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.

SYSTEM DESIGN FOR SAFE ROBOTIC HANDLING OF NUCLEAR MATERIALS

William Drotning, Walter Wapman, Jill Fahrenholtz, Howard Kimberly, and Joel Kuhlmann[1]

Abstract

Robotic systems are being developed by the Intelligent Systems and Robotics Center at Sandia National Laboratories to perform automated handling tasks with radioactive nuclear materials. These systems will reduce the occupational radiation exposure to workers by automating operations which are currently performed manually. Because the robotic systems will handle material that is both hazardous and valuable, the safety of the operations is of utmost importance; assurance must be given that personnel will not be harmed and that the materials and environment will be protected. These safety requirements are met by designing safety features into the system using a layered approach. Several levels of mechanical, electrical, and software safety prevent unsafe conditions from generating a hazard, and bring the system to a safe state should an unexpected situation arise. The system safety features include the use of industrial robot standards, commercial robot systems, commercial and custom tooling, mechanical safety interlocks, advanced sensor systems, control and configuration checks, and redundant control schemes. The effectiveness of the safety features in satisfying the safety requirements is verified using a Failure Modes and Effects Analysis. This technique can point out areas of weakness in the safety design as well as areas where unnecessary redundancy may reduce the system reliability.

Introduction

The Intelligent Systems and Robotics Center at Sandia National Laboratories develops prototype robotic systems to automate handling of radioactive weapon parts and other hazardous materials. These systems reduce the occupational radiation exposure to workers by replacing operations that are currently performed manually. An important aspect of these systems is the multitiered approach of incorporating independent, and sometimes overlapping, mechanical, electrical, and software safety schemes. In this paper, we describe the safety approaches used in the design and development of a robotic system for packing, unpacking, and handling of nuclear weapon materials. The primary robotic safety issues are related to the need to handle the materials safely by preventing uncontrolled robot motions or dropping of

[1] Intelligent Systems and Robotics Center, Sandia National Laboratories, Albuquerque, NM 87185

payloads during handling. Safety is implemented through system design, mechanical design, and integration of safe practices into control software. Sensors are integrated into the system to provide added information to the control system about the state of the workplace environment. The fundamental approach is to provide additional information to the software control system in order to make intelligent decisions for safely handling these hazardous materials, but ultimately, to provide mechanical and electrical means to ensure safe operation without reliance on software. (The safety systems described here are in addition to those typically employed in robotic systems for personnel safety, as described in Ref. 1.) These safety practices can be conveniently discussed under the topics of robot, tool, station, procedure, and software safety. In addition, a Failure Modes and Effects Analysis (FMEA) has been conducted to evaluate the effectiveness of the safety features in satisfying the safety requirements. This technique can point out areas of weakness in the safety design as well as areas where unnecessary redundancy may reduce the system reliability.

Robot Safety

The robots used in our systems, like most current commercial robots, contain many built-in safety systems that operate regardless of the tools with which the robot is working. Safety features for motor overcurrent protection, detection of following error, and destination error detection are built into the robot controller by the manufacturer. Internal detection of these conditions typically causes the robot system to shut down by removing power to the robot linkage motors. When power is removed, the robot linkages are held in place by brakes on the joints. The robot's range of motion is limited in several ways. First, the robot motion (position, velocity, and acceleration) is continuously controlled by the user-defined program currently in operation. Next, limits are set in the robot controller software, independent from the user-defined application software, that restrict the range of motion of the robot, and the speed and acceleration of operations. Additionally, electrical switches are used to stop the robot motion if software limits are exceeded. Finally, mechanical hard-stops are used to physically limit the range of motion.

Commercially available hardware devices are attached to the robot's end-of-arm to both enhance safety and ease automated operations. A typical end-of-arm tooling configuration for our systems is shown in Figure 1. A force-torque sensor is attached directly to the robot arm, followed by a safety clutch and a tooling interface mechanism. Because its operation relies on a functioning computer and software, the force-torque sensor is not used as the primary means of safety, but rather as one facet of the overall safety approach.

In our robotic systems, the force-torque sensor connected to a computer is used in several ways to enhance safe operation of the system. First, the force-torque sensor is used to verify expected forces and moments when a payload is picked up but before the robot moves away from the pickup location. Second, the force-torque readings can be used to control the robot directly and modify its motion in real-time [2]. Two methods are used. In the *reaction* mode, software monitors the sensor readings to *stop* a controlled robot motion when a specific set of force-torque values is achieved. This mode is typically used to signal completion of a movement that places a tool or payload. In the *compliance* mode, software is used to *adjust* the robot motion in continuous response to the sensor readings. This mode is frequently used for precisely positioning a payload into a specific location by "feeling" the forces encountered during the placement. Finally, an additional, independent computer system is used to monitor the force-torque sensor and to trigger the robot's emergency stop (E-stop) circuit if force-torque limits become exceeded during robot motion in the workspace. Thus, if the robot control system failed, essential force-torque sensing can still stop the robot's motion through the primary E-stop circuitry.

Next to the force-torque sensor, a safety clutch is attached to the end-of-arm. The safety clutch is designed to prevent or minimize tooling and payload damage if an unexpected collision occurs. The safety clutch uses springs and pneumatically back-loaded plates to provide both collision detection and protection. When a force or torque is detected above a preset value, an electrical circuit triggers the robot E-stop circuit. For protection, the clutch allows the attached tooling and payload to deflect and rotate away from the collision, thus absorbing some of the impact energy.

The tool changer interface consists of a tool plate for attaching and releasing tools that have mating plates, and mechanisms for passage of electrical and pneumatic energy through the interface to a tool. The tool interface is mounted on the safety clutch and is the last in the series of hardware permanently mounted onto the end of the robot arm. (For handling and carrying payloads, the tools grip the payload, and are often referred to as grippers.) The tool latching mechanism is air activated. Safety is enhanced in several ways by control of this air pressure. First, the system is designed to ensure that air pressure remains at operational values whenever a load is carried. Second, the valve position during a power loss will maintain the air pressure to retain a tool. Third, the tool changer mechanism is designed to mechanically hold the tool if air pressure bleeds down over time through a leak in a valve seal or the plumbing. Thus, the tool is held in a fail-safe position on loss of air pressure. Finally, the system is designed with an electrical interlock circuit that prevents activation of the tool release air system unless every tool is in its proper tool storage location in the workcell. This prevents an inadvertent air system activation from causing a release of a tool. In other system designs, a design was used that mechanically locked the mating tool plates together; release was accomplished by activating switches or mechanical lock releases at particular locations in the workcell [3].

An additional safety system planned for the robot consists of a three-axis accelerometer that provides an independent measurement that relates to the loads measured by the force-torque sensor. The accelerometer sensor threshold is set slightly higher than the accelerations that occur in normal operations. The E-stop circuit is invoked if an unexpected motion causes the robot to accelerate more rapidly than normal.

Tool Safety

The robot tools are designed to provide safety in a number of ways. First, sensors at the tool storage locations ensure that automated system operation can only begin if all the tools are at their respective home locations. Second, each tool has a unique mechanical feature that prevents misplacement into an incorrect storage location. Additionally, each tool has a unique electrical identification code that is interrogated by software when the tool is initially picked up. Together, these features verify that the robot has picked up the correct tool. Sensors and switches on the tool are used to detect its current state.

An important safety concern is to prevent a spurious or inadvertent electrical signal from opening a gripper and releasing the payload at an incorrect location. Safety is enhanced in our designs by electrical and mechanical means. The air valve responsible for activating the gripper is a three-position, center-blocked spool valve. To translate the spool to the opposite position and switch the valve, the active solenoid must be deactivated before a second solenoid can make the spool shift. Thus, a single spurious signal to the second solenoid would not move the spool unless the first solenoid was deactivated. The loss of a signal to the first solenoid without a signal to the second will place the spool in the center blocked position, which would maintain air pressure at the gripper. Thus, the payload is held in the case of a loss of air pressure or electrical power.

However, without additional safety designs, the correct sequence of two spurious electrical signals would cause the gripper to open. Also, the sequence could be generated by an inadvertent computer command to open the gripper, caused by a software error or computer malfunction. To avoid these safety-related failures, every gripper that handles radioactive or valuable payloads is equipped with a mechanical latch mechanism that physically prevents the gripper from opening except at particular locations where the part should be released. These locations in the workcell have a mating mechanism that releases the mechanical safety latch; the release is activated either by a software command or as a result of the mechanical positioning of the gripper at the location. These safety latch mechanisms also protect grippers from opening and dropping payloads if a pressure loss occurs in the gripper. A safety latch mechanism example is shown in the gripper in Figure 1.

Station Safety

A station is a location in the workcell where the robot delivers or retrieves a payload. Specific station applications are quite diverse because of the variety of functions occurring at the different stations. The design goals for safety are to protect payloads by avoiding collisions, to perform operations in a precise, controlled manner, and to prevent payloads from becoming damaged as a result of a seismic event. Before payloads are brought into or removed from stations, or mechanical operations are performed on an assembly, the location of relevant station and system hardware is checked to ensure that the next set of motions will be collision-free. This may be accomplished by reading the status of a switch, interrogating another computer system for hardware status, asking for operator confirmation to proceed, or using a robot-mounted camera for video inspection or machine vision analysis.

Vision analysis uses mathematical algorithms to check visual features against geometric information about the workcell. Once it is determined that an operation can be performed without a collision, the robot-mounted camera may be used to automatically position the robot end effector properly, and the force-torque sensor is used to ensure the specific operation is accomplished in a controlled manner. Protection against seismic events is accomplished by using shields to prevent payloads from rolling or falling. Shields can consist of a permanent or retractable fence around a station or location, or the robot gripper acting as a temporary enclosure until the next action occurs.

Safety Procedures

In addition to the many hardware and software safety checks described in the previous sections, administrative procedures and requirements for running the system provide an extra level of safety to the automated systems. As part of the requirements for working on radioactive parts, two authorized, trained operators must be logged in to the computer control system before operations can occur. Different operator capability levels are recognized by the system for different types and safety levels of operations. Logins are accomplished through the use of badge scanners and passwords. Operators are continuously involved in the system operation through providing task instructions and by confirming critical operations. This provides safety by maintaining human control over the system while allowing the system's sensors and control features to provide the appropriate level of detailed computer control. The primary system operations occur from remote or shielded control areas that minimize personnel radiation exposure yet provide visual oversight of the system. When manual operations are necessary, they are performed with protective gloves and shielding.

Several design and implementation features prevent unsafe situations with the radioactive payload. To minimize control room exposure, the amount of time that the payload is near the gloveport is minimized, and the distance between the gloveport and storage locations is maximized. To prevent criticality issues, stations have been positioned in the workcell to ensure that unshielded radioactive payloads will never be closer to each other than a specified minimum distance.

In addition to those already discussed, several other types of sensors and actuators are employed to E-stop the robot in the event of unsafe conditions. Operators have access to manual E-stop buttons in the control room and the workcell. Light beams are used as personnel protection devices around the robot. Facility alarms or a loss of system air pressure will also stop robot motions.

Software Safety

Although the system contains multiple layers of safety features that are independent of software, the system is fundamentally controlled by software, and thus software is involved in various safety-related features of the system.

A rigorous software development methodology is used to help ensure reliable and safe operation of the software. The software is developed using a standard software engineering process with requirements definition, design, implementation, and testing phases. Each phase includes a verification component to identify and correct defects as early as possible. Formal inspections are performed on all documents and software components. During the formal inspections, strict attention is paid to safety-related issues and concerns. At the inspections and throughout all software development activities, decisions are made with careful considerations regarding the impact on system and software safety. Configuration management methods are used throughout.

During the testing phase, the software is validated by rigorous testing using automated tools. The tools are used to instrument the software and, during testing, to return information on code coverage (i.e., what portions of software were tested by the test cases). Other tools are used to automatically repeat tests for regression testing, to detect memory errors, and to perform static analysis on the software to detect defects and indicate potential problem areas. Finally, the system is tested using mock workpieces prior to any operations on real items.

The system contains an independent software process responsible for monitoring various safety-related aspects of the system and generating a robot E-stop if an unsafe condition is detected. As discussed earlier, this process monitors real-time force and torque data from the robot's sensor. The process also monitors robot gripper activity (i.e., get, put, open, and close) in order to detect and report the activation of electrical and mechanical devices associated with grippers. To ensure that the system cannot operate without the safety monitoring process, a watchdog timer is used that will stop the robot if the process is not operating.

In addition, the software contains multiple safety-related features within the mainline code. High-level supervisory control software maintains system state information and schedules the activities of the system. Low-level server software uses sensory information to enforce many constraints to help ensure safe operations. For example, the robot will put down a gripper only if the gripper is open, which indicates that the gripper is empty. Also, the integrity of critical switches is verified during operation by noting the correct state transition, not just the current state. Correct robot movement between stations is enforced by software through extensive verification of the planned motion commands, just prior to execution. For example, the destination must be valid for the current gripper and robot configuration. The software performs system self-testing to ensure that the robot, cameras, and other system components are functioning correctly. The software logs extensive diagnostic information to a database that is essential in determining the cause of an unexpected system event.

Risk Analysis

Because the Sandia robotic systems will handle nuclear materials, the Department of Energy (DOE) requires that safety information about the system be provided as part of the Safety Analysis Report (SAR) required for the facility in which the system is installed. A portion of the SAR includes a risk analysis of the system, and the DOE orders specify a particular safety analysis technique that must be used, called a Failure Modes and Effects Analysis (FMEA). Project engineers in the Intelligent Systems and Robotics Center have worked with Sandia risk assessment analysts to develop the FMEA. The analysts have been able to apply their experience in conducting safety analyses for the nuclear reactor industry to these robotic systems. Two papers in this conference have been written by the Sandia analysts that describe the unique requirements [4] and processes [5] involved in risk assessment for these systems.

The process of developing an FMEA involves determining possible failures of the system (failure modes) and the responses (effects) of the system to each of the failures. For each failure mode, the appropriate failure mechanisms are determined. Then for each failure mechanism, the appropriate detection and compensation schemes are determined. Next, the failure effect is noted. Then a hazard level is assigned based on a qualitative estimate of the likelihood that the failure will occur as well as the severity of the consequences of the failure. As an example, consider the failure mode "joint failure". One of the possible mechanisms that can lead to a joint failure is "seizure of motor or reducer". One of the ways that this failure is detected comes from "overcurrent noted by control software" and the compensation is "excessive current noted by control software results in automatic system shutdown with operator notification at console". Finally, the failure effect is "system shutdown by control software". The process of determining failure mechanism, detection, compensation, and effect is repeated for each failure mode and involves significant effort and cooperation between the project team and the analysts. However, when the process has been completed, the FMEA provides a very detailed picture of the safety features of the system and can point out areas of weakness in the safety design as well as areas where unnecessary redundancy may reduce the system reliability.

Summary

Automated handling of radioactive weapon parts is a sensitive operation and requires much attention to safe operation throughout the design, implementation, analysis, and operation of the system. Safety has been a primary consideration in the design and implementation of the robot, tools, and workcell stations, as well as in the system software and procedures. A combination of mechanical and electrical interlocks was designed for the system. Advanced sensor systems (vision and force) are used to enhance the robot motion control and automated decision capability through improved information about the robot workcell. To help ensure the safety of the software, a rigorous software development process was followed that includes formal code inspections and extensive software testing using automated testing tools; software was developed at multiple levels that monitors various software/system state information and enforces correct behavior. The Failure Modes and Effects Analysis provides a very detailed picture of the safety features of the system and can point out areas of weakness in the safety design as well as areas where unnecessary redundancy may reduce the system reliability.

Acknowledgment

This work was performed at Sandia National Laboratories and supported by the U. S. Department of Energy under Contract DE-AC04-94AL85000.

References

1. "Standard for Industrial Robots and Robot Systems - Safety Requirements," ANSI/RIA R15.06-1992, Robotic Industries Association (RIA), Ann Arbor, MI.
2. B. J. Petterson and J. F. Jones, "Force Servocontrol of a Commercial Gantry Robot," *Robots 12 Conference Proceedings,* Detroit, MI, 1988.
3. J. C. Fahrenholtz, A. K. Morimoto, J. F. Jones, and C. Turner, "Automated Weapon Disassembly," Proceedings of the ANS Fifth Topical Meeting on Robotics and Remote Systems, Knoxville, TN, April 20-23, 1993.
4. W. H. McCulloch, "Safety Analysis Requirements for Robotic Systems in DOE Nuclear Facilities," current proceedings.
5. David Robinson and Chris Atcitty, "Safety Assessment of a Robotic System Handling Nuclear Material," current proceedings.

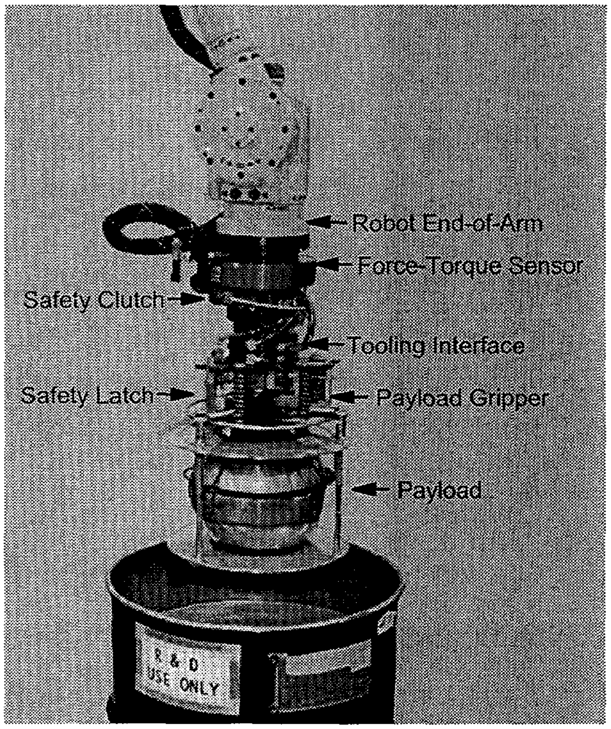

Figure 1. End-of-arm robot tooling configuration.