FAILURE MODE EFFECTS ANALYSIS FOR AN ACCELERATOR CONTROL SYSTEM *

S. M. Hartman†, Spallation Neutron Source,
Oak Ridge National Laboratory, Oak Ridge, TN, USA

Abstract

Failure Mode Effects Analysis (FMEA) has been used in industry for design, manufacturing and assembly process quality control. It describes a formal approach for categorizing how a process may fail and for prioritizing failures based on their severity, frequency and likelihood of detection. Experience conducting a FMEA of an accelerator subsystem and its related control system will be reviewed. The applicability of the FMEA process to an operational accelerator control system will be discussed.

INTRODUCTION

Formal failure mode effects analysis were first used for evaluating safety issues in the aerospace industry in the 1960s. It was then applied to safety in the chemical process industries, and later in the automotive industry where it was applied as a quality improvement tool [1]. FMEA provides for a standardized framework for recognizing and preventing problems before they occur. The analysis involves identifying possible failure modes for each identified function or system requirement of the design or process. For each potential failure mode, effects are identified and classified based on severity. Potential causes of the failure are enumerated and assigned values representing estimated rates of occurrence and likelihood of detection. The severity, occurrence and detection levels are used to compute a risk priority number (RPN). The severity and RPN values are then used as a means to prioritize actions and plans to reduce the frequency or the effect of the failure [2]. Recommended actions are identified and after implementation, a new RPN value is calculated . Through this iterative process, actions are prioritized to prevent future problems and improve quality.

FMEA FOR AN ACCELERATOR SYSTEM

In the summer of 2009, the cryogenics group of the Spallation Neutron Source (SNS) conducted a Process FMEA of the Central Helium Liquifier (CHL) and related systems. The scope of the FMEA was limited to the cryogenics systems for the super-conducting radio-frequency linac, but it was conducted it a way which could be expanded to other accelerator systems or to an overview of the accelerator complex as a whole. Occurrence and detection levels were based on operational experience and history. Severity levels were based on cost of potentially damaged equipment, and on downtime and availability goals for the SNS. The "cost" of downtime provided a useful metric in defining severity levels based on internal availability goals. The FMEA identified a number of potential failures which are being addressed to reduce the likelihood of occurrence or severity should the failure occur, and measures are being taken to increase the detection of problems.

The control system for the cryogenics plant came up in a number of places during the FMEA. For each potential cause of failure identified, a detection level was assigned to indicate the likelihood of detecting the fault soon enough to prevent the failure. In many cases, the detection level was directly related to the effectiveness of the alarm system. This brought up two issues related to alarm rationalization [3]. First, alarms need to be considered throughout the system design and implementation to be an effective tool. In a number of cases, the FMEA revealed places where an alarm point was not providing the expected notification or where the wrong point was chosen for the alarm. Second, if the mitigating action for the potential failure is to add alarm points, it is very easy to trade one problem, a potential failure, with another problem, alarm proliferation and overload [4].

The control system also appeared in the analysis as a potential cause of failure. Several incidents where faults in the control system interfered with operations of the cryogenics plant had been identified prior to implementing the FMEA and were one of the motivating factors towards undertaking the analysis [5]. A failure of control system hardware (input/output modules, processor, etc.) or software (errors in logic, missing fault handling, etc.), or in the control system infrastructure (servers, network) can directly lead to a failure in the CHL process or can contribute by interfering with operator control of the plant.

However, calculating meaningful RPN values (severity, occurrence and detection) for elements of the highly distributed control system proved to be problematic. The severity levels are potentially quite high for the cryogenics control system as a failure of a control system component can shut down the cryogenics plant and lead to an extensive recovery time. The occurrence level for any potential failure mode of an element of the control system was uniformly low. While failures have occurred in the control system, no systematic failures were in evidence, and mitigating responses have been taken to reduce the chance of a repeat of a previous fault. Detection was scored uniformly quite high (i.e. unlikely to detect in time) since typically

* SNS is managed by UT-Battelle, LLC, under contract DE-AC05-00OR22725 for the U.S. Department of Energy
† hartmansm@ornl.gov

little warning is available prior to a failure. The resulting RPN values for potential control system failures thus provided very little differentiation to be used for prioritization. Each subsystem received similar or identical RPN values. This can be expected somewhat based on the use of modular, standardized components throughout a distributed control system. There is little to differentiate the occurrence or detection levels as used in the FMEA of one node of the system as compared to another, leaving only the severity of the potential failure to differentiate. In contrast, highly centralized utilities such as electrical power and cooling water systems were reflected in the FMEA in a way which provided a useful measure in the analysis. Actions such as adding backup power systems or cooling systems would clearly be shown in the resulting change in RPN for a potential failure mode.

FMEA for an Accelerator Control System

To address some of the shortcomings in the cryogenics Process FMEA in prioritizing improvements to the cryogenics control system, a preliminary Design FMEA was undertaken to look at the control system. The first step was to map the relationships between various components or subsystems to indicate inter-relationships and dependencies. An example of one design diagraph, representing a global view of the control system, is shown Fig. 1. Additional diagraphs were made for software component interrelationships and for a particular rack-level assembly showing a complex series of inter-relationships.

The inter-relationship diagraph is used to identify the "drivers" to the system, i.e. those nodes with a larger number of output links have a greater potential impact in the event of a failure then do nodes with fewer output links. In the FMEA, additional focus is applied to these subsystems to help prioritize effort to eliminates problems.

The Design FMEA continued with a preliminary review of control system functions and requirements, and then identification of potential failure modes and their effects. For the potential causes of failure, an attempt was made to assign a meaningful RPN value. But as with the controls elements of the cryogenics Process FMEA, the format of the FMEA allowed for little differentiation in prioritization. Severity was dependent on which system included the controls component. Opportunities for detection in time to avert a failure on a production system are limited. Occurrence levels were uniformly low and depended more on how subsystems were grouped then actual failure rates.

For the purpose of prioritizing actions to improve availability for the cryogenics system, the controls related issues were evaluated outside the FMEA process. Areas for improvement based on past performance, available upgrade options, and identified system weaknesses were identified and prioritized, and then folded back in to the FMEA.

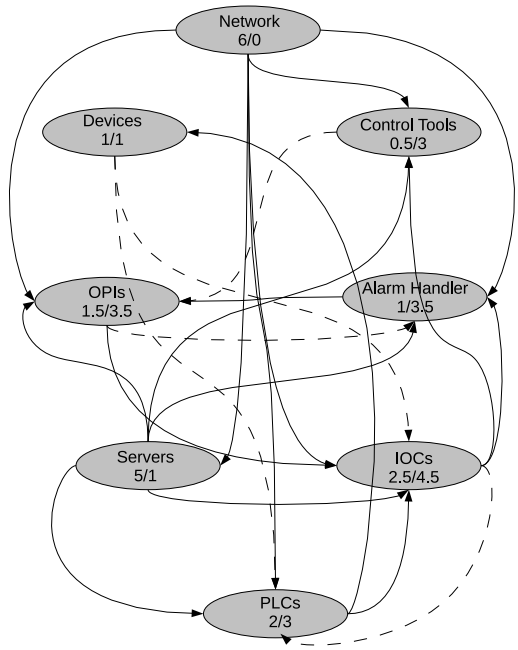

Figure 1: Controls design FMEA inter-relationship design diagraph showing subsystem dependencies. Each subsystem labeled with sum of output links / input links. Solid lines indicate strong dependency (value=1); dashed lines indicate weak dependency (value 0.5).

CONCLUSION

The preliminary attempt at a Design FMEA for the distributed control system did not yield useful insight towards identifying areas for availability improvement. The effort to assign meaningful RPN values did not provide a useful metric for differentiation and prioritizing areas of potential failures. Measures and estimates of severity, occurrence and detection levels for elements of the control system did not contribute towards a better understanding of areas for improvement.

However, part of the value of the FMEA is in the process itself. Although a full, formal FMEA process was not completed, there is potential utility in a formal review of a control system to better understand points of failure and areas of improvement. A systematic review of system dependencies and possible points of failure may yield useful insight. A Design FMEA at the planning stages of a large distributed control system may also be of use. And others have found benefit from using a FMEA for software quality control (see, for example, [6]).

The Process FMEA for the cryogenics group did yield useful insight towards areas of improvement of system availability. The first iteration of improvements based on the FMEA has already been implemented with a marked improvement in RPN values afterward. The experience from this FMEA does indicate that the process can be use-

ful in evaluating accelerator systems. A FMEA overview of an accelerator as a whole may be an effective means for prioritizing upgrades and resources across the facility.

Acknowledgment

Thank you to Bill Martin of National Quality Services and to Fabio Casagrande, Matt Howell and the other members of the SNS cryogenics group who participated in a formal Process FMEA for the cryogenics system and contributed towards a preliminary and informal Design FMEA of the SNS control system.

REFERENCES

[1] R. E. McDermott, R. J. Mikulak, M. R. Beauregard, *The Basics of FMEA*, Resource Engineering, Portland, OR (1996).

[2] W. R. Martin, "Failure Mode Effects Analysis," National Quality Services (2008).

[3] K. S. White, K. U. Kasemir, "Alarms Philosophy," these proceedings.

[4] B. R. Hollifield, E. Habibi, *Alarm Management: Seven Effective Methods for Optimum Performance*, ISA, Research Triangle Park, NC (2007).

[5] S. M. Hartman, "Control System Availability for the Spallation Neutron Source," these proceedings.

[6] D. E. Stamatis, *Failure Mode Effect Analysis: FMEA from Theory to Execution*, 2^{nd} Edition. American Society for Quality, Quality Press, Milwaukee, WI (2003).