Fault Tree Analysis for an Inspection Robot in a Nuclear Power Plant

Thomas A. Ferguson¹ and Lixuan Lu¹
¹Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology, 2000 Simcoe Street North, Oshawa, Ontario, Canada L1H 7K4
E-mail: thomas.ferguson1@uoit.net; Lixuan.Lu@uoit.ca

Abstract. The life extension of current nuclear reactors has led to an increasing demand on inspection and maintenance of critical reactor components that are too expensive to replace. To reduce the exposure dosage to workers, robotics have become an attractive alternative as a preventative safety tool in nuclear power plants. It is crucial to understand the reliability of these robots in order to increase the veracity and confidence of their results. This study presents the Fault Tree (FT) analysis to a coolant outlet piper snake-arm inspection robot in a nuclear power plant. Fault trees were constructed for a qualitative analysis to determine the reliability of the robot. Insight on the applicability of fault tree methods for inspection robotics in the nuclear industry is gained through this investigation.

1. Introduction

Most existing Nuclear Power Plants (NPPs) around the world are facing the challenges of aging equipment. As of 2013, 190 out of the 437 civil nuclear reactors have been in operation for more than 30 years [1]. However, the need of these power plants has increased over the past decade due to concerns over greenhouse gas emissions and the increasing demand for electricity. Therefore, the extension of the life expectancy of the aged/aging reactors has becoming more and more imperative [2].

In order to maintain safe and profitable operation of these life-extended reactors, important components have to be replaced. In cases where replacement is too costly or not feasible, the continual inspection and maintenance becomes paramount [3]. However, to limit the dosage exposure for workers, inspection can become difficult and costly. An attractive alternative for human inspection of critical components is the use of remotely operated robotics [3, 4].

Since the inception of the robotic industry, the major benefits of using robots in hazardous environments have become increasingly evident. This is particularly true in the nuclear industry, where robots have been used routinely [4, 5]. The versatility of the robotic technology has been fully exploited over the years. Common roles performed by robots include handling high level radioactive loads [6], decommissioning [4], testing and maintenance [3, 4], and assisting after nuclear disasters [6]. Although nuclear robotics are a well used technology, there is still continual development as more challengers are presented as the industry ages. One of the most prominent challenges is the increasing demand of inspection. Inspection robotics play an important role in monitoring and detecting defects in critical components so as to determine early warning of component failure and prevent possible nuclear accidents. It is essential to understand the reliability of the robots performing these required inspection tasks, so as to gain confidence in the inspection results. Furthermore, the need for clear
understanding of the paths to failure is compounded by the fact that these inspection robots work in an ionizing radiation field and have limited amount of exposure before failure. A significant cause of malfunction of tele-operated robots in the nuclear industry is a result from radiation damage [5, 7]. This paper presents a reliability assessment of such robotics using the Fault Tree (FT) analysis technique, with emphasis on a case study of a snake-arm robot for inspection of primary heat transport pipes of a nuclear reactor.

2. Snake-Arm Pipe Inspection Robot

The pressurized coolant outflow pipes from the nuclear reactor are components that are not feasible for replacement, and with age must be monitored. These pipes become prone to thinning due to flow-assisted corrosion, after years of operation. Furthermore, due to the long length of the pipes structural support is required. The constant motion between the feeder pipes and the support structure caused outside pipe fretting, which further caused the thinning of the pipes. This could cause a compromised pressure boundary, which could result in the release of high pressure radioactive steam.

The potential of fretting requires frequent and continual external inspection to be conducted. The examination has historically been performed manually by visual inspection, where the operator uses a camera to capture data for further inspection. This procedure can only be performed during outages, and therefore, due to geometric and time restraints, some areas cannot be viewed and points of concern are difficult to revisit. To alleviate these problems a snake-arm robot with high resolution cameras attached was developed.

The inspection robot is a remotely operated machine with a 2.2 m long, 12.5 mm width, and 18 DoF snake arm attached to a remotely controlled vehicle base. At the tip of the arm is the main inspection tool equipped with two forward pointing and one sideways facing fixed focal length cameras. The cameras have high powered LED lights matched to each respective camera’s focal point. The video captured by the cameras are sent to a workstation outside of the hazardous area, by an umbilical cable. The arm is divided into multiple sections, with multiple control cables attached at the end of each section. The arm is manipulated by actuators at the base of the arm, so no wires or electronics are in the arm itself. Tip-guiding software is used to operate the arm.

The implementation of the robot provides multiple benefits, which include reduced operator exposure, constant availability since inspection is not limited to outages, and examination of difficult-to-reach places. The robot itself is not a high risk device to damage any equipment because of its size and structure. However, if the robot was to fail in locating any defects, a significant nuclear incidence could occur [3], due to the consequence of inspection robotic not being able to complete its task. Therefore, the reliability of the robot must be assessed. Furthermore, the dominant cause for failure of components is from radiation damage. Although the radiation tolerance for components is well known [7, 8], the propagation of these failures should also be assessed for a strong understanding of the robotic system reliability.

3. Fault Tree analysis

Fault Tree Analysis (FTA) is a top-down deductive failure analysis, which illustrates the sequence of failures that could result in a system failure (top event). The methodology uses a graphical illustration of the failure events. A failure path is determine by combining failure events using the standard logic gates (AND, OR, etc.) in a tree like fashion [9]. Fault Tree analysis is a well defined and commonly used tool in many different industries. Common fields of use include aerospace, nuclear power generation, and other events that have a significant safety risk to human health. FTA has also become a common method for assessing the reliability and safety of robotic systems [10-15], including those used within the nuclear industry [5, 16]. For a more general review of reliability assessments for robotics please refer to references 13 and 14.

Since the snake-arm robot itself is not a high risk device, the top events for the construction of fault trees for analysis are determined by the events that would not allow the robot to inspect the feeder pipes and identifying defects leading to a compromised pressure boundary. The top events were
evaluated to be arm deployment apparatus failure, arm control systems failure, and the inability to control the locomotion of the device. The top event with lowest risk tolerance was determined to be the arm control systems failure, and will be the focus of this study.

A number of assumptions were made to produce the fault trees. The design and function of the device are described in [3, 17, 18]. The references state that the device arm is controlled by multiple cables connecting to each segment of the arm. The actuators are described as electronic motors. Furthermore, each segment of the arm can be adjusted independently from other segments, so the failure of actuators of one segment does not lead to loss of control of the whole arm. As a result, it is assumed that the inability for inspection occurs with failure of all section actuators. Any adjustments to the above assumption could lead to variation in the fault trees.

4. Results and Discussion

As mentioned above the top event with the lowest fault tolerance was found to be the arm control system failure. The main reason for this is because for failure of the arm deployment apparatus to occur all sections of the arm are required to fail. Each segment of the arm is controlled in parallel, so if one arm segment were to fail the other arm segments can still mechanically be controlled.

Although the actuators for each segment of the arm are independent of each other, the control calculations do not share the same independence. The device uses a tip-guiding software to aid in the control of the arm by the operator. In order to determine the position of a segment the controller requires measurements both from the arm segment under control and measurements from the other segments. As a result, if there was a failure in the measurement in one section of the arm all other sections will be affected. Therefore, if a fault was to occur lower down on the tree it will propagate up to the top event, as demonstrated by the OR-gates present in the tree. The constructed fault tree is shown Figure 1 below.

![Fault tree of arm control system failure.](image)

As can be seen from Fig. 1, the fault paths resulting in arm control system failure can be clearly extracted from the fault tree. From the failure paths, the effect of radiation susceptible component malfunctions can be determined. Components and materials that are susceptible are well known in literature, examples include: electronics, sensors, fibre optics, insulating materials and lubricants [7, 8]. From this knowledge the initiating events that are caused by dosage limited component failure were determined.

After the construction of the tree, the number of minimum cut-sets was determined. There were a total of 12 minimum cut-sets of the first order, and of the 12 minimum cut sets, 7 of them are susceptible to radiation damage. The initiating events with the lowest limit of exposure are:
communication from sensors to controller failure, visual systems hardware failure, input hardware failure, and encoder circuitry failure. Since the system has a low fault tolerance, and any failure will propagate up the tree, dosage limits should be known and monitored. Radiation hardened components and materials should be used. However, they do not grant indefinite exposure and failure paths are still important to know.

Improvements can be made to reduce the fault propagation in the system. Suggested improvements to be made include the following: An increase in the number of sensors would reduce the risk of sensory failure. To take full advantage of the redundant sensors, a sensor fault detection and reconfiguration algorithm implemented in the arm controller would be necessary [19]. The purposes of the algorithm would be to detect a faulty sensor, exclude its respective signal in control calculation and include only the remaining functional sensors. In order to take advantage of the multi-redundant manipulator, the control software must be able to adjust the kinematics of the arm after a segment failure. A method to achieve such flexibility is by having multiple kinematic calculations for possible section failure present in the controller, and a reconfiguration algorithm to correct the controller to the appropriate calculation after failure [20].

The fault tree analysis presented in this study was an entirely qualitative study due to limitations of available data. However, the purpose of this study was to demonstrate fault tree analysis as a tool to understand the reliability of nuclear inspection robots and determine the areas of most concern in terms of radiation damage. The ability to identify these areas is very useful for both operation and design phase of the robotic systems life cycle. Operators are able to determine which components require the most detailed dosage monitoring, and formulate corresponding mitigation strategies. The understanding of low fault tolerance of radiation damage areas of concern determined from the FTA, can allow for identifying improvements required, and what components require radiation tolerant hardware while designing the robot.

5. Conclusion
The reliability of nuclear inspection robotics was investigated by fault tree analysis with emphasis on a case study of a pipe inspecting snake-arm robot in a nuclear reactor. The top event for the FTA with the lowest fault tolerance was found to be failure of the arm control system. A significant source of component malfunction of nuclear robotics is from radiation damage. The fault tree analysis allowed for determination of failure paths for malfunctions of radiation damage susceptible components, which allows identification of areas of concern for possible improvement and formulation of mitigation strategies. The insights gained through the fault tree analysis of the snake-arm pipe inspection robot in this paper are beneficial for both design and operating phases of the system's life cycle.

References
[1] Schneider, M., & Froggatt, A. (2013). World nuclear industry status report 2013
[2] León, P. T., Cuesta, L., Serra, E., & Yagüe, L. (2010). Life Extension of Nuclear Power Plants: World Situation and the USA Case. Revue générale nucléaire, 6, 50-56.
[3] Buckingham, R., & Graham, A. (2012). Nuclear snake-arm robots. Industrial Robot: An International Journal, 39(1), 6-11.
[4] Bogue, R. (2011). Robots in the nuclear industry: a review of technologies and applications. Industrial Robot: An International Journal, 38(2), 113-118
[5] Lauridsen, K., Christensen, P., & Kongso, H. E. (1996). Assessment of the reliability of robotic systems for use in radiation environments. Reliability Engineering & System Safety, 53(3), 265-276.
[6] Kawatsuma, S., Fukushima, M., & Okada, T. (2012). Emergency response by robots to Fukushima-Daiichi accident: summary and lessons learned. Industrial Robot: An International Journal, 39(5), 428-435.
[7] Sharp, R., & Decreton, M. (1996). Radiation tolerance of components and materials in nuclear robot applications. Reliability Engineering & System Safety, 53(3), 291-299.
[8] Houssay, L. P. (2000). Robotics and radiation hardening in the nuclear industry (Doctoral dissertation, University of Florida).
[9] Xing, L., & Amari, S. V. (2008). Fault tree analysis. In Handbook of Performability Engineering (pp. 595-620). Springer London.
[10] Karbasian, M., Mehr, M. R., & Agharajabi, M. (2012). Improvement of the Reliability of Automatic Manufacture Systems by Using FTA Technique. International Journal of Industrial Engineering, 23(2), 85-89.
[11] Winfield, A. F., & Nembrini, J. (2006). Safety in numbers: fault-tolerance in robot swarms. International Journal of Modelling, Identification and Control, 1(1), 30-37.
[12] Yakymets, N., Dhouib, S., Jaber, H., & Lanusse, A. (2013, November). Model-driven safety assessment of robotic systems. In Intelligent Robots and Systems (IROS), 2013 IEEE/RSJ International Conference on (pp. 1137-1142). IEEE.
[13] Khodabandehloo, K. (1996). Analyses of robot systems using fault and event trees: case studies. Reliability Engineering & System Safety, 53(3), 247-264.
[14] Visinsky, M. L., Cavallaro, J. R., & Walker, I. D. (1994). Robotic fault detection and fault tolerance: A survey. Reliability Engineering & System Safety, 46(2), 139-158.
[15] Dhillon, B. S., Fashandi, A. R. M., & Liu, K. L. (2002). Robot systems reliability and safety: A review. Journal of quality in maintenance engineering, 8(3), 170-212.
[16] Walker, I. D., & Cavallaro, J. R. (1996). Failure mode analysis for a hazardous waste clean-up manipulator. Reliability Engineering & System Safety, 53(3), 277-290.
[17] Graham, A. C., & Buckingham, R. O. (2014). U.S. Patent No. 8,635,928. Washington, DC: U.S. Patent and Trademark Office.
[18] Buckingham, R. O., & Graham, A. C. (2012). U.S. Patent No. 8,126,591. Washington, DC: U.S. Patent and Trademark Office.
[19] Visinsky, M. L., Cavallaro, J. R., & Walker, I. D. (1994). Robotic fault detection and fault tolerance: A survey. Reliability Engineering & System Safety, 46(2), 139-158.
[20] Lewis, C. L., & Maciejewski, A. A. (1994). Dexterity optimization of kinematically redundant manipulators in the presence of joint failures. Computers & electrical engineering, 20(3), 273-288.