The Effects of Inaccurate Analyses on the Selection of Safety Controls

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

I. Introduction

The United States Nuclear Regulatory Commission (USNRC) implements and maintains the Fuel Cycle Operating Experience (FC OpE) Program. One purpose of the program is to identify and share issues that may generically apply across the fuel cycle industry. A recent USNRC FC OpE analysis identified key concepts regarding the implementation of safety programs at fuel cycle facilities. This paper discusses those concepts with an emphasis on their generic nature, including fundamental drivers and the potential implications to safe operations. The authors chose this emphasis to facilitate understanding of the broad applicability of the issues identified.

Two generic models will serve to demonstrate the key concepts. Figure 1 illustrates Facility A, a generic facility with three process areas that are physically separated on the site. In other words, the processes take place in three separate building structures that do not have common ventilation systems or ingress and egress points but do share electrical cabling and a system of transferring product from one process to the next. Facility A has one primary control room with three auxiliary control rooms, each located in one of the three process areas. The safety program for Facility A applies to all process areas and designates controls to prevent or mitigate the hazard of concern identified in each area. Figure 2 illustrates Facility B, a generic facility with three process areas that are co-located in the same building structure. The processes have common ventilation systems and share ingress and egress points and electrical cabling. Facility B has one main control room with one emergency backup control room, located outside of the main building. The safety program for Facility B is conceptually the same as that for Facility A.

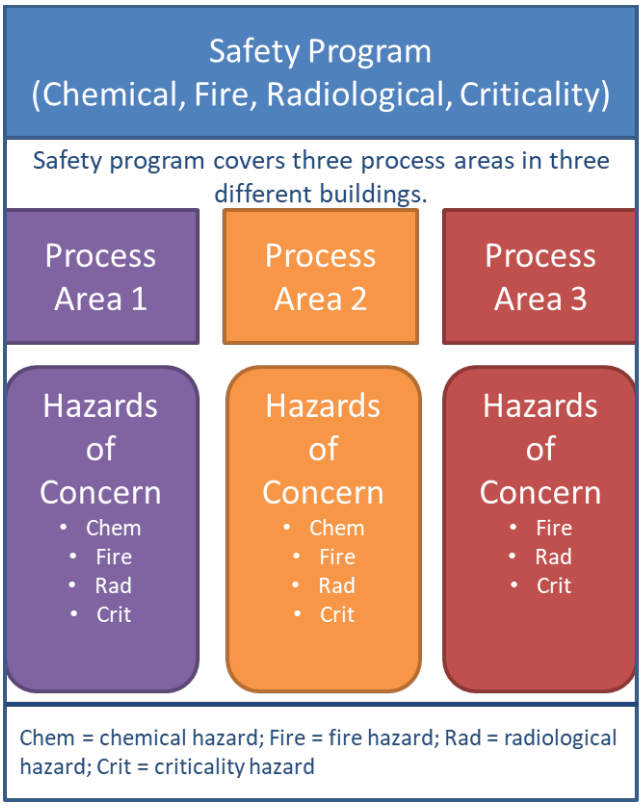
Using these models, the authors will demonstrate three concepts:

1) The importance of complete and accurate analyses of credible plant conditions and identification and implementation of reliable safety controls;

2) How one invalid technical assumption can cause an error that propagates over time, past the operator's quality assurance program as well as through the regulator's licensing and oversight programs, leading to upset conditions, and

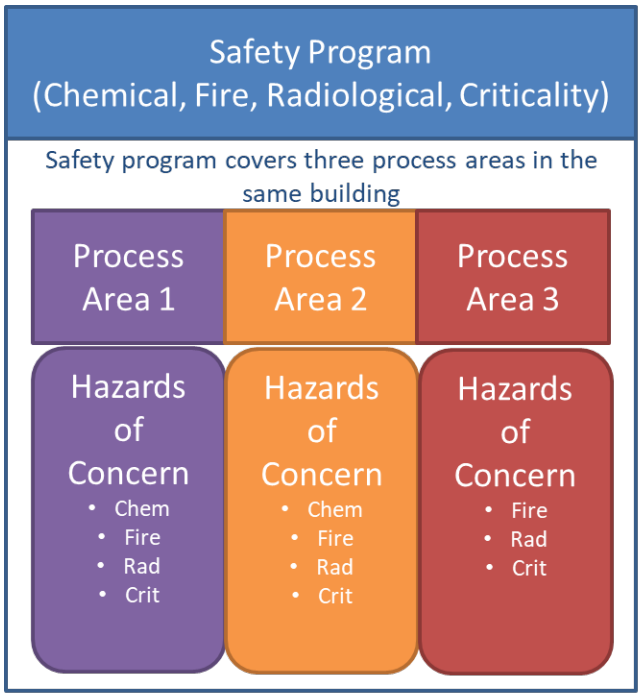
3) The importance of verifying analyses of event sequences through operational data, while looking for trends that indicate degrading performance that may need to be addressed to maintain the validity of technical assumptions.

One could make the argument that these three concepts are self-explanatory and, therefore, do not require any in-depth discussion. However, the authors will also discuss these concepts in the context of actual events that recently occurred at facilities licensed in the United States of America (US). Through those discussions, the authors highlight the lessons learned from delving into the details of these seemingly self-explanatory concepts.



- One main control room
- Three auxiliary control rooms
- Separate ventilation systems
- Separate ingress/egress points for personnel
- Shared ingress/egress for product movement
- Shared electrical cabling

Figure 1: Fuel Cycle Facility A



- One main control room
- One emergency back-up control room
- Shared ventilation systems
- Shared ingress/egress points for personnel
- Shared ingress/egress for product movement
- Shared electrical cabling

Figure 2: Fuel Cycle Facility B

II. Unanalyzed Facility Conditions

The USNRC FC OpE analysis reviewed event data from 2015 to 2018 related to either licensee- or USNRC- identified facility conditions that the licensee had not evaluated in its safety program, i.e. unanalyzed facility conditions. The USNRC chose to analyze these data because of the occurrence of several events in a relatively short period of time related to incomplete or inaccurate safety analyses. Consistent with the purpose of the USNRC FC OpE Program, the analysis looked for trends or common themes. The results of the analysis revealed common types of unanalyzed facility conditions, including:

- Non-routine activities, such as non-routine maintenance or extended periods of shutdown;
- Routine maintenance activities that removed equipment from service;
- Overlooked failure modes of safety controls, and
- Overlooked alternate flow paths for hazardous material.

To conceptualize the importance of considering these types of facility conditions, the authors chose two generic cases: non-routine maintenance specific to a process area and non-routine maintenance on components common to all process areas. Figure 3 considers Facility A and an unanalyzed condition of non-routine maintenance that is specific to Process Area 1. Given that this condition is unanalyzed, the authors made the conservative assumption that no safety controls are present that could either mitigate or prevent an event initiated by the non-routine maintenance activity. Assuming such an event occurs, it is likely Process Area 1 would be affected. Given the configuration of Facility A, it is less likely the other process areas would be affected, depending on the nature of the event and whether it involves electrical cabling or product transfer from one area to the next.

Figure 4 considers Facility A and non-routine maintenance on components that are common to all process areas. Again, given that the condition is unanalyzed, the authors conservatively assumed no safety controls have been designated. Because the non-routine maintenance activity could take place in any of the process areas, all process areas are vulnerable to this maintenance-initiated event. Alternatively, Figure 5 illustrates the potential effects of non-routine maintenance on Facility B. Because Facility B shares the same building structure as well as other systems and components, either unanalyzed, non-routine maintenance activity

(specific to an area or on common components in all areas) could impact any process area either directly or indirectly.

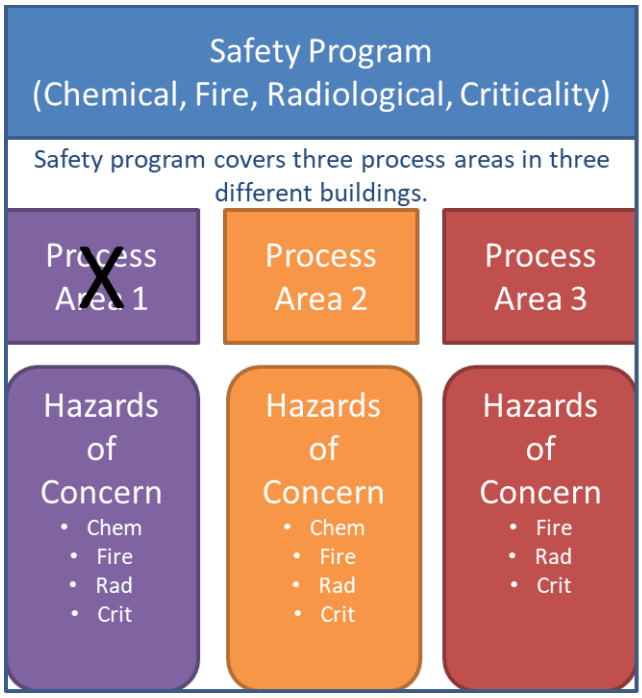
In 2015 and 2018, the USNRC documented events related to unanalyzed conditions. These events span the common types of unanalyzed conditions identified from the results of the FC OpE analysis. Information Notice (IN) 2015-08, “Criticality and Chemical Safety Events Involving Unanalyzed Conditions and Unanticipated Unavailability of IROFS at Fuel Cycle Facilities,” describes four events involving unanalyzed conditions (United States Nuclear Regulatory Commission, 2015).

During periodic checks of equipment, a licensee discovered moisture in a container used to feed fissile material from one process to another. The safety control that was meant to detect moisture in the container had been disabled during previous system maintenance. The maintenance procedure did not require that disabled detectors be reset or functionally tested after maintenance. The licensee had not analyzed a condition whereby the detector became disabled.

IN 2015-08 also describes an event where operators deviated from procedures and scraped accumulated fissile material into large piles, exceeding a prescribed safety limit. The licensee had not analyzed the possibility of operators deviating from procedures.

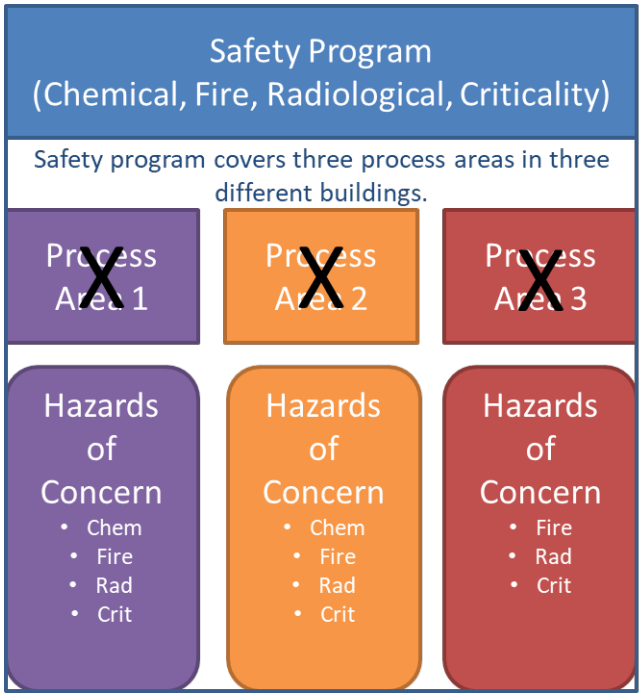
Another event in IN 2015-08 describes the identification of fissile material in a junction box. A pinhole leak had developed in a thermowell seal connected to the junction box, providing an alternate flow path of fissile material to collect in the junction box. The licensee had not considered the failure of the thermowell and electrical conduit seals as a source of possible accumulation of fissile material.

As a final example, Information Notice 2018-05 discusses an issue identified during maintenance to address decreased system performance (United States Nuclear Regulatory Commission, 2018). Specifically, a licensee discovered unexpected fissile material in an area assumed to be free of fissile material. Because the licensee assumed that only non-fissile material could be present in that area, no analysis had been performed and, therefore, no safety controls had been implemented to prevent or monitor fissile material. Furthermore, the system was not routinely surveyed to detect or monitor the accumulation of fissile material. Although the licensee found only small amounts of fissile material, this event is significant to criticality safety. Had this unanalyzed condition not been discovered in time, enough material could have accumulated to set the stage for a criticality accident.



- One main control room
- Three auxiliary control rooms
- Separate ventilation systems
- Separate ingress/egress points for personnel
- Shared ingress/egress for product movement
- Shared electrical cabling

Figure 3: Unanalyzed condition in Facility A - Non-routine maintenance specific to a single process area.



- One main control room
- Three auxiliary control rooms
- Separate ventilation systems
- Separate ingress/egress points for personnel
- Shared ingress/egress for product movement
- Shared electrical cabling

Figure 4: Unanalyzed condition in Facility A - Non-routine maintenance on components common to all process areas.

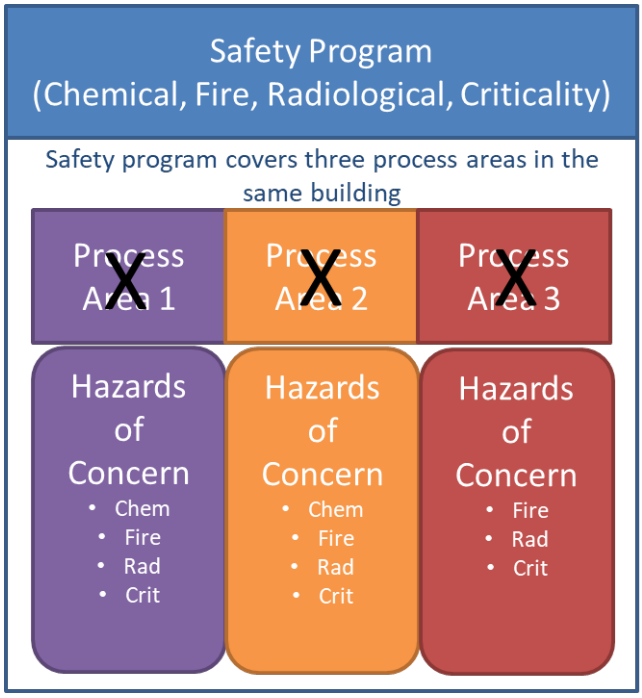


Figure 5: Unanalyzed condition in Facility B - Non-routine maintenance either specific to or on components common to all process areas.

III. Unchallenged Technical Assumptions and their Effects on Regulatory Licensing and Oversight

In addition to events involving unanalyzed facility conditions, the USNRC FC OpE analysis identified events driven by technical assumptions that neither the licensee nor the regulator challenged. These technical assumptions were fundamental in nature, i.e., their declaration automatically excluded the possibility of certain types of accidents. In general, these unchallenged technical assumptions included:

- No or limited presence of moderator;
- A limit on the concentration of reactive material;
- No or very limited changes in the geometry of vessels or areas containing reactive material, e.g., the volume of a tank could not change, and
- No alternate flow paths for reactive material to flow.

Figures 6 and 7 illustrate generic effects of propagating unchallenged assumptions from the safety program to the process areas. Figure 6 shows Facility A after assuming certain criticality assumptions like no presence of moderator or a limit on the concentration of fissile material.

Once the assumption is incorporated into the safety program, it can be transmitted to all process areas involving criticality hazards. In the case of Figure 6, because of these criticality assumptions, the results of a hazards analysis could determine that no additional criticality safety controls are needed in any or some part of each process area. In any case, all process areas could be left without adequate safety controls. The generic effects of propagation in Figure 7 are similar because of the fundamental nature of incorporating unchallenged assumptions in a safety program. The specific effects, however, may be more significant. Unlike Figure 6, should a criticality occur in one process area because of a lack of adequate safety controls, it is less likely that the resulting damage could be contained only to that area.

Information Notice 2018-05, as discussed in Section II, is an actual example of the importance of challenging technical assumptions. A more complex example is discussed in IN 2016-03, "Uranium Accumulation in Fuel Cycle Facility Ventilation and Scrubber Systems." This IN discusses the details of an event where, over time, a licensee did not closely monitor changes to its ventilation and scrubber system (United States Nuclear Regulatory Commission, 2016). Generally, it would be expected that these changes would have been controlled through a quality assurance program, specifically configuration management. However, fundamental to the failure of configuration management was an assumption that the concentration of uranium was low and could not exceed a specified weight limit. This assumption led the licensee to determine that the system was low risk in terms of criticality safety. Eventually, the changes to the ventilation and scrubber system were significant enough to result in large accumulations of uranium-bearing material in unexpected locations with geometry that could facilitate a criticality, i.e. unfavorable geometry. Again, because of the assumption of low uranium concentration, at times, licensee personnel would use water, a moderator, in an attempt to wash away the accumulation. After the licensee discovered in the scrubber insoluble material containing approximately 87 kg of uranium, the process was finally shut down and evaluated. That amount of material far exceeded the limit the safety program had established via its technical analyses. Not only was the safety limit on the amount of material surpassed, a chemical analysis revealed that the concentration of uranium far exceeded the assumed concentration. Although the licensee was able to safely shut down the process, this event was still significant given the risk of criticality.

Another facet of this example is the licensee's failure to use operating experience to re-validate its assumptions on system performance. There were several instances where licensee personnel discovered unexpected accumulations of material in parts of the system with

unfavorable geometry. Although the amounts discovered were technically below the established safety limit, they were still substantial, and the licensee did not challenge its original assumptions regarding concentration or weight. Furthermore, when the results of one safety analysis suggested that the concentration of uranium could exceed the assumed safety limit, the licensee dismissed the results. When system performance and operating experience indicated that initial technical assumptions may not have been valid, the licensee did not take the opportunity to re-validate those assumptions.

This example also demonstrates the propagation of unchallenged technical analyses through regulatory licensing and oversight programs. The USNRC has two programs, licensing and oversight, that work together to verify a fuel cycle licensee is operating safely in compliance with USNRC regulations. Essentially, the licensing program reviews applications to possess and produce nuclear material, while the oversight program verifies, through inspection, that applications are being implemented as intended. Harrison and Smith discuss the propagation of errors from unchallenged technical assumptions through these programs (Harrison & Smith, 2018). Specifically, Harrison and Smith outline key regulatory vulnerabilities that can lead to an event. Licensing program vulnerabilities are rooted in the initial credibility given to the technical analyses the licensee reports in its application. Applying too much credit to the accuracy of the technical analyses or the validity of the underlying assumptions can expose other vulnerabilities. Those vulnerabilities may include:

- An over-reliance on the licensee's technical analyses to prioritize and define the scope of the review and
- No verification of the licensee's technical assumptions underlying the technical analyses.

Vulnerabilities in the licensing program can affect the oversight program should inspections over-rely on the results of the licensing review to plan for inspections. As Figure 8 shows, when technical assumptions are unchallenged in the licensing and oversight programs of either the licensee or regulator, the conditions are set for an event to occur.

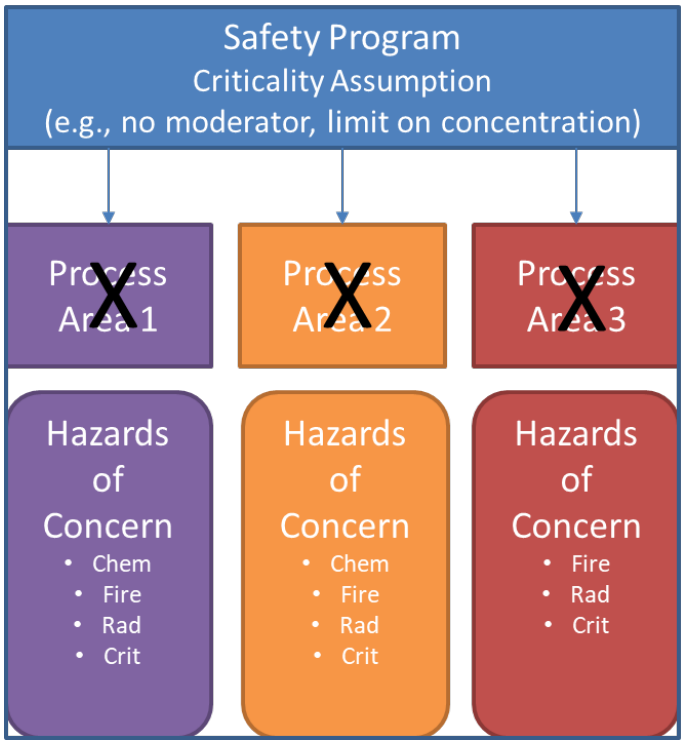


Figure 6: Processes in Facility A that may be affected from criticality assumptions made in the safety program.

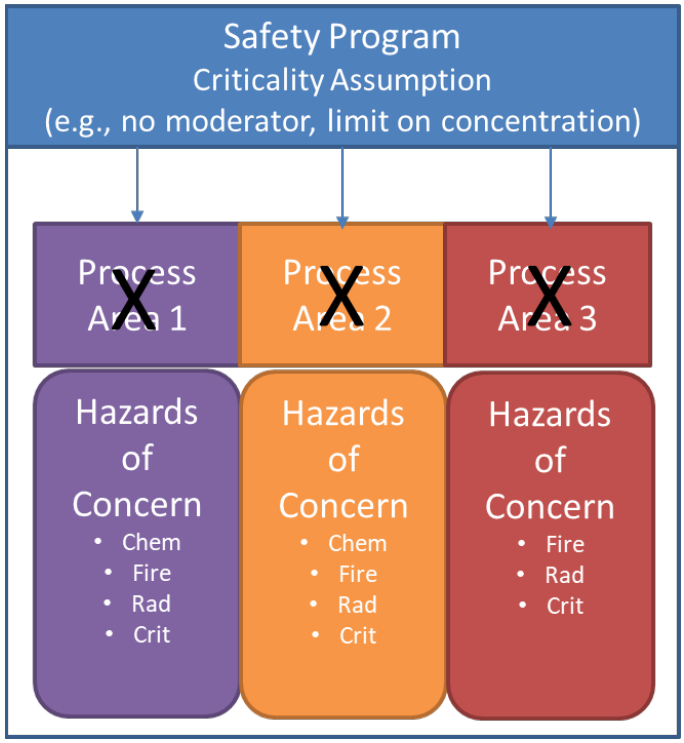


Figure 7: Processes in Facility B that may be affected from criticality assumptions made in the safety program.

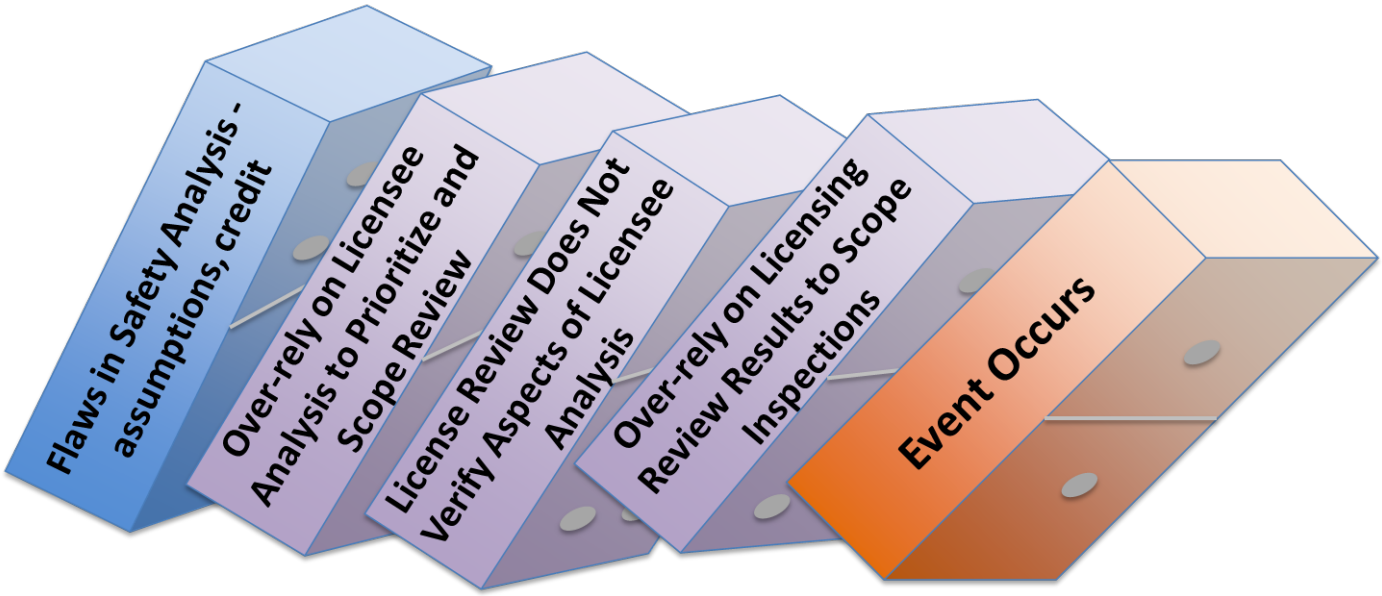


Figure 8: Regulatory domino-effect of unchallenged technical assumptions in a safety analysis.

Harrison and Smith apply the example from Information Notice 2016-03 to demonstrate the propagation of unchallenged technical analyses through regulatory licensing and oversight programs. Harrison and Smith discuss the results of a lessons learned activity the USNRC conducted after the event described in IN 2016-03 (United States Nuclear Regulatory Commission, 2017). The results showed that USNRC license review guidance does not establish a level of review nor provides specific guidance for reviewing processes and systems the licensee determines are low risk. This lack of guidance resulted in license reviewers not reviewing the ventilation and scrubber system in any depth, including no challenge to the assumption of low uranium concentration. Furthermore, because the licensee determined the system to be low risk, the USNRC did not consider this system for detailed inspection. Several inspectors noted that had the system been part of a detailed inspection, it is likely that the inspectors would have identified the licensee's deficiencies.

IV. Conclusions

The authors discussed lessons learned from an analysis of recent USNRC FC OpE events. Through generic models and specific examples, the authors demonstrated these lessons learned and emphasized their generic applicability to the fuel cycle industry. Of particular importance is the complete and accurate analysis of facility conditions, re-validation of technical assumptions and the verification of accident analyses through operational data.

For all the events described in Sections II and III, licensees addressed the issues identified through their corrective action programs under the oversight of the USNRC. Corrective actions included re-evaluations of the systems in question, along with implementing new safety controls. Licensees also conducted extent of condition investigations to explore the generic impact of those events on other systems in their facilities.

Also, for the events discussed in Sections II and III, the USNRC took regulatory action to ensure licensees continued safe operations and complied with the regulations. These actions included supplemental and reactive inspections and the issuance of orders and violations. The information notices cited in Sections II and III further illustrate the USNRC FC OpE Program's mandate to share information with the industry, including recommendations to prevent reoccurrence. Those recommendations included:

- Challenging assumptions to verify their bases,
- Investigating system dependencies to ensure that selected safety controls take those dependencies into consideration;
- Ensuring equipment and manual actions are capable of achieving the intended function;
- Critically reviewing analyses, assumptions, bases when planning and implementing changes to the facility, and
- Periodically re-verifying analyses and assumptions with operational data.

Furthermore, given that the USNRC pursues its mission on a platform of continuous improvement, the lessons learned activity discussed in Section III yielded recommendations that are being enacted to improve licensing and oversight programs, including the revision of guidance for license review and inspection planning.

V. References

Harrison, D., & Smith, A. (2018). Perceived Low Risk Processes Can Be Important - Lessons to a Regulator Based on a Nuclear Fuel Facility Process Event. *Probabilistic Safety Assessment and Management 14* (pp. 1-9). International Association for Probabilistic Safety Assessment and Management.

United States Nuclear Regulatory Commission. (2015). *Information Notice 2015-08, Criticality and Chemical Safety Events Involving Unanalyzed Conditions and Unanticipated Unavailability of IROFS at Fuel Cycle Facilities.* Washington, D.C.: United States Nuclear Regulatory Commission.

United States Nuclear Regulatory Commission. (2016). *Information Notice 2016-03, Uranium Accumulation in Fuel Cycle Facility Ventilation and Scrubber Systems.* Washinton, D.C.: United States Nuclear Regulatory Commission.

United States Nuclear Regulatory Commission. (2017). *Report on Lessons-Learned from the Westinghouse Uranium Accumulation In Scrubber And Ventilation Event.* Washington, D.C.: United States Nuclear Regulatory Commission.

United States Nuclear Regulatory Commission. (2018). *Information Notice 2018-05, Long-Term Fissle Material Accumulation or Improperly Analyzed Conditions at Fuel Cycle Facilities.* Washintgon, D.C.: United States Nuclear Regulatory Commission.