AECL'S USE OF FMEA AND OPEX FOR FIELD SERVICE TOOLING AND PROCESS DEVELOPMENT, IMPLEMENTATION AND IMPROVEMENT: A MODEL FOR THE FUTURE

E. Cox, R.F. Dam and E. Wilson
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

Abstract

Failure Modes and Effects Analysis (FMEA) is a systematic and rigorous process applied to new or complex systems to predict system failures and assist with the development of mitigating strategies. The process is especially beneficial when applied to higher-risk applications such as nuclear systems. FMEA may be used for design verification and maintenance program development.

For field service tooling, FMEA is complimented well by operating experience (OPEX) and continuous improvement initiatives. FMEA is generally conducted while developing systems and processes to ensure safe and successful implementation, while OPEX is fed back into the system design and operation to improve those systems and processes for subsequent field applications.

This paper will explore these techniques as they have been applied to AECL's CANDUclean™ system. The portable CANDUclean system is employed to mechanically clean the inside of steam generator (SG) tubes in CANDU® nuclear power plants. During normal plant operation, the steam generator tubes in the heat transport system develop a build-up of magnetite on their internal diameter, which decreases heat transfer efficiency, impedes SG maintenance activities and increases the radiation fields in and around the boilers. As part of a regular plant aging management routine, the CANDUclean system is used to remove the magnetite layers. The nature of this work includes risks to personnel safety, however by continually applying FMEA and other improvement initiatives, safety and system effectiveness are maximized.

This paper will provide an overview of the integrated continuous improvement approach applied to the CANDUclean system and consider the value of strategies when applied to field service tooling and CANDU systems.

1. Introduction

Failure Modes and Effects Analysis (FMEA) is a systematic and rigorous process applied to new or particularly elaborate systems, components or processes to predict failures and assist with the development of mitigating strategies. The process was originally developed by the United States Armed Forces for military applications, and was later adopted for use in aerospace/rocket development. Today FMEA is used in most industries including automotive, electronics and the general manufacturing sector. The FMEA process is especially beneficial when applied to higher-risk applications like nuclear systems, and helps to ensure safe and effective system operation.

For field service tooling, FMEA is complimented well by the use of operating experience (OPEX) feedback and other continuous improvement tools. FMEA is generally conducted while developing systems and processes to ensure safe and successful implementation, while OPEX is fed back into

™ CANDUclean is a trademark of Atomic Energy of Canada Limited
® CANDU is a registered trademark of Atomic Energy of Canada Limited

the system design and operation to improve those systems and processes for subsequent field applications.

This paper will explore the various continuous improvement strategies applied to AECL's CANDUclean system and consider the value of this approach when applied to field service tooling and CANDU systems.

2. FMEA criteria, methodology and application

FMEA is described as a process "…to systematically evaluate and document, by item failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability, and maintenance requirements" [1]. The method is generally applied to systems and processes with a high degree of complexity, those with significant safety concerns and/or those which are considered first of a kind (FOAK) applications. A system or process that meets one or more of these criteria may typically be subject to some form of FMEA.

FMEA is employed to provide early indication of all catastrophic and critical failure possibilities so they can be eliminated or minimized through design correction. The process also provides a means for designers to understand and appreciate system response to failures.

FMEA is most effectively applied as a verification tool, ideally during the initial design process. In some cases, FMEA may be applied as part of a root cause analysis, and may also be carried out to a level of detail sufficiently specific to identify precise maintenance requirements. In general, the FMEA approach can be tailored to suit the requirements of the system or component under study and serve the needs of the assessment. The overall effort associated with performing FMEA can be minimized by applying the methodology early on in the design process.

Any analysis may typically be conducted using one of two approaches, quantitative or qualitative. While a quantified approach uses numerical data, for instance metrics or statistics, a qualified approach draws on data such as words and observations. As an important part of Plant Life Management (PLiM) activities at AECL, FMEA has been developed into a standardized, *qualitative* method, built upon conventional aging management activities, and thus the qualified approach is considered further in this paper.

The analysis process can be more specifically referred to as a Failure Modes, Effects and Criticality Analysis (FMECA), which takes into account the severity of the effects of component and system failures. For the purposes of this paper, the term FMEA will be used.

2.1 FMEA methodology

The FMEA analysis sequence is carried out as follows:

- Gather system information and compile a list of components.
- Define system functions and functional failures.
- Assign failure modes to each component.
- Determine the effects of the component failure on overall safety and system performance, assuming no mitigating strategies are in place.

- Based on criticality of the failure effects (consequences of failure), streamline the equipment list to include only critical components in further analysis.
- Determine the failure cause(s) that could result in the assigned failure mode(s) for each component.
- Identify mitigating strategies (controls) in place to reduce or eliminate the occurrence of identified failure causes; suggest implementation of additional strategies (actions) where controls are lacking.

As part of the qualitative analysis, a list of generic failure causes is applied, rather than relying on more specialized component-specific failure causes. This method engages the system designers in the FMEA thinking, invoking their expertise to further specify the failure causes with respect to individual components. This in turn helps to identify explicit mitigating strategies where required, and improves the efficiency of the process. The generic failure cause categories include:

- **Design Error**: This failure could include incorrect sizing, incorrect material selection, failing to address all design requirements, etc.
- **Manufacturing Error**: This failure cause encompasses manufacturing & Quality Assurance (QA)/Quality Surveillance (QS) related issues.
- **Mechanical Failure**: Component fails to perform any number of internal functions.
- **Operator Error**: Any operations the operator performs that could affect the component function.
- **Support System Failure**: This is the failure of systems that are required to operate the component. These could include power supply, air supply, etc.

In a similar manner, the analysis results are categorized into common groupings of potential issues. For example, the FMEA may find that there are several system processes that require enhanced operating instructions. These may be further categorized as requiring improved documentation, procedures or training. In general, the controls and actions resulting from a FMEA can be categorized using this technique, which again serves to engage the system designers and accelerate the process. By pre-defining these categories and standardizing the process, consistent analysis results can be produced independent of the individual system assessor. Employing the use of a specially designed software tool further expedites and standardizes the process.

2.2 FMEA software

The AECL-designed software tool SYSTMS™ (SYstematic STrategy for Maintenance and Surveillance) has been used in performing streamlined reliability-centred maintenance analyses, more commonly referred to as Systematic Approach to Maintenance (SAM) assessments. Given that some of the SAM principles are shared with the FMEA approach, the tool was easily modified to cater to FMEA methodology. A prototype module was developed for use in performing and tracking the FMEA process and results.

SYSTMS facilitates the analysis by providing access to generic component information, organizing the system components, performing and tracking the analysis and action disposition activities, and storing the data. This allows for quick and easy review and updating of the results

™ SYSTMS is a trademark of Atomic Energy of Canada Limited as required, meaning design and process changes can be accommodated in a reasonable timeframe.

Given that the FMEA prototype version of SYSTMS was developed based on an existing, day-to-day tool, users were able to adapt to the new software with minimal effort. Furthermore, the tool provides a consistent, well-structured approach to each analysis, which ensures the means to teach new analysts to perform FMEA in an efficient, reliable manner.

3. CANDUclean process system

The portable CANDUclean system is employed to mechanically clean the internal diameter (ID) of steam generator (SG) tubes in CANDU nuclear power plants. During normal plant operation, the steam generator tubes in CANDU reactors develop a build-up of magnetite on their internal diameter, which decreases heat transfer efficiency, impedes SG maintenance activities and increases the radiation fields in and around the boilers. As part of a regular plant aging management routine, the CANDUclean system is used to remove the magnetite.

3.1 Process system description

The system uses a remotely controlled manipulator to connect with groups of tubes at the cold leg side of the steam generator, blasting stainless steel shot into the tubes in order to mechanically remove the magnetite layers. A collection system is used on the hot leg side to collect the shot and magnetite removed from all tube-sets. Shot and magnetite are conveyed from the collection equipment back to a separation system, where the shot is separated out and reused, and the magnetite is delivered to a waste container.

The process system is technically complex, considering the mechanical and electrical equipment modules, the control system hardware and software implemented to remotely operate various system equipment, and the relationships and communications between system components. Aside from the physical tooling, there are other essential details pertaining to system operation, such as engineering design and procurement, and rigorous procedures employed to manage the field implementation. Unlike similar commercial sandblasting systems, the need to maintain a closed system with no material releases is critical, as the magnetite removed from the steam generators is highly radioactive and personnel safety is paramount. These factors present unique challenges and stringent operating requirements.

3.2 System field implementation

<u>3.2.1 System Configuration</u>

While the basic principle of operation remains the same, the system may be alternatively configured and implemented for a variety of field applications, for example the cleaning of external preheaters (PH). Each application presents its own unique challenges, such as waste management, radiation dose, foreign materials exclusion (FME), etc.

<u>3.2.2 Maintenance</u>

Unlike fundamental reactor systems that operate continuously, the CANDUclean system is used for only short-term application, generally during regularly scheduled reactor outages. The system is then stored until it is used again for another short-term assignment. As such, maintenance activities are not assigned in the same way as typical reactor system maintenance programs; instead long-term maintenance activities – such as spare parts management and component inspections – are implemented, generally between campaigns and as required.

3.2.3 Implementation

Due to the system complexity and the safety implications related to the work, the reality is that field implementation may not produce optimal results, and unexpected events can and do occur. The most recent implementation of the CANDUclean system has been on steam generators at each unit of Bruce Nuclear Generating Station (BNGS) 'B'. Problems were encountered during the first application, and though the immediate issues were dealt with accordingly, concerns remained regarding the robustness of the system as a whole, prompting further evaluation of the system equipment and operating procedures. In order to ensure an in-depth study was completed, a system FMEA was prescribed.

4. CANDUclean and FMEA

A systematic and rigorous FMEA was performed on the CANDUclean system, resulting in numerous recommendations for system and process improvements. Specifically, control system constraints were tightened; equipment design and function were verified through inspection, testing or analysis; and documentation and training requirements were enhanced. As a result, the CANDUclean system performance improved significantly on subsequent campaigns.

An upcoming campaign at BNGS is planned for the ID cleaning of the external preheaters. Given the configuration changes needed to apply the system for PH cleaning (heightened FME concerns, different operating environment, etc.), a review and enhancement of the system FMEA was completed. Performing this review ensured that the FMEA process was applied to new components and functions introduced as a result of system modifications. In addition, the review captured any changes to criticality rankings as a result of system design changes.

4.1 'Maintaining' the results

As noted previously, the FMEA methodology includes assigning controls, or mitigating strategies, associated with the identified potential failure causes. While a specific set of control categories was assigned for the CANDUclean system FMEA, this is an area that can be either generically applied, or custom-tailored to suit the application.

While other analyses similar to FMEA (for example, SAM) are often performed with a view to developing specific maintenance strategies, the FMEA performed on the CANDUclean system often employed 'maintenance' itself as a control. Given the unique, relatively short-term nature of the CANDUclean system applications, maintenance takes on several different forms:

1. **Mission critical maintenance**: This includes activities performed as needed throughout the system operation in order to achieve mission success, for example spare parts replacement or component repairs.
2. **Pre-operational maintenance**: This includes activities performed in advance of system commissioning that ensure the system will operate as intended, for example instrument calibration.

3. **Long-term maintenance**: This includes activities performed between campaigns to ensure that system equipment remains safe to operate, for example, taking thickness measurements of pressure vessel walls.

A comprehensive maintenance program can prolong the life of system equipment and ensure safe and successful operation over numerous campaigns. By drawing attention to the importance of maintenance through the FMEA findings, a culture of *maintenance-based design thinking* is promoted, which involves designing systems and components to be readily maintainable. This ties in with an overall *FMEA-based design approach*, which has been generally adopted by CANDUclean system designers over the course of the analysis process. This approach means system engineers try to design for anticipated failures, thus incorporating FMEA into the design process and, often, eliminating the potential for said failures altogether. When systems and processes are designed using FMEA thinking, future analysis efforts are minimized, and a sensible design results.

4.2 FMEA field implementation issues

While an in-depth FMEA can result in significant system improvements, what looks good on paper does not always translate directly to the field. The biggest issue facing the efficacy of FMEA is the process of turning results into actions. A thorough analysis will not result in significant system improvements unless the recommendations are tangibly implemented. Herein lies a common problem, where well-intentioned suggestions for improvement may not be entirely plausible for field implementation. This is due in part to a disconnect between system analysts – who typically are not the system engineers – and system operators and designers. In addition, there may be implicit requirements, which the analyst may take for granted as being in place, associated with requisite actions. If the analyst does not explicitly describe the assumed requirements, the system designers may not implement the action correctly.

For example, the CANDUclean system FMEA identified many ways to augment the system operating procedures that would result in enhanced safety and efficiency. However, improved procedures also rely on the following conditions in order to be truly effective:

1. **Procedures are written so as to be practicable under in-situ field conditions**. This requires an understanding – on behalf of both the FMEA analysts (when making procedural recommendations) and the procedure authors – of circumstances typical to the field environment.
2. **Operators are appropriately trained to the procedures prior to field deployment**. This requires a rigorous training plan and acceptance of the procedure validity on the part of the field workers.
3. **Operators understand the context and significance of the procedure steps**. This requires the operators to have some knowledge of the FMEA activities and the particulars of system design and operation.
4. **Procedural use and adherence are enforced on the job**. This requires specific training, as well as tight project management and effective leadership.

These conditions are generally beyond the control of the FMEA analyst, thus the system designers and operators must have a bigger picture understanding of the requirements for implementing FMEA results in the field. In a similar manner, a FMEA action item may indicate the need for a test, but does not provide details of how the test is to be designed or conducted, or what results may be expected.

It is incumbent on the system designers and operators to determine these fundamental details, and to ensure that suggested actions are implemented appropriately. This can be accomplished easily when the system designers adopt the FMEA-based design approach outlined above. In the case of the CANDUclean system designers, once this approach was embraced, tests were often conducted before even being prescribed by FMEA results.

4.3 Sources of knowledge

To avoid some of the above-described problems associated with field implementation, it is imperative that system analysts develop a solid understanding of the system as a whole, and how the components work together to accomplish the system goals. Knowledge of the field implementation process is also vital. In essence, the analyst need not only understand the system design and operating principles, but the field environment, system surroundings, installation, removal and operating procedures, and project scheduling. This way, recommendations for system enhancements can be provided in a way that allows for their successful implementation.

Overall knowledge of system implementation and operation cannot be gained overnight. In most cases, it is not feasible to send a system analyst into the field to receive this education. As such, effective communication with system operators and designers provides the crucial details needed to effectively complete the FMEA. This is accomplished in part through the regular feedback of operating experience (OPEX).

In the case of the CANDUclean system FMEA, the analysts performed walkdowns of prototype equipment to gain an understanding of system operation and function. Further communication with system engineers and designers provided ancillary knowledge.

4.3.1 OPEX

Following the first field implementation of the CANDUclean system at BNGS after FMEA-based system changes were made, OPEX was provided to the analysts regarding system performance and effectiveness of the FMEA-based enhancements. While system performance was considerably better than the previous campaign, there was still room for improvement, both to the system and the FMEA process.

5. Continuous improvement process

5.1 FMEA/OPEX continuous improvement process

In general, feedback from system implementation provides information as to how equipment actually behaves under field conditions, versus the expected results based on design testing and analysis. In addition, experience related to individual component failure modes, where applicable, feeds back nicely into FMEA and is used to enhance the analysis.

Specifically, the continual feedback of OPEX serves two distinct purposes:

1. Provide system engineers and designers with valuable lessons learned during system operation, which are then used to enhance system design and operating parameters to improve future performance.
2. Provide system analysts with feedback as to how successful the implementation of FMEA actions was. This in turn helps to fine-tune the FMEA process in an iterative manner over time.

Thus, FMEA and OPEX form a mutually beneficial relationship, with one always helping to improve the other.

Using the example of the CANDUclean system, the following sequence of events occurred:

1. Initial system design and testing.
2. First site implementation – non-optimal results.
3. System FMEA performed; various system and process improvements made.
4. Second site implementation – improved results; some legacy issues remained.
5. OPEX and lessons learned review, including review of FMEA based on site feedback. System and documentation improvements made in consultation with FMEA analysts.
6. Third site implementation – superior results, no significant issues.
7. OPEX and lessons learned review, minimal involvement from FMEA analysts.
8. Fourth site implementation – successful campaign with no significant issues.

By the time step 6 was reached, system engineers and designers were already using FMEA thinking and strategies while fine-tuning the system design. In addition, a FMEA of the next system application (for external preheaters) was being conducted in parallel, with results feeding back into the SG application system design where applicable.

OPEX helps to enhance the FMEA process by providing real field experience relating to failures. For example, a CANDUclean system failure considered to have considerable safety implications in theory had no significant effects in reality. Feedback of this nature prompts the analysts to refine aspects of the analysis such as the criticality and likelihood of failure. The more accurate and complete the information available to the assessors, the more precise the analysis results will be, resulting in an efficient, streamlined process.

5.2 Continuous improvement tools

Supplementary to FMEA and OPEX, a number of tools are used that contribute to the overall continuous improvement process. While each tool has its own primary purpose, it serves a secondary function to feed back into the iterative design process to continually enhance system operation.

5.2.1 Field Change Requests (FCR)

It is the nature of field services work that no matter how sound a design, constantly changing circumstances in-situ can add a level of difficulty to field implementation that cannot always be anticipated. When a design change or new procedure is required in the field, this is handled through the use of a FCR.

The site engineer fills out a form detailing the reason for the request, and providing necessary information, such as attaching a drawing for a design change, or outlining the proposed steps for a new procedure. FCRs are extremely useful at site in order to complete work in a timely manner, while still ensuring tasks are performed to the appropriate QA standards.

Often when a change or addition is deemed necessary at site, it should thereafter become part of regular operating procedures. As such, upon campaign completion, FCRs are fed back into system design and documentation as applicable.

In the case of the CANDUclean system, numerous FCRs were written at site when the existing operating procedures were insufficient to complete work that had been previously unanticipated.

After the campaign, a review of the FCRs and their associated field circumstances indicated that some of the procedures should be formally captured for future use. As such, they were incorporated into system operating manuals, which are subject to a more thorough review process than is possible in the field. Hence, going forward, the repertoire of procedural documentation remains as up-to-date as possible, ensuring a high level of QA in performing future work. Essentially, FCRs provide a means to feed back some of the lessons learned on the job.

5.2.2 Non-Conformance Reports (NCR)

A non-conformance is defined as the non-fulfillment of a requirement for a product, process or program. At AECL, a NCR is raised when requirements are not followed or when there is a quality issue. To resolve a NCR, the following actions are taken:

- Corrective Action: action that prevents the problem from occurring again.
- Remedial Action: action that fixes the problem at hand.

With respect to site work, specifically for the example of the CANDUclean system, remedial action is generally implemented in the short-term to ensure that work can proceed without significant delay, while corrective action may be taken over a longer term, for example between campaigns. In some cases, the remedial action may suffice as the corrective action as well.

When NCRs are generated at site, or throughout the course of a project, they generally result in product or project improvements. Actions resulting from NCRs can be fed back to the system engineers and designers to further augment the continuous improvement process.

5.2.3 Event-Free Tools (EFT)

EFTs are learned and adopted work practices used to minimize human performance errors, ensure competent and safe execution of activities, and support a strong safety culture based on a formal and disciplined approach to all activities.

While EFTs are generally behavior tools that are applied on-the-job to maximize safety and minimize errors, they have some use in feeding back information as well. For example, key EFTs include adopting a “questioning attitude” – an approach also required for FMEA – and conducting pre- and post-job briefings.

When employees approach their work with a questioning attitude, it may mean they inquire about a particular procedure – how something is installed, for example, and why. This can lead to changes or enhancements, particularly where the field work perspective is applied to procedures that were likely written back in the office. From a FMEA perspective, maintaining a questioning attitude means the analyst is always looking to gather pertinent information and determine the effects and consequences of decisions and actions.

Pre-job briefings are conducted to ensure that workers know what task they are performing, and identify any potential safety hazards and how they can be mitigated, and discuss any other details pertinent to the job. Post-job briefings review how the job was conducted, and any issues or problems that occurred and how to prevent them from reoccurring. Post-job briefings are conducted after equipment installations or removals, system walkdowns, maintenance activities, and after the entire campaign is complete. Through post-activity review, field supervisors and project managers may learn of issues relating to component design and operational procedures. Field workers often have valuable feedback regarding enhancements to design and operation of system equipment. This information is then fed back to system engineers and designers and implemented where applicable.

5.2.4 Record Keeping

In addition to FCRs and NCRs, other important records detailing field implementation activities may be kept, which provide another valuable resource for OPEX and worker feedback. For the CANDUclean system, journals are kept during the campaign and important activities are logged by system operators, engineers and supervisors. These logbooks provide a means to record information pertaining to system operation, unexpected events, process feedback, enhancement suggestions and much more. Upon completion of the campaign, the logbooks are reviewed to extract any useful lessons learned throughout the course of the job, and the feedback is implemented where applicable.

Other valuable records created during the campaign include the "live feedback" produced as a result of documentation mark-ups. For example, an operator may discover errors or shortcomings of a procedure during its use, in which case he or she may provide corrections directly on the document hard copy in use. When the documentation is reviewed between campaigns, these suggested improvements are considered for incorporation into the formal documentation. Through these activities, there is continual 'self-assessment' occurring, ensuring that processes and procedures remain relevant and practical from job to job.

6. Future applications

The integrated continuous improvement process described above can be applied in a similar manner to any system or application, including other field service tooling and CANDU systems. The CANDUclean system has unique characteristics due to its portability and repeated field applications. Each system, whether a portable maintenance system or an integral CANDU reactor system, will present its own unique challenges with respect to ensuring optimum performance and reducing the likelihood of failures. For example, portable field tooling and prototype equipment may be more readily accessible to FMEA analysts than a system located inside the reactor vault, making familiarization for the purposes of analysis more difficult for the latter. However, the multifaceted nature of the approach outlined above typically ensures that sufficient information is available through a unique combination of the various feedback mechanisms. For CANDU reactor systems for example, analysts may make use of the CANDU Owners Group (COG) OPEX system available online, rather than relying on feedback only from AECL employees and contractors as is the case for the CANDUclean system.

Just as the FMEA process itself can be tailored to suit the requirements of the system, the entire integrated approach can be tailored based on the available information and the nature of the system and application. Where detailed FMEA is involved, the SYSTMS tool can be used to facilitate the analysis and ensure that results are obtained in the most efficient manner. AECL has refined the process for the CANDUclean system, and is well positioned to do so for other systems and applications in the future.

7. Conclusion

The world is in the midst of a nuclear renaissance, with a focus on longer reactor design lives and extending the operating lives of existing plants. As such, aging management programs are on the forefront of nuclear engineering. The CANDUclean system has been successfully implemented as part of an overall aging management program in CANDU plants, with continuous improvement strategies working behind the scenes to ensure that the evolving technology and operations continue to produce exceptional results. Applying a systematic and rigorous FMEA review process to the system ensures that it can be operated as safely and successfully as possible, even when design or process changes are implemented. FMEA is complemented well by other feedback mechanisms such as OPEX, FCR, NCR, EFT and record keeping. Together these strategies form an integrated approach to continuous improvement that will benefit any nuclear system. In fact, FMEA is essential to the continued safe and successful operation of complex, evolving systems, and should continue to play a major role in system design processes.

8. Acronyms

AECL	Atomic Energy of Canada Limited
BNGS	Bruce Nuclear Generating Station
CANDU	CANada Deuterium Uranium (registered trademark of AECL)
COG	CANDU Owners Group
EFT	Event-Free Tools
FCR	Field Change Request
FME	Foreign Materials Exclusion
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FOAK	First of a Kind
ID	Internal Diameter
NCR	Non-Conformance Report
OPEX	Operating Experience
PH	Preheater
PLiM	Plant Life Management
QA/QS	Quality Assurance/Quality Surveillance
SAM	Systematic Approach to Maintenance
SG	Steam Generator
SYSTMS	SYstematic STrategy for Maintenance and Surveillance

9. References

[1] MIL-STD-1629A, "Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis", *United States of America Department of Defense*, 7 June 1983.