No Equipment Failed/No Malicious Intent (NEF/NMI) Cyber-System Failures

Alyssa Lopez, Sam Faulconer, Hissah Almarzook, and Edwin Padilla-Gonzalez
Cyber Security Engineering Department, George Mason Univeristy

Systems Engineering and Operations Research

GEORGE MASON UNIVERSITY

Introduction

No Equipment Failed/No Malicious Intent (NEF/NMI) cyber-system failures are failures caused by unforeseen complications that arise from changes made to complex systems. NEF/NMI failures occur with no equipment failure nor a malicious actor. Organizations that need to apply updates or make configuration changes to their system(s) will inevitably experience a NEF/NMI cyber-system failure if the proper precautions are not taken to prevent them. The results of these failures can range anywhere from inconvenient to catastrophic.

This research was conducted based on a case study of a NEF/NMI failure at the Hatch Nuclear Power Plant (NPP). In this example, a nuclear engineer connected his work computer to a reactor control system for remote monitoring and administration. This configuration change allowed the remote monitoring and administration software to push an unauthorized software update to the reactor control system. This update caused the reactor control system to reboot and clear its historical data of reactor coolant levels. Once other safety systems observed the very sudden drop in coolant levels, a full shutdown of one of the plant's two reactors was initiated.

Concept of Operations

In order to test and prevent NEF/NMI complex system failures a Systems Integration Engineer (SIE) will require the probability that a failure will occur, as well as the impact this failure would incur. The SIE will be responsible for the ensuring components/ software are introduced to the overall system safely. In order to determine the probability of system failure in a NPP, the SIE will query the Common Critical Failure (CCF) database for failures involving the system that is to be modified. The CCF database collects failure data in commercial NPPs so a SIE can search for failures involving the system/component being modified. The SIE will take the results of this query, as well as their expert knowledge of the system to determine a probability the modification will cause a failure. The SIE will then determine the systems criticality based on its classification as one of the following.

- High: digital assets associated with plant safety and trip functions/communication.
- Medium: digital assets that do not functional primarily as safety systems, but may affect plant safety in their operation.
- Low: independent assets that do not affect plant safety or trip functions/ communication.

The probability and criticality of the system/component being modified are illustrated in the risk matrix in Figure 1 and are used as input values for the Decision Support System.

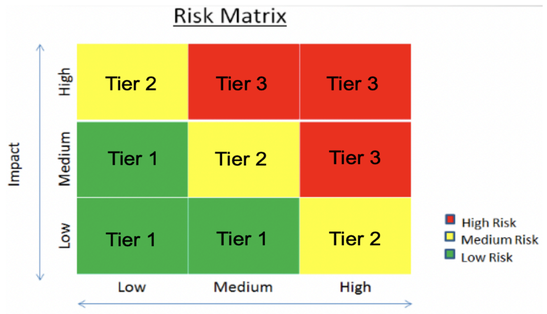

Figure 1

Design

The DSS was built as an Activity Diagram using Innoslate. The Activity Diagram format shows the overall flow of control of the DSS. The Activity Diagram format was able to clearly depict the different decisions, shown as diamonds in Figure 2, that a user needed to make regarding the likelihood and impact of a proposed modification to a BWR system. The Activity Diagram also clearly shows the actions taken by the user, shown as rounded rectangles in Figure 2.

The DSS is based on three different options for each the likelihood of failure and the impact of failure: low, moderate, and high. Since the decisions in the Activity Format are binary, the design of the DSS had to be slightly modified. For example, the first decision node prompts the user to decide if the proposed modification to the system has a low likelihood of failure. The user is able to select "low likelihood of failure" or "not low likelihood of failure." The "not low likelihood of failure" option would lead the user to be prompted to decide if the proposed modification to the system has a moderate likelihood of failure. Here, [W4] the user is able to select either "moderate likelihood of failure" or "high likelihood of failure." The impacts of potential failures were addressed in the same way to fit the binary representation of decisions in the DSS.

The output of the DSS will be the required testing that a system modification must go through before it may be safely implemented. The probability of failure and the system in question criticality directly influence the standard of testing that must be implemented. At the highest level, Tier 3, statistical testing must first be done to provide sample data to a subsequent white box test. This will use the provided sample data to execute each branch of the software in the system/component being modified. Next, Tier 2 testing can be done. This includes using sample data, either from previously conducted statistical test or system/component specification, to conduct a black box test. Finally, Tier 1 specifies that the system/component pass a functional test to ensure that the system/component operates as intended without failing.

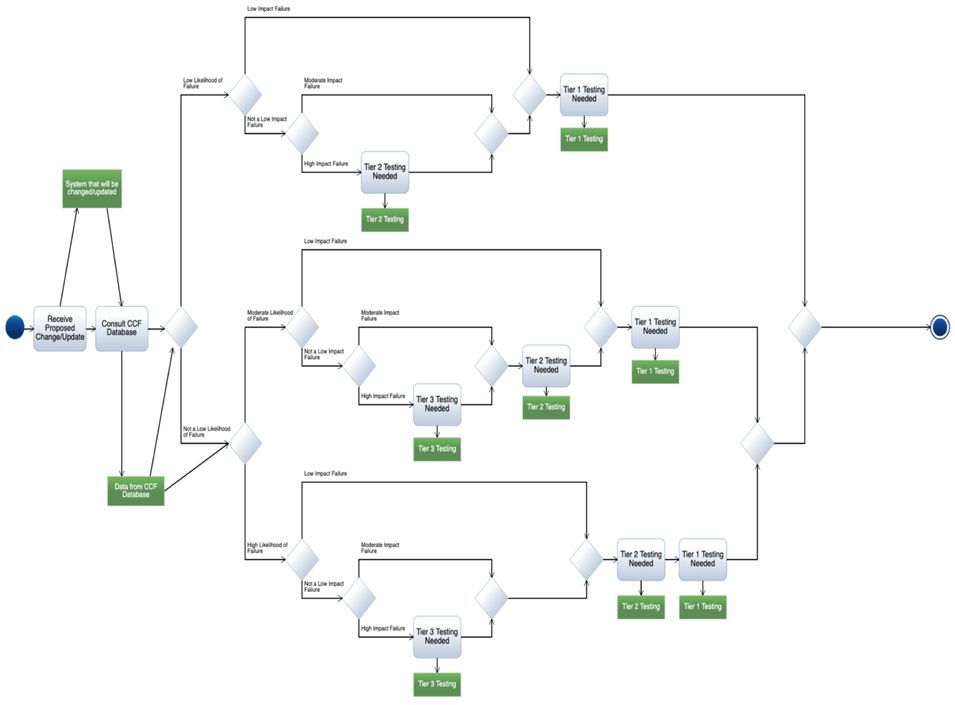

Figure 2

Verification

The tiers of testing that the DSS outputs are based on the levels of risk associated with proposed modifications to the BWR system. Because the information contained in the CCF database is proprietary information, the DSS was unable to be tested with actual probabilistic inputs. However, if the correct inputs are used in the DSS for the likelihood and impact of failure based on the CCF database query, the DSS will output the correct testing tier that is needed for the proposed modification.

While the DSS was unable to be tested, the concept of testing proposed modifications based on the level of risk that they pose a risk on the BWR system could help lower the likelihood of NEF/NMI failures in BWR systems. Performing the testing that the DSS outputs will allow engineers to understand how BWR system components react to the proposed modification. By understanding how BWR system components react to proposed modifications prior to their implementation in the operational environment, the engineers at the plant will have a better understanding of how the proposed modification will affect the BWR system. The results of testing the proposed modification to the BWR system will determine whether the Systems Integration Engineer will implement the proposed modification in the operational environment

Conclusion

NEF/NMI cyber-system failures can occur if the proper precautions are not taken when implementing modifications to a system. The Edwin I. Hatch nuclear power plant experienced a NEF/NMI failure due to a configuration change that did not go through prior testing to indicate that the configuration change was safe to implement. The solution provided above is robust enough to prevent this failure and similar BWR NEF/ NMI failures. If the engineer at the Edwin I. Hatch NPP had tested the configuration change prior to implementing it in the operational environment, the engineer would have been able to see how the BWR system would have interacted with the configuration change.

The DSS was designed to aid organizations in making risk-based decisions regarding proposed modifications to a BWR system. This is done by utilizing data-based probabilities and standardized risk categories to determine different tiers of integration testing. The DSS accepts a proposed modification to the system and data from the CCF database as an input. The outputs are the tiers of testing that should be conducted based on established industry standards. The results of the testing can aid plant engineers in determining if it is safe to proceed with the given modification.

The DSS that was created is specialized to be used in a BWR NPP, but further research can be done to apply the concept behind the DSS to other complex systems to help prevent NEF/NMI failures in other systems.

References

1. [1] B. I. Spinard and W. Marcum, "Nuclear reactor," *Encyclopædia Britannica, inc.*, Sept. 2019. Accessed on: Mar. 26, 2020. [Online]. Available: https://www.britannica.com/technology/nuclear-reactor
2. [2] M. Brain, R. Lamb, and P. J. Kiger, "How nuclear power works," *HowStuffWorks.*, Oct. 2000. Accessed on: Jan. 2020. [Online]. Available: https://science.howstuffworks.com/nuclear-power.htm
3. [3] "License Amendment Request Guidelines," *Nuclear Energy Institute.*, Oct. 2010. Accessed on: Feb. 2020. [Online]. Available: https://www.nrc.gov/docs/ML1033/ML103360404.pdf
4. [4] "Cyber security programs for nuclear facilities," *U.S. Nuclear Regulatory Commission.*, Jan. 2010. Accessed on: Jan. 2020. [Online]. Available: https://scp.nrc.gov/slo/regguide571.pdf
5. [5] M. Caruso, M.C. Cheok, M. Cunningham, G.M. Holahan, T. King, G. Parry, A.M. Ramey-Smith, M. Rubin, and A. Thadani, "An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis," *Reliability Engineering & System Safety.*, vol. 63, no. 3, pp 231-242, Mar. 1999. Accessed on: Jan. 2020. [Online]. Available: doi: 10.1016/S0951-8320(98)00038-6
6. [6] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," *The Washington Post Company.*, Jun. 2008. Accessed on: Nov. 2019. [Online]. Available: https://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html
7. [7] "Federal, state, and local, and tribal, responsibilities," *U.S. Nuclear Regulatory Commission.*, Jun. 2018. Accessed on: Jan. 2020. [Online]. Available: https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/federal-state-local.html
8. [8] T.E. Wierman, D.M. Rasmuson, A. Mosleh, "Common-cause failure database and analysis system: event data collection, classification, and coding," *U.S. Nuclear Regulatory Commission.*, Sept. 2007. Accessed on: Feb. 2020. [Online]. Available: https://www.nrc.gov/docs/ML0729/ML072970404.pdf
9. [9] J.W. Lee, C.K. Lee, J.G. Song, K.C. Kwon, and D.Y. Lee, "A cyber security risk assessment for the design of I&C systems in nuclear power plants," *Korea Atomic Energy Research Institute.*, vol. 44, no. 8, pp. 919-928, Dec. 2012. Accessed on: Jan. 2020. [Online]. Available: doi: 10.5516/NET.04.2011.065
10. [10] G.S. Bedi, "Guidelines for inservice testing at nuclear power plants," *U.S. Nuclear Regulatory Commission.*, Oct. 2013. Accessed on: Jan. 2020. [Online]. Available: https://www.nrc.gov/docs/ML1329/ML13295A020.pdf
11. [11] V. Grover, W.J. Kettinger, *Process Think: Winning Perspectives for Business Change in the Information Age.* " Hershey, PA: IGI Global, 2000.
12. [12] "Systems Integration," *The MITRE Corporation.*, Mar. 2016. Accessed on : Apr. 2020. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/systems-integration
13. [13] *IEEE Standard for Software and System Test Documentation*, IEEE Standard 829, 2008.
14. [14] "BWR14 technology manual (R-104B)," *USNRC Technical Training Center.*, Accessed on: Mar. 2020. [Online]. Available: https://www.nrc.gov/docs/ML0228/ML022830867.pdf
15. [15] "Risk-informed categorization and treatment of structures, systems, and components for nuclear power reactors," *U.S. Nuclear Regulatory Commission.*, Aug. 2017. Accessed on: Mar. 2020. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0069.html