Addressing Fire Safety “the right way”

Robert Kalantari  
President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: rbk@epm-inc.com

Thomas Jutras  
Vice-President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: thj@epm-inc.com

Paul Ouellette  
Vice-President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: pro@epm-inc.com

Abstract

The paper discusses the evolution of fire safety regulations in the United States since the 1975 Browns Ferry fire. It discusses the challenges the nuclear power industry had with the original, unrealistic deterministic rule and the reasons why, 20 years later, risk-informed methods were introduced. The paper will discuss in-depth why addressing fire safety has been one of the most challenging and costly regulation for US NPPs. The paper analyzes the problems with the original proposed regulation and the efforts the US nuclear power industry took to address this complex regulation. The paper will also provide key lessons learned, and provide methods and solutions for addressing fire safety, “the right way” which will be essential for other countries facing strict fire safety regulations.

1. BACKGROUND

The significance of the issue of fire safety at nuclear power plants was made evident by the impact of the fire at Browns Ferry in the US in 1975. In this fire which was started by an employee using a lit candle to check for air leaks, the fire damage extended from the cable spreading room into an adjacent area in the unit 1 reactor building and impacted approximately 1600 cables which affected two separate units at the site. Electrical cables shorted together and grounded to their supporting cable trays and conduits, resulting in the loss of control power associated with required equipment. All of the emergency core cooling systems for the Unit 1 reactor were rendered inoperable and portions of Unit 2’s systems were likewise affected [1]. The fire and its aftermath revealed some significant inadequacies in design and procedures related to fires. The fire protection programs in the U.S. today, as well as many other countries across the globe, are a direct result of this fire and its lessons learned.

Today, fire is considered a major or even dominant contributor to the total risk of core damage for most plants. Based on the similarities of many of the nuclear plant designs globally, and the fact that fires can occur anywhere, this nuclear safety issue is considered universal in nature. The solutions outlined below are, therefore, also considered to be effective universally and this has been witnessed through our experience internationally in Canada, Europe and Asia.

2. US REGULATIONS

Prior to the Browns Ferry Fire, Title 10 of the Code of Federal Regulations Part 50 (10 CFR 50) Appendix A, General Design Criteria (GDC) 3 [2] formed the basis for regulatory acceptance of fire protection programs in the US. The requirements of GDC 3 are broad and provide no specific details with regard to ability to safely shutdown.

In the early days following the Browns Ferry fire, regulations were developed in the US to make fire protection measures more robust. These early regulations, however, did not address the concept of fire safe shutdown adequately and in many cases were implemented in a manner that provided little safety benefit while costing utilities tens of millions of dollars.

While several fire safety concepts were developed soon after the Browns Ferry fire, it took more than twenty (20) years before the concepts were sufficiently understood and documented such that some consistency in the
nuclear industry was achieved. Even today, however, complete consistency has not been reached and the approach to some concepts (e.g. multiple spurious operations) remains dynamic and unsettled.

3. **BTP APCSB 9.5-1.** "GUIDELINES FOR FIRE PROTECTION FOR NUCLEAR POWER PLANTS" MAY 1, 1976 [3]

Branch Technical Position (BTP) APCSB 9.5-1 was a quick response to the Browns Ferry fire and provided guidelines acceptable for implementing fire protection criterion for nuclear reactor power plants. The primary purpose of the Fire Protection Program for nuclear power plants is to maintain the ability to perform safe reactor plant shutdown functions and to minimize radioactive releases to the environment in the event of a fire. This BTP relied on Regulatory Guide 1.75 [4] for criteria for cable separation distance. Appendix A to BTP provides specific guidance on the preferred and, where applicable, acceptable alternatives for fire protection programs at nuclear facilities whose construction permits were docketed prior to July 1, 1976, and applies to plants that were under review, under construction or operating prior to July 1, 1976.

The BTP and Appendix A to the BTP provided detail design methods and requirements for various plant areas with regard to the need for systems such as fire suppression and detection systems and features, and required performing a detailed fire hazards analysis. It also provided very general requirements for separation of plant safety related systems, with no specific details, other than stating: “Separate redundant safety related systems from each other so that both trains are not subject to damage from a single fire.”

While meeting the requirements for fire protection system and feature upgrades was relatively straightforward, meeting the safe shutdown requirements was not practical and plants were unable to show compliance to the requirements. What BTP 9.5-1 and Appendix A to the BTP did not completely address was Post-Fire Safe Shutdown capability.


By the late 1970s, the majority of operating plants in the US had completed their analyses and had implemented most of the fire protection program requirements of Appendix A to the BTP. In most cases, the analysis and the proposed modifications by the utilities were reviewed by the US NRC and were found to be acceptable. However, the issue that remained unresolved was addressing safe shutdown, and the requirement for developing an alternative shutdown capability in the event of fire requiring control room evacuation.

In May of 1980, the US NRC decided to resolve this issue through the rule-making process and by February of 1981 issued a new rule, 10 CFR 50.48, "Fire Protection" and Appendix R to 10 CFR 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979". However, newer plants were subject to essentially the same technical requirements which were specified in their operating license. In July 1981, the US NRC issued Section 9.5.1 of the Standard Review Plan which describes fire safety provisions applicable to all plants licensed after January 1, 1979. In general, this document closely reflects the technical requirements of Appendix R.

The proposed rule was deterministic and mandated a strict compliance for all plant areas. It simply stated: “Ensure one train remains free of fire damage.”

This new deterministic rule made significant strides toward addressing the problem of ensuring a safe shutdown in the event of fire. In many cases, however, this deterministic rule was misinterpreted, misapplied or was impossible in some cases to comply with. The US NRC recognized the shortcomings of literal compliance to this regulation and allowed plants to apply for exemptions to demonstrate safe shutdown in lieu of literal compliance.

5. **WHAT IS FIRE SAFE SHUTDOWN ANALYSIS?**

A Fire Safe Shutdown Analysis (FSSA) is a comprehensive analysis that demonstrates those SSCs important-to-safety can accomplish their respective post-fire safe-shutdown functions. Such an analysis demonstrates that the success path SSCs, including electrical circuits, remain free of fire damage in the event of postulated fires. As required by applicable regulations, fire barriers, physical separation with no intervening combustibles, and/or automatic detection and suppression are acceptable means to provide this protection. Where a safe shutdown success path cannot be adequately protected, an alternative or dedicated shutdown success path must be identified and protected to the extent necessary to ensure post-fire safe shutdown.

The major steps involved with the Fire Safe Shutdown Analysis (FSSA) include:
- Determination of Fire Safe Shutdown (SSD) Performance Goals;
Selection of SSD Systems and Components;
- Circuit analysis for each SSD component to identify the required SSD Cables;
- Identification of physical location of SSD Cables and Components;
- Evaluate Potential Impact of Fire Hazards to SSD systems;
- Identify equipment and cable interactions’
- Document resolutions.

As can be seen from the list above, the tasks involved to address fire safety and fire safe shutdown requires not only involvement of knowledgeable fire protection engineers, it also requires a significant amount of support from mechanical systems and electrical engineers trained in the area of fire-induced equipment and circuit failures. These engineers play a large role in the performance of a successful FSSA.

6. EFFORTS AND CHALLENGES ADDRESSING THE PROPOSED REGULATION

In general addressing the requirements of BTP and Appendix A were relatively straightforward, although costly. US plants typically spent between $5 million to $50 million for the analysis and physical plant modifications. However, the efforts for addressing the safe shutdown capability during a fire was far from being done, and done per the requirements of the proposed Appendix R rule.

Literal compliance to the requirement that one train of equipment free of fire damage, is impossible when considering a full area burnout that results in complete damage to all FSSA equipment and cables in plant areas like the cable spreading room or the main control room. Also in some plant areas, it does not improve plant safety, especially in large open areas with low or no combustibles and/or hazards. Nevertheless, a number of US plants tried to meet this requirement by proposing extensive modifications to safe shutdown systems, circuits, and in many cases provided three hour raceway barrier protection where no fire hazards existed, but they still did it to meet the requirements of the rule. The modifications were very costly. By the late 1980s, every utility had completed “an analysis” and millions of dollars were spent for the analysis. In addition, millions of dollars were spent modifying the plant. The US NRC also granted several hundred exemptions as part of this process. However, not everyone (i.e., the utilities and vendors) had the same interpretation and understanding of the regulation.

Upon further review in the late 1990s, the US NRC inspectors found new problems with fire induced circuit analysis and also identified concerns about Themolag™ fire barriers that were used as raceway protection. The fire barrier material did not meet the qualification criteria. The industry tried to resolve this issue by reanalyzing their plant and in some cases proposed manual actions in lieu of compliance to the deterministic rule. The industry also tried to defend their position by offering fire testing of cables. This was deemed unfavorable to the industry as the fire test resulted in failures that were not originally anticipated. This resulted in a new requirement for consideration, multiple concurrent spurious operations, due to multiple concurrent circuit failures occurring during the fire.

7. NEW OPTIONAL REGULATION, PERFORMANCE BASED APPROACH

Fire science has evolved during the many years since the early regulations and with it so have the fire safety regulations. An effort to develop a Performance-Based standard by the National Fire Protection Association (NFPA) started in the mid-1990s. The standard, NFPA 805 [7] was developed by the Technical Committee on Fire Protection for Nuclear Facilities. The technical committee included several fire protection and fire safe shutdown engineers from the US nuclear utility industry, the insurance industry and the US regulator, the NRC. The standard was approved and issued by NFPA in 2001, and later on endorsed by the US NRC (with some exceptions) as a new RIPB compliance rule on July 16, 2004.

This new optional regulation allows the use of performance-based analysis and fire modeling tools as well as probabilistic risk assessment to determine compliance. Driven in part by the results of the industry cable fire tests mentioned above, and corresponding new interpretation of the fire protection rule to consider multiple concurrent spurious operations, this option provided utilities with an alternative to the deterministic approach of demonstrating compliance with the US fire protection regulations. To date, NFPA 805 has been adopted by approximately half of the operating US plants.

8. WHAT WORKED AND WHAT DID NOT WORK SO WELL WITH RIPB APPROACH

This new RIPB compliance rule change required the creation of hundreds of pages of new regulation and supporting guidance documents beyond NFPA 805 in the form of NUREGs, Regulatory Guides, NEI
Implementation guides, Frequently Asked Questions (FAQs), etc. Unfortunately, this complex compliance option proved costly and did not get implemented smoothly for several reasons. Although there was a pilot process to implement the new approach at two sites, regulatory incentives resulted in most plants adopting the new rule to commit to schedules which caused them to perform the transition at essentially the same time as the pilots. This defeated the purpose of having the pilot plants vet the process, which in turn caused significant iteration, rework and delays. Two other major contributors to the cost were the extensive revalidation of the existing fire protection licensing basis mandated by the new rule in order to transition from deterministic to risk informed regulation, and the requirement by the regulator to perform a risk assessment, which required plants to perform full fire Probabilistic Safety Analysis (PSA). Fire PSA identified high risk plant areas which required extensive modifications and huge cost.

However, in the end, utilities that performed a RIPB analysis recognized significant safety benefits by identifying and addressing hidden risks in areas considered “compliant” with the existing deterministic rules. The varying results of these RIPB analyses performed in the US revealed that it was critical for the analysis team to have a sound understanding of the fire hazards and corresponding scenarios and how to model them, as well as being very cognizant of the subsequent impact to electrical circuits, components and associated plant safety systems. Those that performed the analysis properly saved millions of dollars over those who didn’t by achieving this increased level of safety without the need for significant unnecessary plant modifications.

9. A REASONABLE APPROACH TO ADDRESS FIRE SAFETY AT NPPS

As discussed in this paper, deterministic compliance is not practical, nor does it improve plant safety in all plant areas. Assuming all cables will fail due to a deterministic fire in an area that contains no hazards and protecting such cables in order to achieve compliance with a rule does not provide any appreciable improvement to plant safety. A performance based method, with realistic engineering evaluation based on qualitative and/or quantitative assessment of the plant design will provide the best results. Based on this, instead of separating plant redundant systems by three hour barriers or 6 meters of separation in all plant areas, the redundant systems should be separated adequately, commensurate with the hazards in the area. This process is fully documented in the NFPA 805 standard. It should be noted that a very similar performance based technique was utilized to address fire safety in all Canadian plants, even before NFPA 805 became a standard in 2001. Canadian regulation for addressing fire safety was initiated by CSA N293-95, and later on revised in 2007 and 2012 [8]. This standard allowed the use of a performance-based approach to fire safe shutdown for all Canadian nuclear plants.

A performance based analysis is not less onerous than a deterministic one. It requires a very similar effort to that of the deterministic analysis discussed earlier, and in some cases, may require more effort to collect and analyze the data, especially the fire modeling efforts. However, in the end, it does provide better results by focusing on plant areas that are vulnerable to fire damage to safe shutdown systems from real fire hazards and realistic fires. Performance based approaches provide focused resolutions and less plant modifications that provide little or no safety benefit. A high level overview of the analysis and the screening process for each plant area is presented below.

Screen 1, no credited safe shutdown equipment and/or cables in the fire zone. For screen 1, evaluate fire zone boundaries and fire hazards. If the zone has no fire hazards, no further analysis is necessary. If fire hazards exist, postulate a realistic fire based on the hazards, and potential impact of fires on adjacent screen 2 or 3 fire zones.

Screen 2, all performance goals can still be met, even with loss of all credited equipment and/or cables in the fire zone. For screen 2, evaluate fire zone boundaries and fire hazards. If fire hazards exist, postulate a realistic fire based on the hazards, and potential impact of fires on adjacent screen 2 or 3 fire zones. Assume that no single fire could impact redundant safe shutdown systems if fire can propagate into adjacent zones. Identify where performance goals may be impacted due to fire spread. In addition, combine screen 2 fire zones where possible.

Screen 3, one or more performance goal cannot be met due to loss of all credited equipment and/or cables in the fire zone. For screen 3, evaluate fire zone boundaries and fire hazards. If fire hazards exist, postulate a realistic fire based on hazards and potential impact of fires within the subject zone and on adjacent screen 2 or 3 fire zones. Assume no single fire could impact redundant safe shutdown systems. Identify where performance goals may be impacted due to fire spread.

The following are typical methods for resolving fire impact on safe shutdown systems:

- Removing the fire hazards from the area if feasible;
- Reducing the impact of the hazards (i.e., installing dike around a pump, installing heat shields);
— Protecting the cable trays by installing heat shields;
— Installing or upgrading the detection and or suppression system;
— Provide additional barrier protection;
— Operator manual action if feasible and practical;
— Cable protection, i.e., wrapping raceways should be considered as a last resort.

It is important to note that a deterministic or Performance Based Fire Safe Shutdown Analysis provides an assessment of plant’s capability to safely shut down the plant during a postulated fire. However, it does not provide an indication of plant risk; performance of fire PSA provides insights to plant risk, i.e., Core Damage Frequency (CDF), due to fire.

For example, a deterministic and/or Performance Based Fire Safe Shutdown Analysis may show that a plant can achieve safe shutdown during a fire that adversely impacts one train of emergency power system in the plant. While in general this scenario meets the requirements for safe shutdown during that fire, losing one train of emergency power without having the offsite power available will increase plant’s risk and CDF by one or sometimes by two orders of magnitude. Simply said, Fire PSA identifies additional vulnerabilities due to fires, and provides insights necessary to minimize the risk of fire to a nuclear power plant.

10. RESOURCES AND MANPOWER

In order to effectively perform a Fire Safe Shutdown Analysis (FSSA) using deterministic or performance based approaches, the proper inputs must be provided. This includes general plant arrangement drawings, P&IDs, electrical one-lines and schematics, etc. as well as existing plant databases (e.g., cable and raceway system, plant equipment database, etc.). This information will be used by qualified Mechanical and Electrical engineers to build an accurate FSSD analysis model to allow for evaluation of potential equipment and cable interactions.

Due to the enormous amount of data involved in an FSSA it is recommended to have an analysis software tool that allows the project team to automate the safe shutdown analysis. The software tool would utilize an analysis model, created by the project team, composed of plant systems, equipment and cables, and their physical locations. There are many advantages to using software tools as opposed to performing the analysis manually including efficiency, accuracy, and ease of maintenance of the analysis. This approach enables engineers to analyze each fire zone/fire area with the click of a button and display the analysis model graphically; enabling the analyst to view all components in either an entire layered model or selected portions of the analysis model further assisting them to quickly evaluate the results and postulated resolutions.

Performing an FSSA is a tedious and complex process. Even with qualified engineers using the proper tools and accurate inputs, a complete analysis is extremely time-consuming. At a minimum, this effort, from beginning to end, usually requires a dedicated team of 4 - 6 FTEs and takes in the range of 15,000 - 25,000 man hours.

11. CONCLUSION

Performance based fire safe shutdown analysis that focuses on real fire hazards and realistic fire scenarios will provide an accurate and realistic analysis and is cost effective. Protection in the form of physical separation of critical components and cables as well as the effective use of active and passive fire protection systems and features based on these results assures that no single fire could compromise plant safe shutdown goals.

REFERENCES