3	2	3	22	22.65075993
2	3	2	4	24	23.10754847
2	3	3	1	20	20.57906459
2	3	3	2	22	22.65075993
2	3	3	3	24	23.51145038
2	3	3	4	26	24.00399027
2	3	4	1	22	20.9554221
2	3	4	2	24	23.10754847
2	3	4	3	26	24.00399027
2	3	4	4	28	24.5176081
2	4	1	1	18	18.59394369
2	4	1	2	20	20.26896596
2	4	1	3	22	20.9554221
2	4	1	4	24	21.34580199
2	4	2	1	20	20.26896596
2	4	2	2	22	22.27565236
2	4	2	3	24	23.10754847
2	4	2	4	26	23.58313993
2	4	3	1	22	20.9554221
2	4	3	2	24	23.10754847
2	4	3	3	26	24.00399027
2	4	3	4	28	24.5176081
2	4	4	1	24	21.34580199
2	4	4	2	26	23.58313993
2	4	4	3	28	24.5176081
2	4	4	4	30	25.05368647
3	1	1	1	15	17.55986317
3	1	1	2	17	19.04631029
3	1	1	3	19	19.65121225
3	1	1	4	21	19.99411429
3	1	2	1	17	19.04631029
3	1	2	2	19	20.80768653
3	1	2	3	21	21.53176946
3	1	2	4	23	21.94412955
3	1	3	1	19	19.65121225
3	1	3	2	21	21.53176946
3	1	3	3	23	22.30806374
3	1	3	4	25	22.75099967
3	1	4	1	21	19.99411429

P1	P2	P3	P4	Tot#	MTTF (months)
3	1	4	2	23	21.94412955
3	1	4	3	25	22.75099967
3	1	4	4	27	23.21188127
3	2	1	1	17	19.04631029
3	2	1	2	19	20.80768653
3	2	1	3	21	21.53176946
3	2	1	4	23	21.94412955
3	2	2	1	19	20.80768653
3	2	2	2	21	22.9280397
3	2	2	3	23	23.81034187
3	2	2	4	25	24.31561884
3	2	3	1	21	21.53176946
3	2	3	2	23	23.81034187
3	2	3	3	25	24.76326604
3	2	3	4	27	25.3102607
3	2	4	1	23	21.94412955
3	2	4	2	25	24.31561884
3	2	4	3	27	25.3102607
3	2	4	4	29	25.88196628
3	3	1	1	19	19.65121225
3	3	1	2	21	21.53176946
3	3	1	3	23	22.30806374
3	3	1	4	25	22.75099967
3	3	2	1	21	21.53176946
3	3	2	2	23	23.81034187
3	3	2	3	25	24.76326604
3	3	2	4	27	25.3102607
3	3	3	1	23	22.30806374
3	3	3	2	25	24.76326604
3	3	3	3	27	25.79564489
3	3	3	4	29	26.3897457
3	3	4	1	25	22.75099967
3	3	4	2	27	25.3102607
3	3	4	3	29	26.3897457
3	3	4	4	31	27.01185715
3	4	1	1	21	19.99411429
3	4	1	2	23	21.94412955
3	4	1	3	25	22.75099967
3	4	1	4	27	23.21188127
3	4	2	1	23	21.94412955
3	4	2	2	25	24.31561884
3	4	2	3	27	25.3102607
3	4	2	4	29	25.88196628
3	4	3	1	25	22.75099967
3	4	3	2	27	25.3102607
3	4	3	3	29	26.3897457
3	4	3	4	31	27.01185715
3	4	4	1	27	23.21188127
3	4	4	2	29	25.88196628
3	4	4	3	31	27.01185715
3	4	4	4	33	27.66400805
4	1	1	1	18	18.21019771
4	1	1	2	20	19.81381306
4	1	1	3	22	20.46928721

P1	P2	P3	P4	Tot#	MTTF (months)
4	1	1	4	24	20.84160381
4	1	2	1	20	19.81381306
4	1	2	2	22	21.72713478
4	1	2	3	24	22.51783881
4	1	2	4	26	22.96922853
4	1	3	1	22	20.46928721
4	1	3	2	24	22.51783881
4	1	3	3	26	23.36826771
4	1	3	4	28	23.85476476
4	1	4	1	24	20.84160381
4	1	4	2	26	22.96922853
4	1	4	3	28	23.85476476
4	1	4	4	30	24.36194896
4	2	1	1	20	19.81381306
4	2	1	2	22	21.72713478
4	2	1	3	24	22.51783881
4	2	1	4	26	22.96922853
4	2	2	1	22	21.72713478
4	2	2	2	24	24.0494732
4	2	2	3	26	25.02202516
4	2	2	4	28	25.58063992
4	2	3	1	24	22.51783881
4	2	3	2	26	25.02202516
4	2	3	3	28	26.07655142
4	2	3	4	30	26.68381413
4	2	4	1	26	22.96922853
4	2	4	2	28	25.58063992
4	2	4	3	30	26.68381413
4	2	4	4	32	27.32003469
4	3	1	1	22	20.46928721
4	3	1	2	24	22.51783881
4	3	1	3	26	23.36826771
4	3	1	4	28	23.85476476
4	3	2	1	24	22.51783881
4	3	2	2	26	25.02202516
4	3	2	3	28	26.07655142
4	3	2	4	30	26.68381413
4	3	3	1	26	23.36826771
4	3	3	2	28	26.07655142
4	3	3	3	30	27.22387215
4	3	3	4	32	27.88642619
4	3	4	1	28	23.85476476
4	3	4	2	30	26.68381413
4	3	4	3	32	27.88642619
4	3	4	4	34	28.58203415
4	4	1	1	24	20.84160381
4	4	1	2	26	22.96922853
4	4	1	3	28	23.85476476
4	4	1	4	30	24.36194896
4	4	2	1	26	22.96922853
4	4	2	2	28	25.58063992
4	4	2	3	30	26.68381413
4	4	2	4	32	27.32003469
4	4	3	1	28	23.85476476

4	4	3	2	30	26.68381413
P1	**P2**	**P3**	**P4**	**Tot#**	**MTTF (months)**
4	4	3	3	32	27.88642619
4	4	3	4	34	28.58203415
4	4	4	1	30	24.36194896
4	4	4	2	32	27.32003469
4	4	4	3	34	28.58203415
4	4	4	4	36	29.31323283

VITA

Name: Lillian Marie Cronholm

Address: Nuclear Engineering Department
3133 TAMU
College Station, TX 77843-3133

Email Address: lillian.marie at gmail dot com

Education: B.S., Radiological Health Engineering, Texas A&M University, 2005
M.S., Health Physics, Texas A&M University, 2011