CONF-960869--15 SAND96-2014C

Safety Assessment of High Consequence Robotics System

David G. Robinson, Ph.D. ; Sandia National Laboratories, N.M.

Christopher B. Atcitty; Sandia National Laboratories, N.M.

Abstract

This paper outlines the use of a Failure Modes and Effects Analysis for the safety assessment of a robotic system being developed at Sandia National Laboratories. The robotic system, the Weigh and Leak Check System, is to replace a manual process for weight and leakage of nuclear materials at the Department of Energy (DOE) Pantex facility. Failure Modes and Effects Analyses were completed for the robotics process to ensure that safety goals for the system have been met. Due to the flexible nature of the robot configuration, traditional failure modes and effects analysis (FMEA) were not applicable. In addition, the primary focus of safety assessments of robotic systems has been the protection of personnel in the immediate area. In this application, the safety analysis must account for the sensitivities of the payload as well as traditional issues. A unique variation on the classical FMEA was developed that permitted an organized and quite effective tool to be used to assure that safety was adequately considered during the development of the robotic system. The fundamental aspects of the approach are outlined in the paper.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Background

The Weigh and Leak Check System (WALS) robot will be replacing human workers who presently check the nuclear material used in weapons for damage, leaks and weight. The system is composed of a track-mounted Fanuc Model S-700 robot and several different workstations. Because the nuclear material is normally mounted in a fixture, one workstation has been designed to automatically assemble and disassemble this fixture. Three other stations are used to perform the inspection procedures. The two main inspection tasks are done by a weigh station and a leak check station. A third inspection station is used to perform manual checks on the material via a gloveport.

The WALS inspection process (Drotning, et al., 1996) begins with the workers bringing a container with the nuclear material into the robot workcell. After the workers leave the work bay, the robot locates the material with machine vision and removes it from the container. Upon removal, the robot shuttles the material to the various workstations in order to perform the inspection procedures. After these tasks are completed, the material is returned to a storage container. By using a robot, the workers will no longer be exposed to radiation during these necessary inspection processes.

While this system's installation will benefit the workers by lowering their radiation exposure, the question of safety remains: Does the robotic system introduce more risk than it eliminates? The potential for additional risk would mostly be due to the fact that the robot is not handling a paint gun or a spot welder but a substantial amount of nuclear material. Not only do workers have to be protected from this robot under normal industrial conditions, but they must also be guarded against any potential mishandling of these dangerous payloads.

In addition to the safety of the workers, every nuclear facility in the United States must be proven to have minimal risks to the people and environment beyond the boundaries of the facility. DOE Order 5480.23 (USDOE, 1992) outlines the requirements for developing safety analyses which evaluate nuclear facilities. Because the WALS robot will be installed in such a nuclear facility, the system must be considered in the facility's Safety Analysis Report.

While safety analyses subject to DOE Order 5480.23 are usually required to be quantitative in nature, exceptions can be made for non-reactor facilities when the hazards are shown to be sufficiently low (Atcitty and Robinson, 1996; McCulloch, 1996). In those cases, the safety analysis needs only to be qualitative. This "graded approach" is intended to keep the level of analysis commensurate with the magnitude of the facility's hazards. Therefore, a safety analysis can initially be qualitative until the need for risk quantification becomes evident (USDOE, 1994).

Methodology

A number of organizations have addressed the issue of robot safety in the United States including the National Safety Council, the American National Standards Institute and the U.S. Department of Labor. The generally accepted approach used in a safety analysis of industrial robotics systems is outlined by the Robotics Industries Association in the standard ANSI/RIA R15.06-1992 (ANSI, 1992). The objective of this standard is to assure that sufficient safeguards are in place to provide for the safety of personnel in the workplace.

While the identification of hazards and anticipated failure modes is a required element under most robotic safety standards, detailed investigation is necessary only for those failures which could potentially result in risks to personnel directly involved with the installation, training, operation, and maintenance of the robot. The standards provide only incidental attention to safeguarding sensitive material and equipment within the robot's maximum operating envelope and do not address damage that the robotic system may cause outside that envelope. Obviously, existing robotic safety analysis methods alone did not provide a methodological basis for the evaluation of the WALS robot.

The primary challenge of this safety assessment is a result of the dynamic nature of flexible robotics systems. Most safety analysis methods have their origins in the study of comparatively static systems such as nuclear reactors or weapon systems; typically, a method like fault tree analysis will use the state of a system at a particular time in order to find developing problems. These methods are not directly suited for the assessment of the complex operations of a system like WALS. In fact, the direct use of a traditional safety analysis method can quickly make the problem larger than project resources allow.

A different approach must be taken for a robotics system to account for the large number of different states which exist for a robot throughout its operation. These differences can manifest themselves not only in the hardware but in the software as well. A robotic system makes use of a common set of features to perform its job; however, a designer can ingeniously use this feature set to perform an extremely varied set of operations. While this adaptability makes a programmable robotic system desirable, it also makes the safety analyst's job that much tougher. In order to overcome this hurdle, the proposed analysis method calls for the entire robotic process to be broken down into logical and more manageable steps. Each step can in turn be analyzed independently by conducting a failure modes and effects analysis (FMEA).

A FMEA for each process step is needed to accurately reflect the differences that exist between the robotics process steps. While the robot itself remains unchanged, other elements of the design can be quite different. For example, each of the grippers incorporates unique features which need to be analyzed. The robot's location in the workcell is also important because even the small changes in the tables, station platforms and other station-specific hardware require individual attention. Also, while software may be built on shared code, each robotic process is comprised of an individually tailored program which can respond differently depending on the current task and location. These subtleties can be missed if the scope of a FMEA is too large.

The results of doing FMEAs in this manner were anticipated to be that the safety analysis would become more tractable in preparation, affect the final design to a greater extent and make the review process proceed more smoothly. These benefits can be realized because the failure modes and effects analysis provides reasonable assurance that all potential hazards will be adequately considered while, at the same time, concentrating on smaller steps in the operations. Therefore, this method provides both depth and breadth to the safety assessment. While this analysis method cannot absolutely ensure that all failure modes and effects have been identified, it does provide a structure for a comprehensive consideration of hazards. Additionally, the FMEA can be extended to a more rigorous quantitative risk assessment, for example, by using fault trees or event trees. This would only be accomplished if the preliminary hazards analysis indicated it was necessary.

It is important to note that this approach is intended to be an iterative one. First, the FMEA ensures that the failure modes being described are basic in nature by requiring that information be available to at least qualitatively assess the likelihood of the failure occurring. If the failures cannot be described adequately, then further detail is required in the system description of the robotic process. Thus, the failure characteristics of the system drive the level of detail required in the system description. Second, when the FMEA does find an unacceptable hazard level, the design engineers are naturally expected to address the problem and the safety analysis repeated for the new design. Safety information incorporated early on will ensure that safety can be properly designed into the system. The FMEA is repeated until both the system description and hazard levels are acceptable.

Results

In order to implement this "divide and conquer" method, the entire WALS robotics process from retrieving nuclear material from a container through weighing and leak checking had to be thoroughly defined. A flow chart showing the WALS process was developed to communicate the division of the operations into a coherent series of process steps.

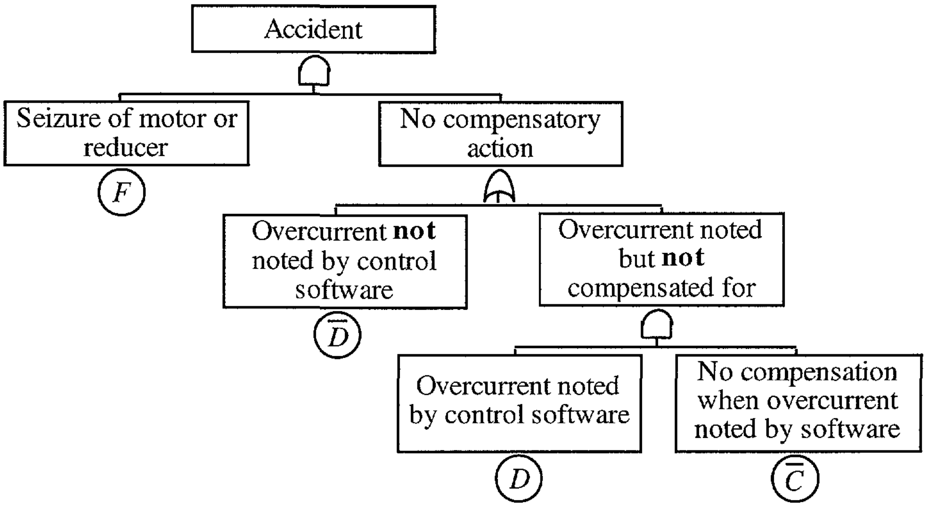
Table 1 - Example from the Failure Modes and Effects Analysis

Joint Failure	Seizure of motor or reducer	Overcurrent noted by control software	Overcurrent noted by control software results in system shutdown initiated by control software and operator notification at console	System shutdown by control software
	$P(F) = \text{H}$	$1 - P(D) = \text{M}$	$1 - P(C) = \text{L}$	

Military Standard 1629A (USDOD, 1980) provided an initial foundation for the definitions and general procedures used in a FMEA and an example from the failure modes and effects analysis is shown in Table 1. From the FMEAs that were developed, hazard levels could be determined for the failure modes of each process step. The two elements which make up a hazard level determination are an accident's probability of occurrence and severity of consequences. An accident would result from an unmitigated failure.

In order to find the probability of occurrence for an accident, the sequence of events which lead up to the accident will have to be examined. A convenient way to look at this sequence is through a simple fault tree. The fault tree in Figure 1 depicts a typical sequence of events leading to an accident.

Figure 1 - Sample Fault Tree


Accident
Seizure of motor or reducer
F
No compensatory action
Overcurrent **not** noted by control software
$\overline{D}$
Overcurrent noted but **not** compensated for
Overcurrent noted by control software
D
No compensation when overcurrent noted by software
$\overline{C}$

Using Boolean algebra to solve the fault tree and assuming independence between the events "F," "D," and "C," one will find that the equation for the probability of the accident event occurring is:

$$P(Accident) = P(F)(1 - P(D)) + P(F)P(D)(1 - P(C)) \tag{1}$$

In order to determine the likelihood of occurrence for potential accidents, three probabilities need to be found for each failure mechanism shown in the FMEA. These probabilities are the probability, P(F), of the failure mechanism occurring, the probability, P(D), of that failure being detected and the probability, P(C), of the system compensating for the detected failure. Instead of exact probabilities, a range of probabilities can be used with equation (1) to render the probability calculation qualitative.

Table 2. Values for a qualitative hazard assessment

Frequency Ranking	***Annual Probability (p)***
VL (very low probability)	0.000001 > p
L (low probability)	0.0001 > p >0.000001
M (medium probability)	0.01 > p > 0.0001
H (high probability)	0.1 > p > 0.01
VH (very high probability)	1.0 ^{3} p > 0.1

To better understand the steps in the qualitative analysis, the fault tree in Figure 1 is analyzed using Equation (1). Please note that the values used are for illustration purposes only. Equation (2) shows three qualitative rankings of likelihood information;

for each of the probabilities, a range of values can be obtained and a best and worst case analysis performed:

$$\begin{array}{rllll} \boldsymbol{P(F)} = \mathbf{H}: & 0.1 & \geq & P(F) & > 0.01 \\ \mathbf{1 -} \boldsymbol{P(D)} = \mathbf{M}: & 0.01 & \geq & 1 - P(D) & > 0.0001 \\ \mathbf{1 -} \boldsymbol{P(C)} = \mathbf{L}: & 0.0001 & \geq & 1 - P(C) & > 0.000001 \end{array} \tag{2}$$

Using these values, upper and lower bounds on the probability of an unmitigated failure can be estimated:

$$\begin{array}{l} P(Accident) \leq (0.1)(0.01) + (0.1)(0.99)(0.0001) = 0.00101 \\ P(Accident) > (0.01)(0.0001) + (0.01)(0.9999)(0.000001) = 0.00000101 \end{array} \tag{3}$$

With these bounds, Table is once again used to qualitatively categorize the hazard associated with this operation. The final classification of this operation would be in the low to medium range. An evaluation similar to this is performed for each operation in the robot operational cycle. Events falling in the medium to high range would be flagged for further analysis. Ultimately, likelihood classifications are used with the severity of consequences for unmitigated failures to determine the level of risk for each failure mechanism.

The other measure used in a hazard level determination, the severity of an accident's consequences, is for most purposes a qualitative measure defined by applicable standards or by the safety assessment team itself. For the WALS analysis, the level of severity was related to the impact of potential radiation exposures to people and the environment. Once the probabilities and consequences of potential accidents are found, hazard levels are established for each failure mechanism in the FMEAs. All hazard levels are subsequently used to assess the entire robotics system as it performs the WALS inspection tasks.

For the WALS safety analysis, FMEAs were developed for each robotic process step and included the important qualitative hazard levels. The analysis focused attention on several issues important to the development of the system. Two of the most significant are: 1) The available failure rate data is derived primarily from service call information supplied by the robot manufacturer and not on an organized test program to evaluate the system (including safety measures) in response to off-normal situations which include potential robot movements that are not part of designed operations. 2) The WALS system places a strong dependence on software systems to prevent accidents and/or mitigate their consequences.

Conclusions

The most important contribution of the approach taken was that the problem broken down into parts became much easier to tackle. In fact, the nature of the robot allowed the analysis of much of the hardware to be performed only once and then replicated for other processes. The FMEAs of processes with roughly similar configurations could then easily share failure modes with each other. The analysis could then be focused around the many other differences in the WALS process steps: robot location, robot configuration, tooling, and payload.

Upon completion of a FMEA for a process step, an estimate of the potential risks is made. The system designers could then judge whether the level of risk was acceptable or if the system needed to be modified to reduce the risk. The safety analysis iterated around the process steps until an acceptable level of safety is achieved for the overall system and its operation. This procedure ensured that safety was explicitly integrated into the system design process.

Since the robotics portion of WALS was still being prototyped at the start of the analysis, concentrating the safety analysis on each process step allowed for minimal changes to the safety analysis as the system design evolved. For example, if the gripper design changed for one tool, then the effect of the change would be felt only by those process steps which used that particular tool.

Lastly, an emphasis needs to be placed on having appropriate failure data in order for the safety analysis to establish meaningful estimates of hazard levels. The failure information obtained from the robot manufacturer was based primarily on service calls made on similar operating systems and not on a test program designed to evaluate the failure modes and safety features of the WALS design. So while this data was used in estimating risks, it substantially increased the uncertainty in the results. The data base might be improved by considering whatever information that can be obtained from the failures which occurred during the design and development process. Obviously, the results of the safety analysis cannot be any more meaningful than the input data.

Acknowledgment

This work was performed at Sandia National Laboratories and supported by the United States Department of Energy under contract DE-AC04-94AL85000.

References

1. ANSI/RIA Standard R15.06-1992, "American National Standard for Industrial Robots and Robot Systems - Safety Requirements," August 19, 1992

2. C. Atcitty, D. Robinson, "Safety Assessment of a Robotic System Handling Nuclear Material," The 2nd Conference and Exposition/Demonstration on Robotics for Challenging Environments, American Society of Civil Engineers, Albuquerque, New Mexico, June 1-6, 1996.

3. W. Drotning, J. Fahrenholtz, H. Kimberly, J. Kuhlmann, and W. Wapman, "System Design for Safe Robotic Handling of Nuclear Materials," The 2nd Conference and Exposition/Demonstration on Robotics for Challenging Environments, American Society of Civil Engineers, Albuquerque, New Mexico, June 1-6, 1996.

4. W. H. McCulloch, "Safety Analysis Requirements for Robotic Systems in DOE Nuclear Facilities," The 2nd Conference and Exposition/Demonstration on Robotics

for Challenging Environments, American Society of Civil Engineers, Albuquerque, New Mexico, June 1-6, 1996.

5. U.S. Department of Defense, Military Standard 1629A, "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," November 24, 1980.
6. U.S. Department of Energy, DOE Order 5480.23, "Nuclear Safety Analysis Reports," April 10, 1992.
7. U.S. Department of Energy, DOE Standard 3009-94, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," July 1994.

Biographies

David G. Robinson, Ph.D.
PO Box 5800, MS 0746
Sandia National Laboratories
Albuquerque, N.M. 87185-0746
drobin@sandia.gov

David Robinson is currently a Senior Member of theTechnical Staff at Sandia National Laboratories. His Ph.D. is in Systems Engineering from the University of Arizona. His current responsibilities include the development of new methods to characterize and control the uncertainty inherent in complex systems.

Christopher Atcitty
PO Box 5800, MS 0746
Sandia National Laboratories
Albuquerque, N.M. 87185-0746
cbatcit@sandia.gov

Christoper Atcitty is currently a Member of the Technical Staff at Sandia National Laboratories. Chris received his Bachelor of Science and Master of Science degrees in Mechanical Engineering from Stanford University in 1994. He is currently involved with a number of projects including risk assessment of surgical systems and safety analysis of systems for handling and storage of nuclear material.