Using an Integrated Safety Analysis to Identify Critical Infrastructure in Need of Aging Management

April Smith, PhD and Margie Kotzalas (United States Nuclear Regulatory Commission)

I. Introduction

The nuclear industry faces challenges to remain as a viable energy provider and weapons producer. Some challenges include direct competition for cleaner, less expensive power and the strategic positioning of fuel for low and high enrichment needs. The infrastructure upon which the industry is built also faces challenges. There are buildings and supporting structures that were constructed more than fifty years ago. Aging management in the nuclear industry, however, involves not only buildings, but a wide range of components from glove boxes to reactor vessels. In particular, non-power nuclear facilities like fuel cycle facilities, have unique challenges as safety programs must consider not only radiological safety, but chemical safety, as well.

One fundamental challenge before some decision makers of non-power nuclear facilities is how to incorporate aging management into their current programs. This paper explores the application of an integrated safety analysis (ISA) to determine critical infrastructure in need of aging management. Assuming a non-power nuclear facility (facility) currently uses a risk-informed framework to identify safety controls and quality assurance measures, an ISA, and consequently an aging management program, could be incorporated into that framework without the need to create a separate program. This paper will describe those elements of an ISA that lend themselves to integration into an existing risk-informed program and how those elements can be modified to accommodate aging management. The concept of incorporating aging management into existing programs is attractive from a safety perspective because overall facility safety can become more effective once aging is routinely considered. Also, incorporating risk-related aging management elements in an existing program is likely more efficient than creating an entirely new program.

Given the wide range of systems, structures and components (SSCs) involved in the nuclear industry, this paper strives to address aging management from the perspective of decision makers faced with identifying general approaches to implementing aging management and assumes that aging management is a necessary safety consideration. To that end, the cost of implementation or the comparison of costs among various approaches is not the focus of this paper. However, the structure of this paper is such that issues like cost and asset protection can be readily incorporated and quantified, if desired.

The remaining sections of this paper discuss the premise regarding incorporating aging management into an existing risk-informed framework and the application of an ISA to demonstrate that premise.

II. Premise: Aging management can fit within an existing risk-informed framework

Assuming a facility already applies some type of risk-informed methodology to identify accident sequences and control the associated risks, the authors surmise that an aging management

program can also be risk-informed and fit within that existing framework. In other words, facilities that consider the likelihood and consequences of accidents to determine safety controls and quality assurance measures already have the programmatic infrastructure to incorporate aging management. The authors chose to demonstrate this premise by considering an existing, generic risk-informed methodology and determining those elements that could readily incorporate aging management concepts. Certain fuel cycle facilities licensed in the United States of America comply with Title 10 of the Code of Federal Regulations (10 CFR) Part 70, "Domestic Licensing of Special Nuclear Material (USNRC, 2019a). Within that part, there is Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical mass of Special Nuclear Material" (USNRC, 2019b). Subpart H requires licensees to perform an ISA which is a risk-informed analysis that considers the consequences and likelihoods of credible accident sequences to establish safety controls. The authors selected a generic methodology for performing an ISA and identified minor modifications to the methodology which would address aging management. The following sections describe an ISA and the generic methodology in comparison to the modified methodology.

III. What is an Integrated Safety Analysis?

A. NRC Definition

An integrated safety analysis, or ISA, is a risk-informed approach that identifies safety controls to prevent or mitigate accidents. The United States Nuclear Regulatory Commission (USNRC) defines the term, "integrated safety analysis," as "A systematic analysis to identify facility and external hazards and their potential for initiating accident sequences, the potential accident sequences, their likelihood and consequences, and the items relied on for safety (IROFS)." (USNRC, 2019c) The USNRC definition clearly outlines the regulatory expectations for those who comply with 10 CFR Part 70, Subpart H. One expectation is that an ISA must be systematic. In other words, an ISA is, and of itself, a process to be performed in a manner that is repeatable and consistent. Its systematic nature is important to consistently and reliably identify potential accident sequences and their likelihoods and consequences. Another expectation is that an outcome of an ISA is the identification of IRFOS or those items relied upon to prevent or mitigate the identified potential accident sequences.

Along with the requirements of identifying the likelihood and consequences of potential accidents, the USNRC also requires the consideration of IROFS to be performance based. In this case, performance is measured by radiological limits and chemical exposure standards as defined in the performance requirements of 10 CFR 70.61 (USNRC, 2019d). These limits, for the most part, are related to a level of consequence to the public or workers at the facility. Therefore, an ISA is risk-informed and performance based. Those two elements (risk-informed and performance based) combined with operating experience allow facilities to define their safety basis and demonstrate safe operation.

B. Generic Methodology

Figure 1 illustrates a generic ISA methodology. Depicted as a process flow chart, the systematic nature of an ISA begins with organizing the facility into parts, nodes, or systems. For each part, internal and external hazards are identified, followed by the associated accident sequences. As the process continues, it allows for the possibility that not every accident sequence is credible. In this category, one could consider sequences with initiating events of

extremely low likelihood, such as natural phenomena hazards, or a series of moderately low likelihood events, e.g., the failure of multiple passive engineered systems.

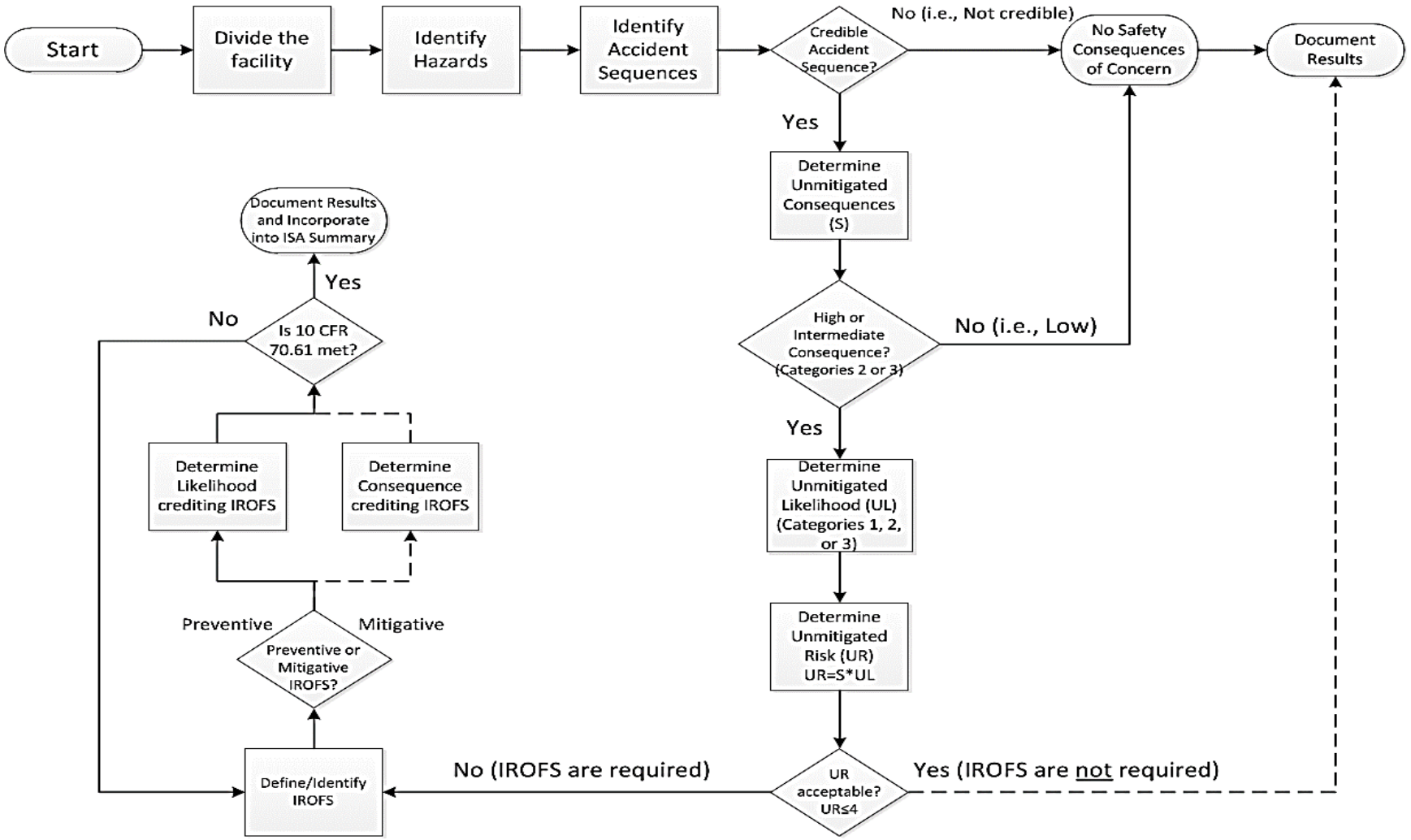

Figure 1: Generic ISA Methodology

Depending on the criteria used to determine credibility, an accident sequence may be screened out of the analysis and documented or continues through the process.

For credible accident sequences, the unmitigated consequences and likelihoods are determined. Unmitigated necessarily means that no controls are credited or applied to the accident sequence. For this generic methodology, an unmitigated consequence (S) is given a score of 2 or 3, where 2 correlates to an intermediate consequence, and 3 is high consequence. Either qualitative descriptions or quantitative limits can be used as the criteria for what consequences are assigned a 2 or 3. The USNRC, for instance has deterministic, quantitative and qualitative criteria. If the unmitigated consequence (S) is low or less than 2, then, again, the sequence is screened from the analysis and documented. If, however, S equals 2 or 3, then the unmitigated likelihood (UL) is determined.

Similar to unmitigated consequences, unmitigated likelihoods are categorized into three levels: 1, 2, and 3, where UL equates to a measure of likelihood described as highly unlikely, unlikely, and not unlikely, respectively. The likelihoods for each category generally cover a range of frequencies related to the occurrence of an event throughout a period of time. For instance, UL = 1 may be an event that is expected to occur less than once in 10,000 years; UL = 2 is expected to occur between 1 out of 10,000 years and 1 out of 1,000 years, and UL = 3 is expected to occur more than 1 out of 1,000 years. The two values of S and UL are combined to obtain an unmitigated risk metric (UR) where UR = S * UL.

Depending on the risk thresholds, UR determines the risk acceptability. If acceptable, the risk metric is documented and the analysis for that sequence is terminated. The risk matrix in Table 1 is an example of how UR may be used to determine the acceptability of risk (USNRC, 2015).

Severity of Consequences	Likelihood of Occurrence		
	Likelihood Category 1 Highly Unlikely (1)	Likelihood Category 2 Unlikely (2)	Likelihood Category 3 Not Unlikely (3)
Consequence Category 3 High (3)	Acceptable Risk 1 x 3 = 3	Unacceptable Risk 2 x 3 = 6	Unacceptable Risk 3 x 3 = 9
Consequence Category 2 Intermediate (2)	Acceptable Risk 1 x 2 = 2	Acceptable Risk 2 x 2 = 4	Unacceptable Risk 3 x 2 = 6
Consequence Category 3 Low (1)	Acceptable Risk 1 x 1 = 1	Acceptable Risk 2 x 1 = 2	Acceptable Risk 3 x 1 = 3

Table 1: Example Risk Matrix

If the risk is unacceptable, the accident sequence is considered in the rest of the process where safety controls or IROFS are determined. In this part of the process, a feedback loop is used to illustrate that not only a safety control must be defined, but it must pass the performance measures. In Figure 1, the performance measures are the requirements of 10 CFR Part 70, Paragraph 70.61 (USNRC, 2019d). Controls are identified that can prevent or mitigate, but in either case, they must meet the performance requirements. Once the performance requirements are met, the results are documented.

After IROFS are identified, their reliability and availability should be maintained. In the USNRC regulatory framework, licensees are required to establish management measures. The USNRC defines management measures as, "Functions performed by the licensee, generally on a continuing basis, that are applied to IROFS, to ensure the items are available and reliable to perform their functions when needed. Management measures include configuration management, maintenance, training and qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements." Figure 2 illustrates where the process to establish management measures occurs relative to conducting the ISA, i.e., it is the last step following identification of safety controls.

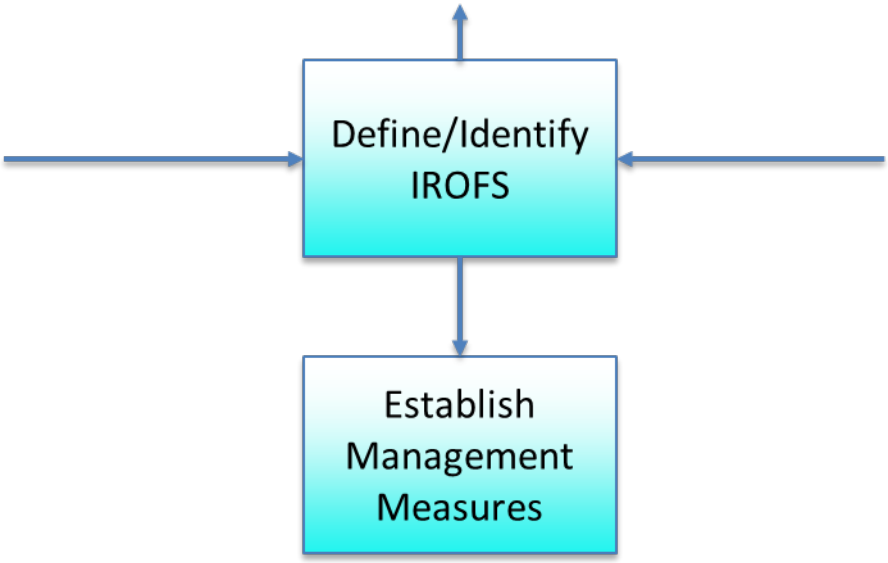

Figure 2: Process step to establish management measures

IV. Modified ISA Methodology to Incorporate Aging Management

The ISA methodology discussed in the previous section is risk-informed, systematic, and can be linked to quality assurance (QA) measures to maintain IROFS as reliable and available. At first glance, there is no explicit connection to aging management. However, in the USNRC regulatory framework, an ISA is a living process performed throughout the lifetime of the facility with the purpose of routinely evaluating hazards and establishing safety controls to limit radiological and chemical risks. Given this characteristic of facility lifetime implementation, the authors sought to determine those changes to the generic methodology that would be important in incorporating aging management.

Because aging management research for non-power nuclear facilities is scarce, the authors reviewed aging management research and literature related to similarly situated facilities such as nuclear power and chemical plants. From that review, the authors identified that key characteristics of aging management programs for these facilities are not incompatible with non-power nuclear facilities. For instance, Blahoianu et al describe the key objectives that a facility's aging management program must accomplish (Blahoianu, Viglasky, Moses, Kirkhope, & Commission, 2011). These objectives include:

- Identifying and managing potentially dangerous plant conditions before challenging defense-in-depth;
- Appropriately integrating aging management to result in an overall review of safety, and
- Maintaining the validity of steady state and dynamic analyses.

Blahoianu et al also identify the outcomes of an aging evaluation. These outcomes include to:

- Identify potential ageing degradation mechanisms for the specific SSC.
- Assess the impact of ageing degradation mechanisms on SSC functionality;
- Establish means to detect and monitor the extent and rate of SSC degradation for the specific ageing mechanisms;
- Specify acceptance criteria to ensure that the required integrity and functional capabilities of the SSC are maintained, and
- Establish means to mitigate ageing mechanisms and their effects (e.g., through maintenance, replacement, or changes in operating.

Again, all these outcomes are compatible with performing the generic ISA methodology. Through the execution and maintenance of an ISA throughout the lifetime of a facility, these key objectives and outcomes can be accomplished. Schoeckle et al discuss an aging management methodology with the goal of controlling aging phenomena and ensuring the availability of the required safety functions throughout a facility's lifetime (Schoeckle, Rothenhoefer, & Koenig, 2014). The basic steps of the methodology highlight a continuous process to:

- Develop a plan to safeguard the quality of SSCs;
- Implement the plan to perform the necessary measures;
- Continuously check the implementation to validate that quality is being maintained, and
- Make modifications to optimize quality or correct quality deficiencies.

These steps are compatible with the generic ISA methodology.

Also, through the research and literature review, the authors identified that a risk-informed aging management program can resemble a process like an ISA. Figure 3 depicts a process-oriented, risk-informed aging management decision model as described in *Dealing with Aging Process Facilities and Infrastructure* (Center for Chemical Process Safety, 2018). The model elements are very similar to those in an ISA, i.e., assessing the consequences, assessing the likelihoods, determining risk acceptability, and implementing risk controls. Given those similarities, the authors readily modified the generic ISA methodology to account for aging management.

Figure 4 highlights the modified methodology. The step to identify hazards will now include those hazards associated with aging such as material degradation, cyclic fatigue, and other potential failure mechanisms that are chronic in nature. After identifying those hazards, most of the remaining steps in the process are the same: identifying the accident sequences along with their associated credibility, consequences, likelihoods and risk acceptability, followed by defining IROFS or safety controls. The next modification is adding a step between defining IROFS and establishing management or QA measures. Specifically, in addition to defining IROFS, the SSCs that support those IROFS are also defined. Those SSCs are then designated as critical safety infrastructure. In other words, those SSCs are critical to the safe operation of

the facility because they directly support the functions of items relied on for safety. Therefore, when the appropriate QA measures are established, those measures cover not only the safety controls, but the availability and reliability of those SSCs that support them. As this modified ISA methodology is implemented throughout the lifetime of the facility, aging management is also implemented through a modified hazards identification scope, further identification of the critical SSCs and QA measures needed to support the identified IROFS or safety controls.

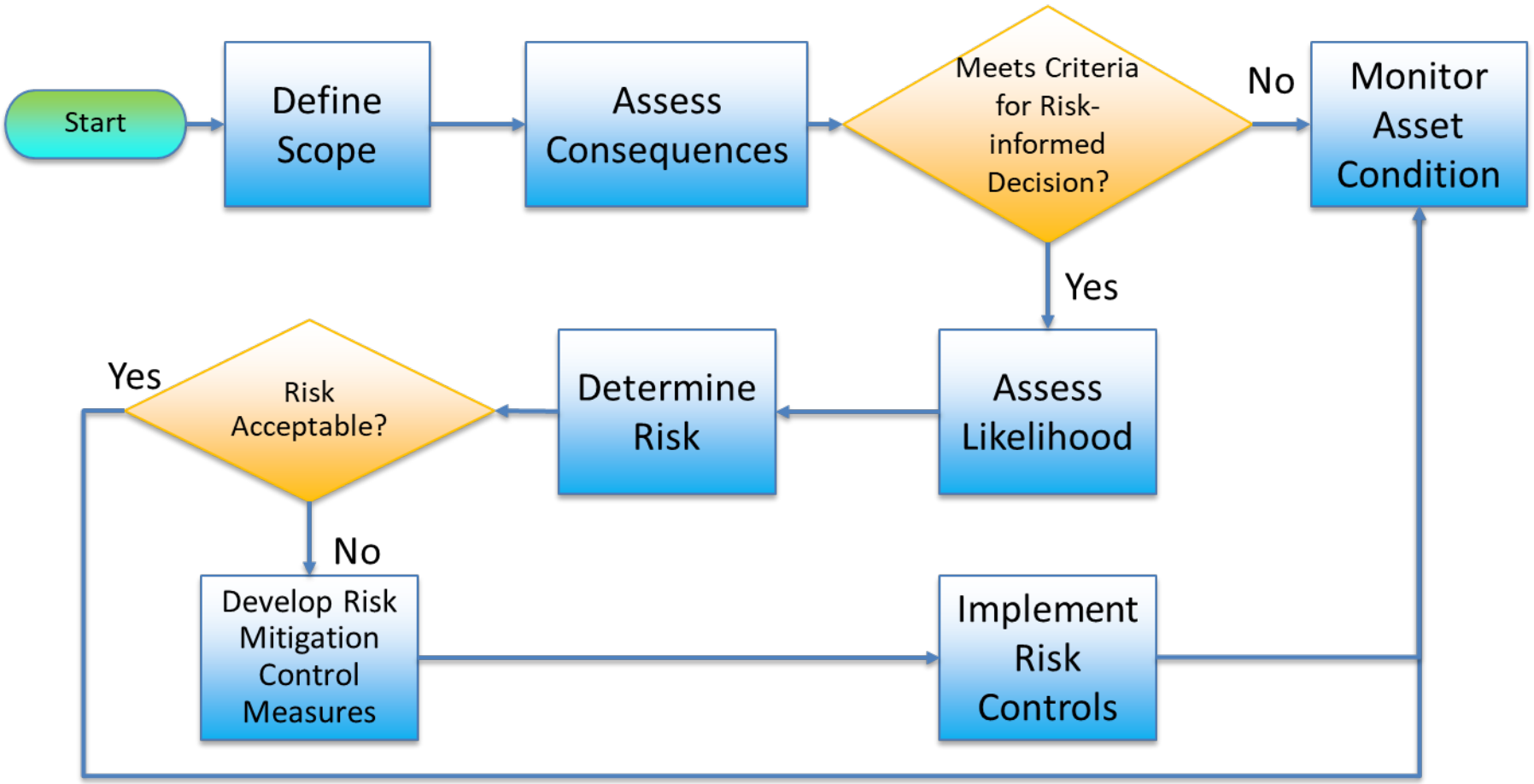

Figure 3: Risk-informed aging management decision model

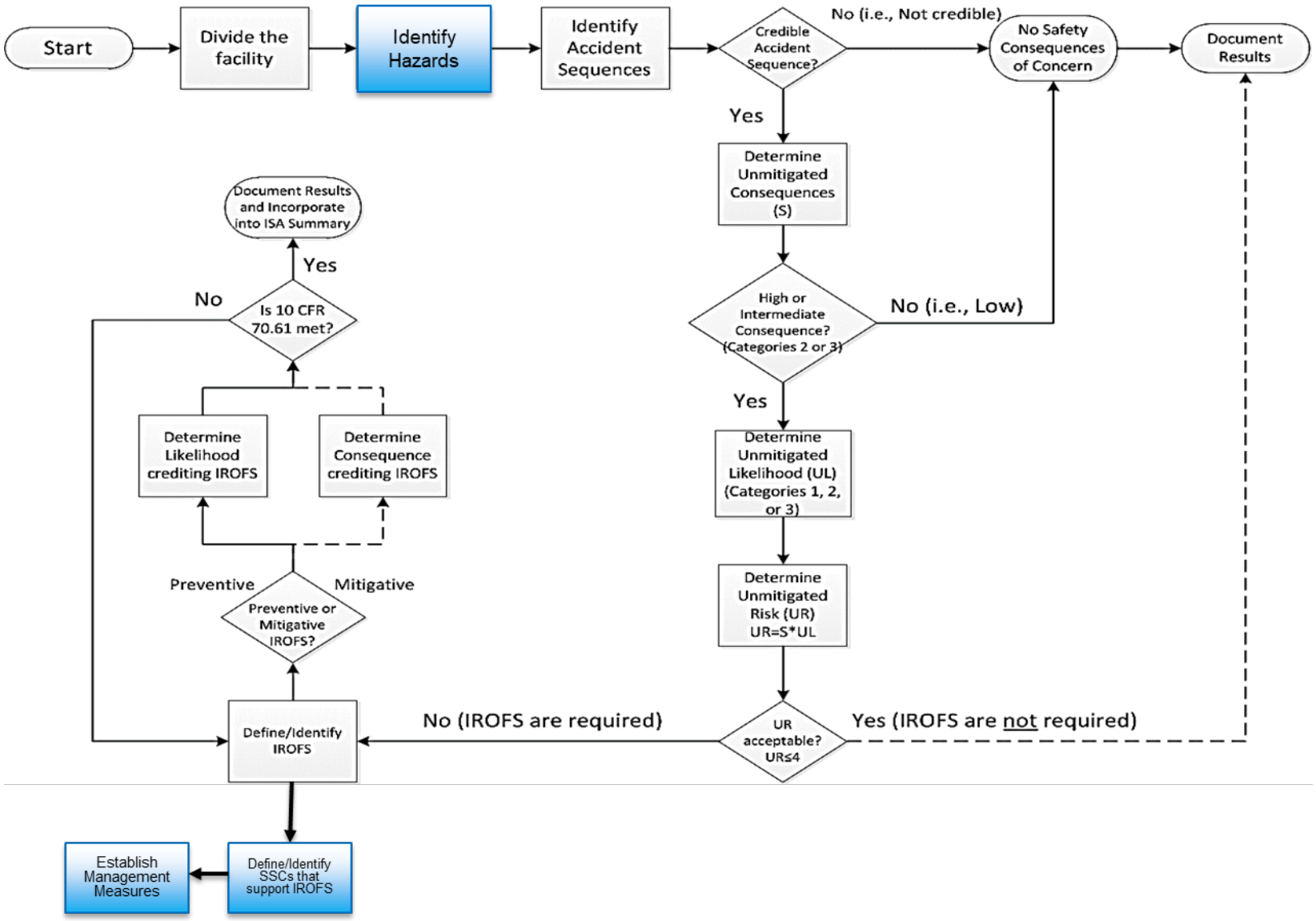

Figure 4: Modified ISA to incorporate aging management

V. Conclusion

The authors demonstrate at a conceptual level that an aging management program can fit within an existing risk-informed framework and augment the existing safety program. Incorporating aging management into a risk-informed methodology augments the existing safety program because the effects of aging are being actively identified and managed through IROFS or safety controls and their critical safety infrastructure, i.e., the SSCs that support them.

Future work to further explore the author's premise could include:

- Implementing the generic and modified ISA methodology on one or more systems at an actual or simulated operating facility and
- Identifying limitations to directly incorporating aging management into an existing risk-informed safety program.

VI. References

Blahoianu, A., Viglasky, T., Moses, C., Kirkhope, K., & Commission, C. N. (2011). Canadian regulatory approach to ensuring the implementation of effective ageing management programs for nuclear power plants. *Nuclear Engineering and Design, 241*, 548-554.

Center for Chemical Process Safety. (2018). *Dealing with Aging Process Facilities and Infrastructure.* New York, NY: Wiley.

Schoeckle, F., Rothenhoefer, H., & Koenig, G. (2014). Aging management: Control of the knowledge data base. *Nuclear Engineering and Design, 269*, 281-285.

USNRC. (2015). Standard Review Plan for Fuel Cycle Facilities License Applications (NUREG-1520). Washington, D.C. Retrieved 2019, from https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1520/

USNRC. (2019a). Title 10 of the Code of Federal Regulations, Part 70. Retrieved 2019, from https://www.nrc.gov/reading-rm/doc-collections/cfr/part070/full-text.html

USNRC. (2019b). TItle 10 of the Code of Federal Regulations Part 70, Subpart H. Retrieved 2019, from https://www.nrc.gov/reading-rm/doc-collections/cfr/part070/full-text.html#part070-0060

USNRC. (2019c). TItle 10 of the Code of Federal Regulations Part 70, Paragraph 70.4. Retrieved 2019, from https://www.nrc.gov/reading-rm/doc-collections/cfr/part070/full-text.html#part070-0004

USNRC. (2019d). TItle 10 of the Code of Federal Regulations Part 70, 70.61 - Performance Requirements. Retrieved 2019, from https://www.nrc.gov/reading-rm/doc-collections/cfr/part070/full-text.html#part070-0061