SAND2019-6328C

SYSTEMS THEORETIC PROCESS ANALYSIS TOOLS FOR NUCLEAR MATERIALS SAFEGUARDS EVALUATION

Z.S. Beauvais[1], W.S. Charlton[1] and A. D. Williams[2]*

ABSTRACT:

Recent advancements in hazard analysis techniques and capabilities have proven insightful in a variety of industries and applications. One of these techniques is Systems Theoretic Process Analysis (STPA). This technique has been applied to evaluate complex systems in the aerospace, automotive, and nuclear power sectors. Recently, it has been applied to evaluate interfaces between safety, security and safeguards in the context of nuclear material transportation. From an evaluation of the literature, STPA has not been applied to evaluate the fundamental activities involved in nuclear material accountability and safeguards implementation for nuclear material process facilities. This work presents a first of a kind, STPA evaluation of the causes of nuclear material accountability and safeguards anomalies that might be encountered while operating a mixed oxide (MOX) reprocessing facility. The STPA evaluates potential upset conditions that could lead to false positive or false negative indications of diversion in a safeguards approach. A computational systems model of a hypothetical but representative MOX reprocessing facility was developed and used to facilitate quantitative evaluation of various process upsets identified through the STPA. Based on the results of the work, STPA shows promise as a technique for evaluating vulnerabilities in a safeguards approach or for identifying the causes of safeguards anomalies. Specifically, STPA could be used to resolve safeguards anomalies through a better understanding of signature patterns associated with specific process upsets.

INTRODUCTION:

As described in Engineering a Safer World, STPA is a hazard analysis technique that builds upon the System Theoretic Accident Model and Processes (STAMP) [1]. In contrast to other accident analysis models that are built upon preventing failures, often through a reliability framework, STAMP is built upon a concept of enforcing behavioral safety constraints, through a systems analysis framework. STPA stemmed from the need to assess new types of causal factors that stem from STAMP.

STPA distinguishes itself from the reliability-based models in its ability to include "design errors, including software flaws; component interaction accidents; cognitively complex human decision-making errors; and social, organizational and management factors contributing to accidents [1]." STAMP has three basic concepts: safety constraints, hierarchical safety control structures, and process models [2]. All of these elements are evident in the structure of an STPA. The key steps for performing an STPA are described in Table 1 [3, 2].

[1] University of Texas at Austin, beauvaiz@utexas.edu
[2] Sandia National Laboratories
*SAND2019-XXXX C. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Table 1: Key steps necessary for an STPA.

1	State the system mission (describe the desired set of outcomes for the system to achieve).
2	State system losses of concern (describe broad categories of undesired outcomes related to the system attempting to achieve its mission).
3	Determine system states of increased risk (use state-space characteristics to describe how the system can exhibit increasingly risky behavior, moving it closer to experiencing an unacceptable loss).
4	Define system requirements (describe the necessary conditions for the system to avoid states of increased risk).
5	Derive control actions necessary to meet system requirements (identify control actions for each controller within the sociotechnical system model necessary related to meeting the higher-level system requirements).

STPA has been applied to numerous applications in the aerospace industry [4, 5]. It has also been applied to specifically evaluate digital instrumentation and control systems in nuclear power plants and proposed for use in evaluating safety control strategies in non-reactor fuel cycle facilities [6, 7]. Williams et al. recently applied STPA to evaluate the combined safety, security and safeguards challenges of transporting spent nuclear fuel [3]. The work described in this paper is the first application of STPA techniques to the fundamental processes underlying nuclear safeguards, with a specific focus on applying the techniques to a hypothetical MOX production facility. This work does not present a full STPA for nuclear material safeguards at a MOX production facility. Rather, it presents a process model, defining many of the interfaces to be considered within a full STPA, and suggests possible causes for undesired system outcomes, described herein as "drivers of increased risk."

The use of a systems model to describe the process under evaluation allows both qualitative analysis—including identification of scenarios that lead to states of increased system risk—and quantitative analysis—including the determination of downstream impacts of nuclear material quantification anomalies at the process level. This work presents a detailed qualitative evaluation of the hypothetical MOX system and a cursory discussion of quantitative techniques that could be further applied in future work.

METHODS:

In the context of nuclear material safeguards, two undesired system outcomes are considered: (1) diversion of a significant quantity of nuclear material occurs but is not detected by the system; and (2) the system alarms, indicating that there has been diversion, when no diversion has occurred. These correspond to the classic "Type I" and "Type II" errors of statistical hypothesis testing [8]. Naturally, the most important undesired system outcome is undetected diversion of a significant quantity of nuclear material. While the system requirements and control actions will be developed to prevent against this high-level concern, the prevention of false alarms is nearly as important. There is real risk associated with stopping production, unnecessarily conducting costly investigations, and possibly cycling law

enforcement and regulators. Balancing the risks associated with the two specified undesired system outcomes is of key importance in designing a safeguards approach. If a facility operator wishes to drive Type I errors to zero, the system would be in a constant state of alarm and no production would occur. If a facility operator wishes to drive Type II errors to zero, the system could easily allow nuclear material to be diverted without detection. Neither of these states is acceptable. For this reason, both error types are considered within this analysis as undesired system outcomes.

The STAMP causality model suggests the following types of unsafe control action [2]:

- A control action required for safety is not provided.
- An unsafe control action is provided that leads to a hazard.
- A potentially safe control action provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).
- A required control action is provided but is not followed.

Specific process actions that could lead to states of increased system risk can be identified for each flow of material and information in the system by evaluating the possible unsafe control actions listed above. Additionally, disconnects between the operators' knowledge of nuclear material quantities within their system and actual nuclear material quantities could result in driving the system to higher levels of risk. Consider the following examples:

- If a measurement of nuclear material concentration in the process vessel is artificially low, it could lead to the operator directing a larger than necessary transfer to the packing station, leading to a higher actual quantity of material than expected. This could mask the effects of other losses in the system.
- Inaccurate models, built into embedded system software or calibration system software, could lead to a disconnect between measured and real material quantities.
- If nuclear material handlers are given specific shipment specifications through an operating procedure, but willfully or accidentally fail to enact the control actions specified in the procedure, there could be inadvertent loss of material.
- If the procedure writers introduce an error to the procedure directing handlers to package a quantity of material different than what is listed in the flowsheet, the system goes to a higher level of risk.
- Acceptable levels of statistical variation are present in subsequent process stages. This variation happens to be compounding, resulting in real material quantities that are lower than expected.

The basis for STPA acknowledges that safety is an emergent property of systems as a whole and is not inherent to any specific stage or activity within the system. Thus, the influences of specific actions on the system as a whole can only be assessed in the context of the whole system. It is insufficient to make claims on the safeguards posture of a fuel cycle system by examining only a single process stage. This work developed a process model of the nuclear safeguards framework for a hypothetical MOX fuel fabrication cycle. The process model is

presented and analyzed in two phases: (1) the individual process-level systems and (2) the full, integrated systems level. The individual process systems level allows the analyst to identify more detailed causal information for equipment and process actions. The full, integrated systems level allows the analyst to identify causal information related to high-level regulatory requirements and facility interactions. Based on the process model, the authors examined each flow of information or material for actions that could lead to increased system states of risk. The authors provided commentary as to immediately evident hazards, actions that could drive the system to increased states of risk, and potential causes of the two undesired system outcomes. The final steps of STPA, defining system requirements and deriving control actions, are outside the scope of this work.

A systems theoretic process model was developed for a hypothetical MOX processing cycle. The process model assumes the cycle is separated into two facilities, a separation facility and a fuel fabrication facility. The separation facility includes individual stages for spent fuel inspection, spent fuel staging, mechanical separation of spent fuel from cladding, dissolution and co-extraction, oxide conversion of the extracted products, waste handling and storage, and oxide powder shipment. The fuel fabrication facility consists of individual stages for the inspection of received oxide powder, storage and staging of both uranium and plutonium oxides, blending of uranium and plutonium oxides, fuel pellet sintering, final fabrication, and offsite shipment. For the purpose of identifying potential drivers of increased risk, it is assumed that separate corporate entities operate the separation and blending and fabrication facilities. It is also assumed that the facility operators are independent of the state-level nuclear establishment.

A quantitative model was developed to allow users to specify a variety of fuel cycle operations, model variations in operational parameters, model uncertainty in nuclear material measurements at user specified points in the process, model the impacts of user specified diversion scenarios, and iterate for a user specified number of cycles. The model was developed for use in the Mathworks Matrix Laboratory[3] platform (MATLAB). The model was developed to address the following process types: used fuel handling, used fuel separation and dissolution, elemental blending, storage, and shipping and receiving. The various model stages introduce physical and statistical uncertainty at each stage based on user specified constraints. The program also addresses the variations in system knowledge due to uncertainties in measured values.

The model reads user specified input values and constructs a system of equations to represent individual process flows and solves the matrix system for each material type to determine the material into and out of each stage. Diverted material is treated as a separate, independent stage. To demonstrate and test the capabilities of this program, a hypothetical MOX fuel fabrication cycle was simulated. This cycle resembles the process-level systems described for the STPA. A full quantitative analysis of this system is left for future work.

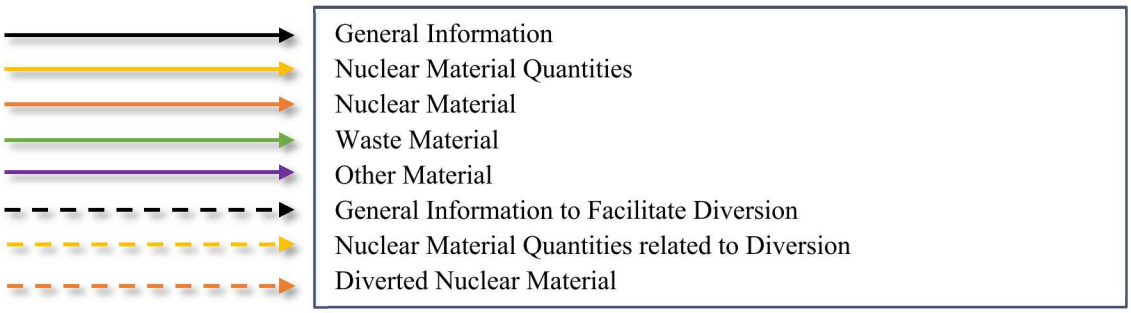
RESULTS AND DISCUSSION:

The process-level systems diagrams for the separation facility, fabrication facility and full, integrated system are presented in Figure 2, Figure 3 and Figure 4 respectively. The process

[3] MATLAB R2017b, Mathworks Inc.

streams in each systems diagram are labeled with sequential numbers. The orange arrows represent the physical flow of nuclear material, the gold arrows represent the flow of information about the quantity of nuclear material at various stages within the system, and the black arrows represent other sources of information, typically operating procedures or human interaction and interpretation of data. This color scheme is used throughout the paper and is depicted in Figure 1. A total of 116 process streams were identified. As a general rule for reading the process diagrams, individual process stream types are numbered sequentially from left to right. General information is labeled before nuclear material quantitative information, which is labeled before nuclear material flows, followed by other miscellaneous material forms. The numbers are referenced in the selections from the process analysis hazards, as presented in Table 2 and Table 3.

Figure 1: Systems Diagram Legend



Through the process analysis, 74 distinct scenarios were developed that could drive the system to increased states of risk for undetected nuclear material diversion or false alarms of nuclear material diversion. These scenarios were identified as possible in a total of 32 aggregated information and material paths within the MOX processing system. Scenarios that involve three or more process streams are presented for the facility-level models in

Table 2. All scenarios identified for the integrated system are presented in Table 3.

There are significant similarities between the hazards suggested for the two process-level models. For example, the hazards associated with inaccurate calibration or measurement models are present in any process where nuclear material is a derived quantity. The specific impacts of inaccurate process models will vary based on the specific measurement method used. While identification of control actions was outside the scope of this work, one could use this framework to designate specific attributes of measurements that could have an outsize impact on the final results. For instance, if quantification of the self-shielding effect of MOX powders proves to be an influential parameter, the results of the STPA could influence facility NMC&A personnel to conduct additional measurements to reduce the associated uncertainty.

Figure 2: Separation Facility Process-Level Systems Diagram

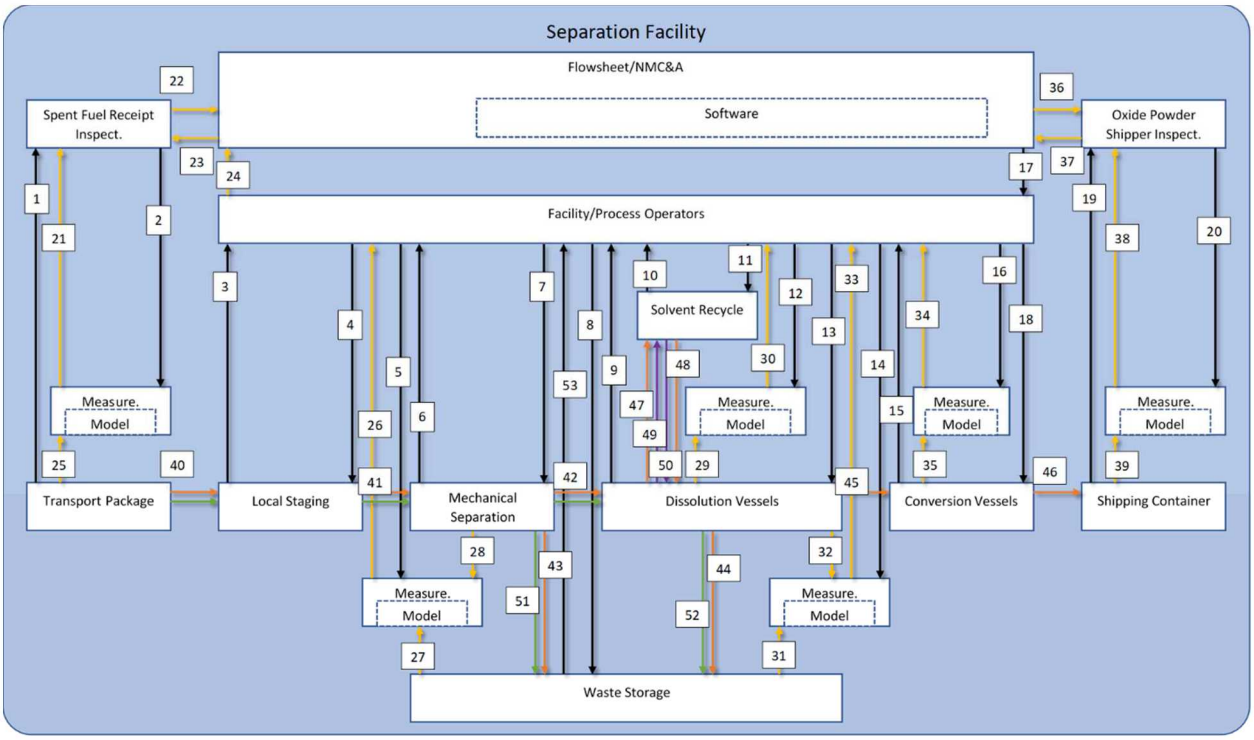


Figure 3: Blending and Fabrication Facility Process-Level Systems Diagram

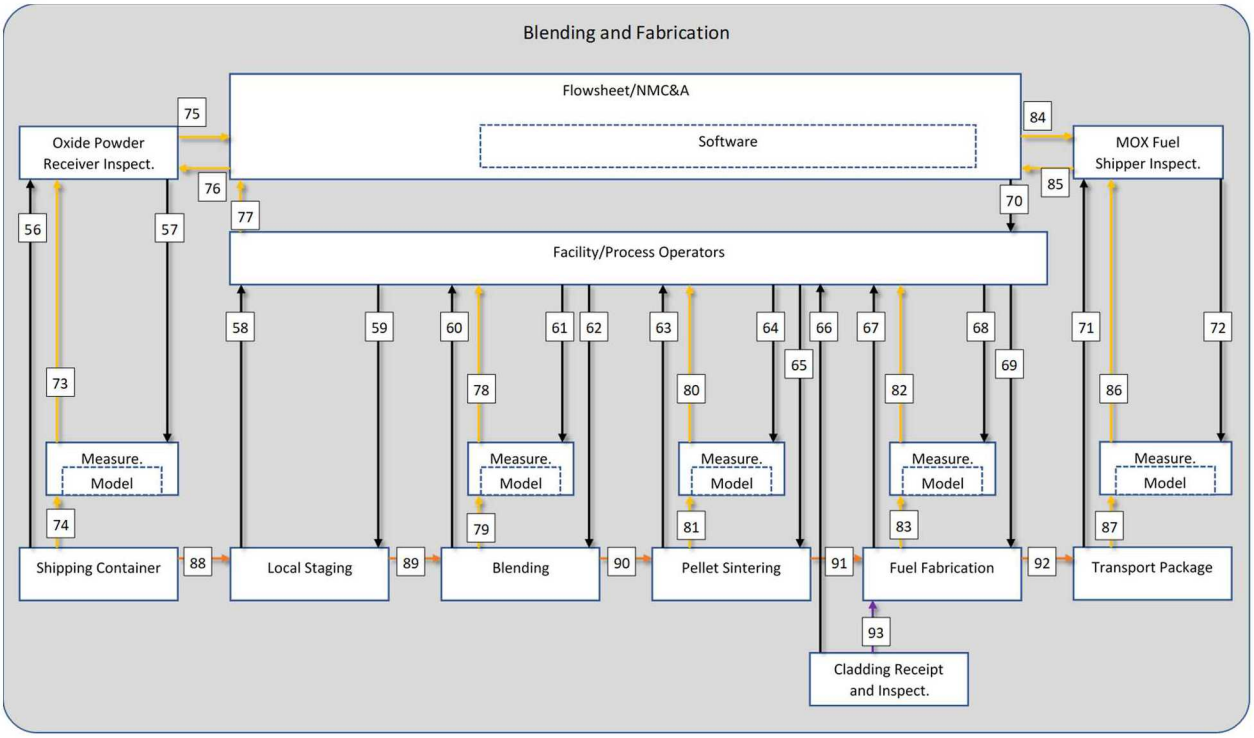
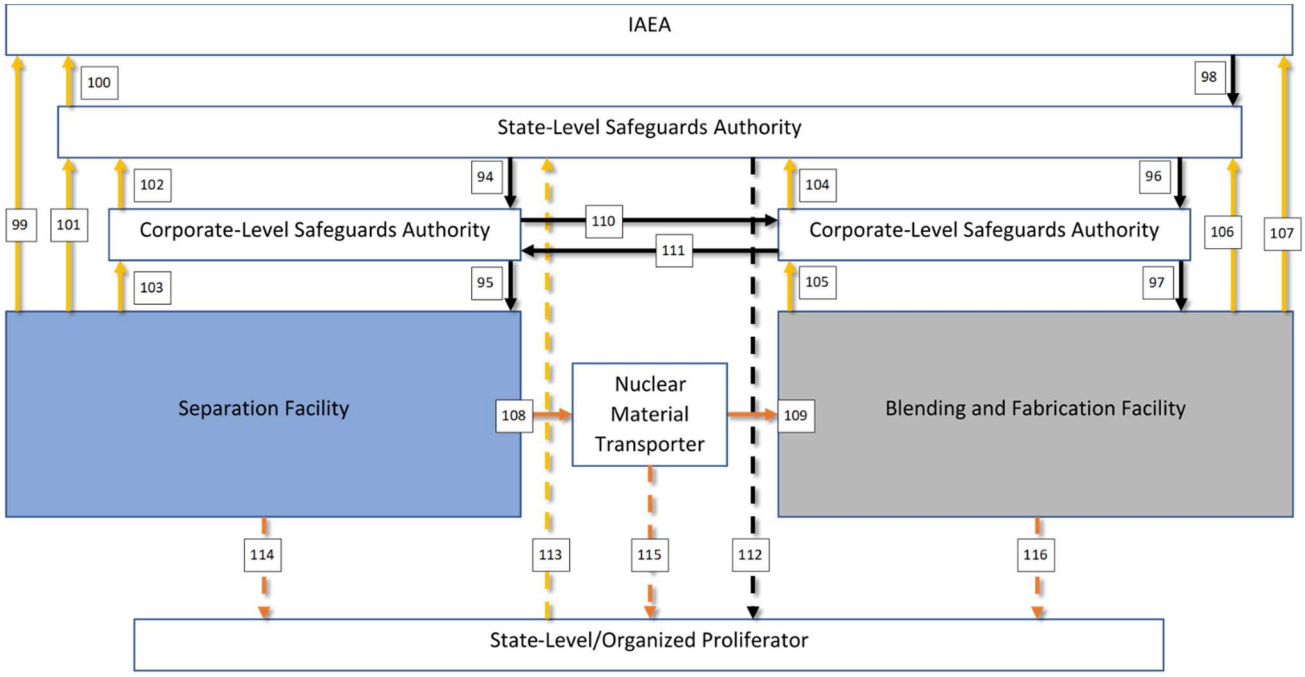


Table 2: Facility-Level Drivers of Increased Risk Involving Three or More Streams

Process Streams	Information or Material Flow Description	Possible Drivers of Increased System Risk
1, 3, 19, 56, 71	Qualitative inspection information collected on the transport package, including visual indications of tampering (i.e., broken TIDs) or loss of continuity of knowledge.	• Information is not collected completely, accurately, or timely. • Information is not relayed to decision authorities.
2, 5, 12, 14, 16, 20, 57, 61, 68, 72	Direction on use of measuring equipment. This includes sampling size, sampling points, count times and desired accuracy.	• Measurement is not conducted per the suggested requirements. • Measurement requirements do not accurately reflect system needs.
4, 7, 8, 11, 13, 18, 59, 65, 69	Direction from facility operations on how to operate this stage. This could include specific procedural instructions or direct commands.	• Procedures do not accurately reflect real process conditions. • Procedures are not executed accurately, completely, or in the designated sequence.
21, 26, 30, 33, 34, 38, 73, 78, 80, 82, 86	Nuclear material measurement information.	• Internal models in the measurement equipment do not reflect physical reality (e.g., incorrect assumptions on self-shielding). • Measurement equipment is mis-calibrated. • Measurements are not performed for as long of a duration as specified by the operators. • Measurements are performed accurately, but statistical variation causes an anomalous value. • Measurements are otherwise incomplete, untimely, or inaccurate.
22, 24, 37, 75, 77, 85	Measured nuclear material quantities, provided for comparison to expected values.	• Measurements are incomplete, untimely, or inaccurate. • Inspectors or operators fail to recognize anomalies in measurement data. • Measurements reflect false assumptions.
23, 36, 76, 84	Expected nuclear material quantities, provided for comparison to measured values.	• Internal software model used for nuclear material tracking introduces an error. • NMC&A personnel fail to recognize anomalies. • Measurements reflect false assumptions.
25, 27, 28, 29, 31, 32, 35, 39, 74, 79, 81, 83, 87	Physical indications of the presence and quantity of nuclear material. This includes radiation signatures and measured masses.	• Physical indications of the presence of nuclear material are not detected by the measurement equipment (i.e., shielding material is present). • Radiation from non-accountable sources (i.e., background) is interpreted as nuclear material. • Anomalous statistical variations are received by measurement equipment.
40, 41, 42, 45, 46, 88, 89, 90, 91, 92	Main, designed flows of nuclear material between process stages.	• Nuclear material is unaccounted for. This could be due to holdup, diversion of nuclear material, or material unexpectedly transferring with waste, solvents or process effluents.
51, 52, 53, 54, 55	Flows of waste material between stages.	• Waste material remains with accountable material, resulting in higher recorded masses or higher activities, potentially masking missing nuclear material.

Figure 4: Integrated Systems-Level Diagram



While there was significant overlap between the two process stages, the integrated model provided a very different set of proposed hazards. The importance of timing as it related to external inspections and audits was far more evident in the integrated model. Diversion of material was explicitly considered in the integrated model as a scenario where the state-level safeguards authority is complicit in the proliferation and diversion activities. Diversion scenarios where this is not the case would reduce in complexity. The integrated model highlights one of the primary benefits of using STPA as opposed to traditional hazard analysis methods in that it allows a user to identify areas where the regulations, consensus standards and shared protocols may be deficient. For example, a scenario was identified in the integrated model where, "corporate stove-piping or proprietary data could prevent the transmittal of information necessary to define an appropriate safeguards protocol at other facilities in the system." If this scenario were determined to represent a significant risk, state-level or international safeguards authorities could develop protocols for ensuring seamless transfer of information between facility operators.

Table 3: Integrated System-Level Drivers of Increased Risk

Process Streams	Information or Material Flow Description	Possible Drivers of Increased System Risk
94, 96	State-level directives that implement the state's safeguards agreements. These specify inspection and accountancy goals.	• State-level directives are not sufficiently rigorous in terms of accurate and timely reporting. • State-level directives require extensive reporting, causing false positives to be elevated beyond what is prudent.
95, 97	Corporate-level implementing procedures for state-level safeguards requirements. These specify local reporting thresholds, NMC&A program specifications, internal audit and inspection frequencies, and decision authorities.	• Corporate-level implementing procedures do not rigorously define requirements for accurate and timely reporting of anomalies. • Corporate-level implementing procedures do not specify sufficient internal audits. • Reporting thresholds are set too low, leading to unacceptably high false-positive rates.
98	Specifications of safeguards agreements between the IAEA and an individual state.	• Safeguards agreements are lacking, resulting in restricted access to all relevant facilities or operations by inspectors.
110, 111	Lessons-learned and process information shared between corporate safeguards authorities.	• Corporate stove-piping or proprietary data could prevent the transmittal of vital information. • Information received too late prevents the operators of other facilities from taking action.
99, 101, 106, 107	IAEA/state inspection results.	• Inspections occur too early, too late, or too infrequently to detect diversion of nuclear material. • Inspectors are denied access.
100, 102, 104	State reporting to the IAEA and corporate reporting to the state level safeguards authority.	• Reports occur too early, too late, or too infrequently to allow inspectors to detect anomalies. • State or corporate safeguards authorities could knowingly falsify records.
103, 105	Facility reporting to the corporate level safeguards authority.	• Flowsheets reflect anomalies introduced by any of the mechanisms identified at the facility and process level. • Facility reports occur too early, too late, or too infrequently to allow corporate auditors to detect anomalies or perform additional inspections. • Facility operators could knowingly falsify records.
108, 109	Transportation of nuclear material between facilities.	• Material could be diverted during shipment. • Anomalies introduced from any of the mechanisms identified at the facility level could be introduced to subsequent process facilities.
112, 113	Nuclear material diversion is sponsored by the state or coordinated through an insider.	• Information is provided to proliferators that enables them to obtain material and spoof formal reports. • Information is provided from proliferators that allows the state-level authority to falsify records or initiate a strategy to spoof results.
114, 115, 116	This is the physical flow of nuclear material that is diverted. This can be from any stage of the sub-level processes or during nuclear material transportation.	• Diversion occurs too early or too late to be detected by specified inspections or measurements. • Diversion occurs in quantities that are masked by other variations in process parameters or measurement uncertainties.

CONCLUSIONS AND FUTURE WORK:

This work presents an STPA evaluation of the causes of nuclear material accountability and safeguards anomalies that might be encountered while operating a mixed oxide (MOX) reprocessing facility. Through this evaluation, numerous scenarios were identified that could result in undetected diversion of nuclear material or an increased rate of false positive events. These scenarios were identified at both the process level and at the integrated systems level. An additional computational systems model was developed to allow further evaluation of the quantitative impacts of scenarios that could drive the system to higher risk levels. The full power of an STPA comes from the identification of emergent systems properties that are non-obvious at the component level. A full quantitative evaluation of these properties could be performed by coupling the computational model and the STPA model, but this is left as future work.

REFERENCES:

[1] N. G. Leveson, Engineering a Safer World, Cambridge, MA, USA: The MIT Press, 2011.

[2] N. G. Leveson, "An STPA Primer," 2013.

[3] A. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, A. H. Mohaghegi, M. DeMenno, M. Thomas, J. Parks, E. Parks and B. Jeantete, "System Theoretic Frameworks for Mitigating Risk Compexity in the Nuclear Fuel Cycle," Sandia National Laboratories, Albuquerque, NM, USA, 2017.

[4] A. Abdulkhaleq, "A System-Theoretic Safety Engineering Approach for Software-Intensive Systems," 2017.

[5] T. Ishimatsu, N. G. Leveson, J. T. Thomas, C. H. Fleming, K. Masafumi and Y. Miyamoto, "Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis," *Journal of Spacecraft and Rockets,* vol. 51, no. 2, pp. 509-522, 2014.

[6] T. Stirrup, "System Theoretic Process Analysis: Practical Application with Traditional HA Techniques," in *EFCOG NFS Workshop held August 8-12, 2016 in Chicago, IL, US.*, Chicago, 2016.

[7] J. Thomas, F. L. de Lemos and N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants," 2012.

[8] J. L. Jaech, Statistical Methods in Nuclear Material Control, Richland, WA, USA: United States Atomic Energy Commission, 1973.