SAFETY CONSIDERATIONS IN A SURGICAL ROBOT

P. Cain, P. Kazanzides, J. Zuhars, B. Mittelstadt, and H. Paul
Integrated Surgical Systems, Inc., Sacramento, CA

Abstract--This paper describes the safety features of the ROBODOC™ Surgical Assistant System, an image-driven robotic system which has been used to perform Total Hip Replacement surgery. These features include a dedicated processor for continuous monitoring of system status, shared data areas (dual-ported RAM), and external sensors (force-torque sensor, redundant positional encoders, and bone motion monitor).

INTRODUCTION

One of the most crucial steps of Total Hip Replacement (THR) surgery is to create a cavity in the femur that can accept an artificial implant. This procedure is currently performed manually, by pounding a broach (chisel) of the same shape as the intended implant into the femur using a mallet. Complications from this procedure may include gouging and chipping of the cortical bone, as well as femoral fracture. The ROBODOC™ Surgical Assistant System was developed in an effort to reduce these complications and promote more precise placement of femoral implants [1].

The steps in the procedure relevant to the use of robotics are summarized below. For a more detailed description, see [1].

1. Three titanium locator pins are implanted in the patient's femur to provide a geometric frame of reference for preoperative planning and robotic milling during surgery.

2. A Computed Tomography (CT) scan of the femur is taken.

3. The ORTHODOC™ Preoperative Planning Workstation reads the CT data and constructs a three-dimensional image of the bone. The surgeon develops a preoperative plan on the ORTHODOC Workstation by manipulating the three-dimensional images of the femur, along with implant (prosthesis) models, to select an appropriate prosthesis and determine its placement. The output from an ORTHODOC preoperative planning session is a data file that specifies the geometry of the selected implant, the position of the implant in CT coordinates, and the relative position of the three locator pins. These data serve as input to the surgical robot.

4. In the operating room, the surgical robot is draped for sterility and the patient's femur is securely attached to the robot base via a femoral fixator.

5. The surgeon installs a ball probe in the robot's end effector and guides the probe to the approximate location of each locator pin. The robot performs a tactile search to determine the respective positions of the pins. Based on locator pin positions, the robot computes a coordinate transform from CT coordinates to robot coordinates and uses it to translate the surgeon's placement of the cavity in the preoperative plan to orientation and placement data that will guide the robot.

6. The surgeon replaces the ball probe with a cutting tool and the robot machines a precise cavity for the femoral component of the prosthesis.

The milling of the femoral canal by the ROBODOC™ Surgical Assistant requires the robot to work safely and reliably with a surgical team stationed within the robot workspace. The three laws of robotics, penned in the early 1940s by Isaac Asimov and John Campbell, accurately depict the function of the safety systems that we have built into our surgical robot:
1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

2. A robot must obey the orders given to it by human beings, except where such orders conflict with the First law.

3. A robot must protect its own existence as long as such protection does not conflict with the First and Second Laws.

Before introducing a robot into the surgical environment, many hardware safety sensors were added to reduce the risk and potential severity of robot-induced injury. The safety systems of an earlier version of our surgical robot have already been described [2]. Our current safety system includes: a digital signal processor board that serves as a dedicated safety processor (SP); dual-ported (DP) RAM that passes data between a robot control computer (RCC) and the SP; a dual-encoder verification scheme that compares the position of the primary and secondary encoders, which are mounted on input and output shafts respectively; a weight-compensated force sensor system that monitors the forces applied to the robot tool tip; a bone motion monitor (BMM) for detecting movement of the femur relative to the robot base; emergency power off (EPO) capability; and surgical cutter control by the application software, which ensures that the cutting tool receives power only in the absence of error conditions. Additional safety features, such as a check that the cutting tool does not stray outside of a defined safety envelope, are implemented entirely in the software, and are not covered here.

SAFETY PROCESSOR (SP)

The SP assures that the robot operates within set safety limits. These limits include tolerances for forces at the end effector, bone motion, and deviations in arm position. The SP also ensures proper signal propagation for surgical cutter control and Emergency Power Off (EPO) output signals.

The SP has a direct hardware interface to the redundant encoders, force sensor, and BMM. The raw data is processed, then checked against safety tolerances. Two safety levels (exceptions) are defined: FREEZE (or "Pause") and EPO (or "Stop"). If either threshold is exceeded, the response starts with a reflex action (described below) and then raises an exception to the application program. Restoration of function from either exception requires all safety systems to be within tolerance, and operator acknowledgment.

When a FREEZE (Pause) threshold is exceeded, the SP sets the corresponding flag in the shared data area (DP RAM), and the RCC performs the reflex action of halting robot motion and deactivating the cutter (if previously enabled). This reflex action is performed virtually instantaneously because the real-time loop component of the RCC software polls the safety flags every 18.2 milliseconds.

When an EPO (Stop) threshold is exceeded, the SP removes power from the robot motors via a hardware relay, and disables the cutter solenoid. As a redundant backup feature, the RCC real-time loop also performs this function when the SP sets any EPO flag.

Generally, the FREEZE threshold is lower than the EPO threshold, and allows the system to exhibit a more graceful error response. Proper response to a FREEZE exception, however, requires that the SP and RCC be functional. The EPO response can be performed by the SP alone, and serves as a last line of defense for serious error conditions.

The SP also provides pertinent feedback data (e.g., measured force and position) to the RCC via the shared data area. The RCC in turn sends input to the SP. Communication protocols facilitate the transfer of safety system data. The RCC and the SP have two modes of communication: (1) Sending data to, or reading data from the RCC via the DP RAM; and (2) The RCC reading or writing to the I/O bus for ASCII message passing.

DUAL-ENCODER VERIFICATION

Two sets of encoders record the current position of the robot arm, with each set containing five encoders. The monitor the end effectors, the femur position, and the bone reference and compensates for errors. The error can be determined from the difference between the position and the reference.
nd BMM. The d against safety exceptions) are and EPO (or ed, the response ed below) and cation program. other exception within tolerance,

old is exceeded, t the shared data forms the reflex deactivating the reflex action is ly because the C software polls nds.
is exceeded, the xt motors via a ter solenoid. As C real-time loop the SP sets any

old is lower than system to exhibit oper response to uires that the SP response can be ves as a last line ns.
it feedback data to the RCC via turn sends input sols facilitate the RCC and the SP m: (1) Sending RCC via the DP or writing to the

IFICATION

- current position
- containing five encoders. The SP and the RCC continuously monitor the encoders to assure that the position reported by both sets are within predefined safety limits. The safety limits have two thresholds: FREEZE, which will pause the robot; and EPO, which will power off the robot motors. A similar system, using redundant resolvers and a watchdog safety computer, was developed at NBS (now NIST) [3]. The FREEZE and EPO thresholds vary depending upon whether the surgical cutter is active: thresholds are tighter when the robot is actively cutting, but greater velocity is allowed while the cutter is off since the risk of injury is minimal.

FORCE SENSOR SYSTEM

The force sensor is an important safety feature on the robot because it prevents the cutter from straying undetected into the dense cortical bone surrounding the femoral canal. Mounted between the robot wrist and the cutting tool, the force sensor measures six parameters (F_x, F_y, F_z, M_x, M_y, M_z). Changes in the pitch angle, with a symmetrical static load (i.e., the cutting tool), cause changes in three parameters (F_x, F_z, M_y). These can be modeled by the following equations:

\[ D = \sqrt{R_1^2 + R_2^2 - R_1R_2[c(a-b)+(a+b)]} \]

\[ a = \cos(\beta_1 - \beta_2) \quad b = \cos(\beta_1 + \beta_2) \quad c = \cos(\theta_1 - \theta_2) \]

where R_1, \beta_1, and \theta_1 are initial radius, incline, and rotation respectively, and R_2, \beta_2, and \theta_2 are current values.

EMERGENCY POWER OFF (EPO)

The EPO system is responsible for removing power from the robot motors and the cutter in the event of an emergency. An EPO can be triggered by the Axis Control Cards in the RCC, via the Servo Power Module (SPM), as part of the normal safety system. In addition, the robot is equipped with an interruptible current loop to sense when to power down the robot motors. This loop is normally closed, but can be opened by any device connected in series within the loop. An EPO can be triggered in one of two ways: automatically by the SP or manually by depressing the Stop button on the hand-held pendant. The surgeon interfaces with the robot via a pendant and the red Stop button is readily accessible. It is a normally closed, latching switch, which must be manually reset. It is wired in series to the switched side of a normally open relay controlled by the SP.

BONE MOTION MONITOR (BMM)

During femoral canal milling, the bone must be rigidly held in a femoral fixator because a slip of the femur would shift the robot’s milling frame of reference and result in a distorted or malpositioned cavity. If the femur is displaced by more than 2 mm for more than one second, the BMM interrupts milling and alerts the surgeon. The surgeon must reestablish the milling frame before surgery can continue.

The BMM is a passive, three-degree-of-freedom, spherical robot. It is attached when the femur is placed in the femoral fixator and initialized by recording its current location within the robot’s space. After initialization it measures spherical displacements from the initial location using the following equations:
there is power to the robot motors. Fig. 1 shows the wiring diagram for the cutter control. When the robot is powered up, Relay B closes to allow the cutter control signal from the SP to be passed to Relay A. When power to the robot drops for any reason, Relay B opens, causing Relay A to open.

![Cutter Control Diagram](image)

**Fig. 1. CUTTER CONTROL DIAGRAM**

**CONCLUSION**

The safety systems in the surgical robot are designed to minimize the risk of injury to the patient, to provide both automated and manual controls, and to allow the robot to function safely within the surgical theater.

**ACKNOWLEDGMENTS**

The authors would like to acknowledge the contributions of all our colleagues at Integrated Surgical Systems, who have made this surgical robot a reality. We also thank Emily Carbone for her assistance with this paper.

**REFERENCES**

