Failure-Tolerant Robots for Industrial Applications *

K. N. Groom, A. A. Maciejewski, V. Balakrishnan
Department of Electrical & Computer Engineering
Purdue University, West Lafayette, Indiana

21 March 1997

Abstract

Industrial robot failures occur frequently. The consequences of these failures include loss of production time and the possibility of collisions between the robot, work piece, and personnel as a result of unanticipated motions of the arm. Improving manipulator reliability through increased component reliability is often prohibitively expensive, and is sometimes beyond current technology. This paper presents an alternate approach toward improving robot reliability in which kinematically redundant manipulators, those with more degrees of freedom than necessary for the production task, are utilized in a failure-tolerant manner to reduce the immediate impact of a failure and, in many cases, allow the robot to continue the task without reprogramming.

*This work was supported by Sandia National Laboratories under contract number AL-3011.

Introduction

The reliability of industrial robots vary, depending on the application environment and the quality of maintenance. However, a mean-time-between-failure of approximately 500 hours and a mean-time-to-repair of 8 hours are typical [1]. As an example, General Motors, while using 26 Unimation robots in its Lordstown plant, reported an average mean-time-between-failure of 400 hours [2]. This resulted in an assembly line failure rate of one robot every 15 hours and a line downtime of 6 minutes per worker shift. The low downtime was largely due to GM's policy of replacing failed robots with human workers until the robots could be repaired.

In addition to disrupting a manufacturing process, robot failures can pose a serious hazard to personnel and property. In over fifty-five percent of the accidents reported in one Japanese study, the accident was the result of a sudden incorrect action by the robot [1]. Such sudden unplanned motions can result in collisions between the robot, workpiece and unwary individuals.

Methods of improving robot reliability include higher component reliability, improved system design, better manufacturing, and higher quality control procedures. However, besides leading to increased cost, it may be technologically infeasible to improve the reliability of some components. An alternate technique to improving the reliability of industrial robots is to employ failure-tolerant technology. Successfully utilized in the computer, aircraft, and nuclear industries, failure-tolerant systems detect failures, identify their cause and implement recovery actions with the goal of keeping the system operational. Designs with redundant components increase the options available to a failure-tolerant system, thus allowing it to tolerate a broader range of failures.

For failure-tolerant robots, redundancy can take the form of duplicate components, like multiple sensors and actuators on each joint, or can take the form of kinematic redundancy, where a robot with more degrees of freedom than necessary for the prescribed task is employed. In the event of a joint failure, a manipulator that is kinematically redundant with respect to the assigned task can use its remaining operational joints to compensate for the failed joint. The main contribution of this work is a technique that maximizes the effectiveness of kinematically redundant manipulators for tolerating joint failures. This technique is presented after a brief review of robot reliability and failure-tolerant robot designs.

Robot Reliability

To understand how and why robots fail, it is helpful to review their underlying structure. Figure 1 illustrates a robot control system design that is similar to systems found on many commercially available robots. The supervisory controller is a digital computer that provides an operator interface to create, store and execute user programs. It also provides an inverse kinematic routine to convert robot end-effector trajectories, specified in a program, into individual joint trajectories that achieve the end-effector motion. Each joint trajectory is digitally transmitted to a closed-loop servo-control system for the corresponding joint. A joint trajectory is received by a servo controller, also a digital device, that computes the joint torque necessary to achieve the commanded joint trajectory. The output of the servo controller is suitably amplified and used to drive a servo motor, which is connected to the robot links through a gear train for increased torque. The motor is also typically equipped with brakes to prevent the joint from moving when electrical power is removed. The position and velocity of the joint are measured, usually with an optical encoder and tachometer, respectively, and the information is transmitted back to the servo controller, thus closing the servo-control loop.

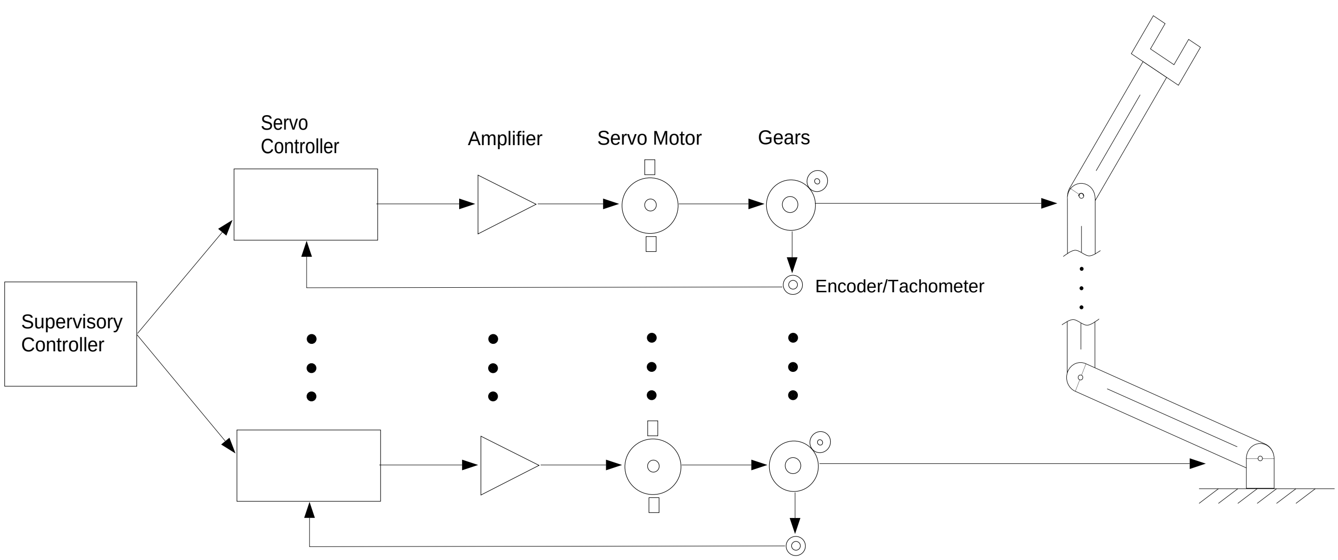

Figure 1: Components of the model robot system.

From the model robot system, two major failure modes are identified. Since the supervisory controller provides data for all the robot joints, its malfunction will likely result in the failure of the entire system. All the remaining components, however, are arranged to control individual joints and a component failure will result in the failure of only the corresponding joint. This point is exemplified by Table 1 where several failure modes for the PUMA 500 are listed with the associated component failures [3].

To quantify the likelihood of a robot failure, Table 2 provides reliability data for the major components of a robot system [4]. The failure rate, λ, of these components is dependent on the application environment. Whenever possible, data for the *ground mobile* (GM) environment was used since this environment more closely resembles that typically found in a manufacturing plant. When ground mobile data was not available, data from an environment that most closely approximates a manufacturing environment was used. Listed with each component are the application environment, the mean-time-to-failure (MTTF) in hours, and the reliability, $R(t)$, of the component at $t = 1,000$ and $t = 10,000$ hours of operation. The reliability, which can be interpreted as the probability of the component working correctly at the given time, was computed from failure rate data assuming an exponential distribution $R(t) = e^{-\lambda t}$. Assuming that the components fail independently of each other, the reliability of a manipulator joint is determined from the product of the reliability for each component. For a robot joint, consisting of an amplifier, servo motor, gear box, and encoder, the reliability, after 1,000 hours of operation in a ground mobile environment, is $R = 0.768$. This can be interpreted as a failure of more than two robot joints for every ten in operation. The MTTF for the joint is 3,784 hours. If every joint of a six degree-of-freedom robot must be operational to successfully complete a task, the reliability of the system, after 1,000 hours of operation, is $R = 0.768^6 = 0.206$. The resulting MTTF is only 630 hours. This figure is consistent with values observed for robots operating in industry; For instance, Dhillon [1] cites a Japanese study in which 75% of the robots had a mean-time-between-failure of less than 1000 hours. Additional figures from that study are given in Table 3.

Failure-Tolerant Robot Designs

Failure tolerance is defined as the ability of a controlled system to continue operating satisfactorily following a failure [5]. To improve the failure tolerance of industrial robots, several techniques may be employed concurrently: automatic decision making by the supervisory controller, robust control by the servo controllers, and redundancy in the robot hardware. These techniques are now discussed.

To avoid halting a robotic manipulator as the result of a failure, the robot must be able to quickly detect that a failure has occurred, identify the source of the failure, and automatically determine an optimal recovery solution. Visinsky et al. [6] and Tso et al. [7] examined the problem of automatic decision making in response to robot system failures and both proposed techniques that use a multi-layer approach, implemented on the supervisory controller. The lower layer uses a pre-computed state machine to provide fast recovery strategies to probable failure situations; rejecting erroneous data from one sensor in a triple redundant sensor group is an example of an action taken at this

Failure Mode	Failed Component
Frozen joint	Supervisory controller failure Servo controller failure Power amplifier failure/overheated Cabling short/open Servo motor failure/overheated Brake failed to release Gear or joint bearing is binding
Runaway joint	Servo controller failure Power amplifier failure Cabling short/open Servo motor failure
Free swinging joint	Power amplifier failure Cabling short/open
Joint position incorrect	Loose drive shaft coupling Slipped gears Potentiometer failure Encoder failure Cabling short/open
Joint improperly tracks trajectory	Payload exceeds recommended weight Servo motor failure Brake dragging Gear or joint bearing is binding
Joint oscillates	Electrical noise on encoder lines Servo controller failure Cabling short/open Servo motor failure Brake failed to release Gear or joint bearing is binding
Joint moves in jerky manner	Supervisory controller failure Servo controller failure Power amplifier failure Cabling short/open Brake dragging Gear or joint bearing is binding Potentiometer failure Encoder failure

Table 1: PUMA 500 failure modes and associated component failures.

Device	Environment	MTTF = $1/\lambda$	$R(1000)$	$R(10,000)$
Servo Amplifier	GB	136,054	0.993	0.929
DC Servo Motor	GM	31,519	0.969	0.728
Gear Box	GM	53,319	0.981	0.829
Hydraulic Servo Valve	GM	6,311	0.854	0.205
Optical Encoder	GM	4,845	0.814	0.127
Tachometer	ARW	9,606	0.901	0.353
Temperature Transducer	GM	75,341	0.987	0.876
Strain Gauge Transducer	GB	83,333	0.988	0.887

Table 2: Reliability of robot components in a ground mobile, or similar, environment. Mean-time-to-failure (MTTF) is given in hours and reliability, $R(t)$, is given at $t = 1000$ and $t = 10,000$ hours of operation. Ground Mobile (GM) components are installed on wheeled vehicles including tactical fire direction systems. Ground Benign (GB) components are installed on non-mobile, laboratory equipment. Airborne Rotary Wing (ARW) components are installed on helicopters.

Percentage of Robots	Mean-Time-Between-Failures
28.7	< 100
12.2	100-250
19.5	250-500
14.7	500-1000
10.4	1000-1500
4.9	1500-2000
1.2	2000-2500

Table 3: Mean-time-between-failures, in hours, for Japanese industrial robots.

level. The upper layer utilizes a more sophisticated decision-making technique, for example an expert system coupled with a knowledge base, to solve more difficult problems. Visinsky et al. [8] proposed utilizing a robot's fault tree as the knowledge base, which allows the expert system to synthesize solutions specifically tailored for that robot. For example, if all encoders for a joint have failed, the expert system can traverse the fault tree to discover a functioning tachometer that can be integrated to provide the position information.

In the event of a robot joint failure, a finite amount of time must pass before the supervisory controller implements a recovery solution, by which time the robot end-effector could have deviated significantly from the desired trajectory. Given that a likely failure recovery action is to lock the failed joint and initiate a short end-effector trajectory back to the original trajectory using the remaining joints, the joint motors may experience large accelerations which can result in instability. The problem is made more difficult if the failure has produced uncertainty in the robot's physical parameters. A servo-control system which provides satisfactory performance, despite the uncertainty in the system model and unusual joint velocities, is described as robust and the problem of robust manipulator servo control is investigated by Ting et al. [9, 10].

While automatic decision making and robust servo control are important to a failure-tolerant robot system, a robot must have redundancy if it is to continue to operate after a component failure. Redundancy is defined as the ability of a system to overcome lost capabilities with remaining resources. For robots, redundancy can take two primary forms, component redundancy and kinematic redundancy. As the name implies, a manipulator with component redundancy is one equipped with backup systems for the manipulator's major subsystems. For example, two encoders, amplifiers, servo controllers and/or servo motors can be used for each joint of the robot [11] [12]. In the event of a component failure, the failed subsystem is disabled and replaced by the backup. However, in addition to the added expense of adding backup systems, it is technically difficult to use two servo motors on each joint of an industrial robot due to the increased weight of the motors and increased complexity of the clutches and gears necessary to disengage the failed motor. These drawbacks motivate the use of manipulators that are kinematically redundant with respect to the task.

A kinematically redundant manipulator is defined as one possessing more degrees of freedom (DOF) than necessary for the intended task. As an example, tasks that require end-effector positioning at various locations within a plane, with the orientation of the end-effector being unconstrained, require a planar manipulator with a minimum of two DOF, as shown in Figure 2(a). Planar manipulators with three or more joints are kinematically redundant for this task and, as a result, can achieve end-effector positions, inside the robot's workspace, with infinitely many joint configurations, two of which are illustrated in Figure 2(b) and (c). Similarly, tasks that require three-dimensional positioning and three-dimensional orienting of the end-effector, require a manipulator with a minimum of six DOF, and manipulators with seven or more DOF are kinematically redundant for the task. Many industrial tasks which currently employ six DOF manipulators actually do not require complete three-dimensional positioning and three dimensional orienting of the end-effector; as a consequence, six DOF manipulators are often kinematically redundant for many common industrial tasks. Kinematically redundant manipulators are capable of tolerating a joint failure since a sufficient number of joints remain operational.

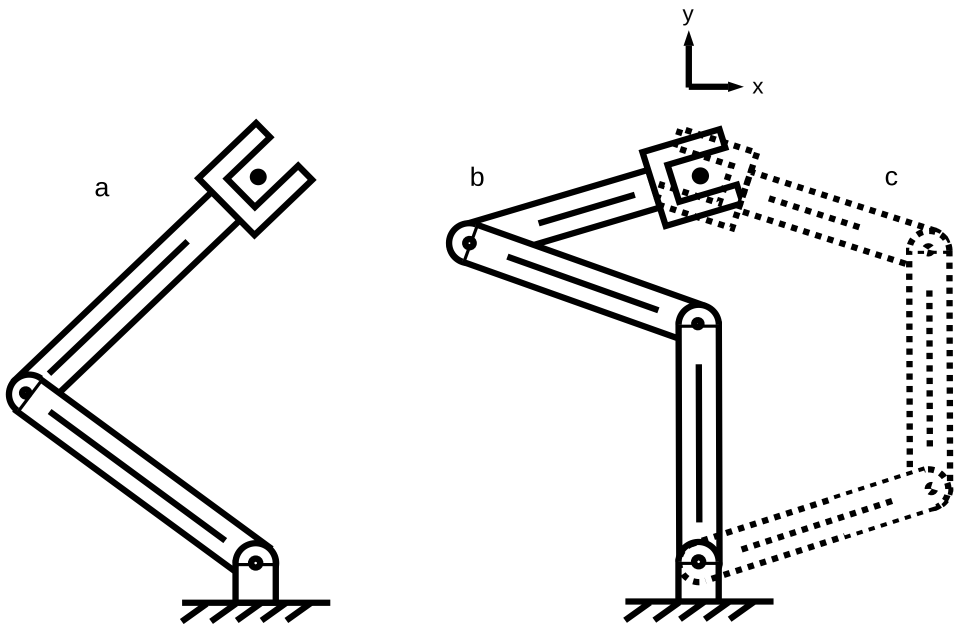

Figure 2: A planar manipulator with two DOF is capable of positioning its end-effector at various locations in the plane, as shown by (a). A planar manipulator with three DOF is therefore kinematically redundant and can achieve the given end-effector position with an infinite number of joint configuration. Two of these configurations are shown in (b) and (c).

Kinematically Redundant Fault-Tolerant Robots

The configuration of a kinematically redundant manipulator at the time of failure has a profound effect on the robot's failure tolerance [13] [14] [15]. For example, if the robot from Figure 2(b), were to experience a locked-joint failure of the third joint from the base, the end-effector would no longer be capable of moving in the positive y direction. Also, high angular velocity in joints one and two would initially be required to move the end-effector in the negative y direction. The robot in Figure 2(c), on the other hand, retains its ability to move in all directions following a failure of any one of its joints and large discontinuities in the joint velocities do not occur as the functioning joints compensate to maintain the commanded end-effector trajectory. Additionally, the post-failure work space in Figure 2(c) is much larger than that of Figure 2(b). This section presents a failure-tolerance measure that gauges these failure effects and provides a method to optimize the measure without interfering with the assigned task.

Kinematic Fault-Tolerance Measure

The position of a robot end-effector, relative to the robot's base, can be determined from simple trigonometric expressions containing the robot's joint angles and link lengths. However, since robot tasks are normally specified by end-effector trajectories, the inverse problem must be solved; i.e., determine the robot joint angles which achieve a given end-effector position. The resulting equations are non-linear and no closed-form solution is know for general robots with greater than five degrees of freedom. A linear relationship does exist, however, between the end-effector velocity and the joint velocity of the robot and is expressed as:

$$\dot{\mathbf{x}} = J\dot{\mathbf{q}} \tag{1}$$

where $\dot{\mathbf{x}}$ is an m-dimensional vector representing the end-effector's translational and/or rotational velocities, $\dot{\mathbf{q}}$ is an n-dimensional vector describing the joint velocities, and J is the m by n manipulator Jacobian matrix [16], which is a function of the manipulator's configuration, $\mathbf{q}$. For a redundant manipulator, $n > m$, so the matrix equation is underconstrained. Therefore, if a single solution to the matrix equation exists, then there exists an infinite number of solutions which also solve the equation. Physically, this means that if the manipulator can achieve the commanded end-effector velocity with one set of joint motions, there are an infinite combination of joint motions which also achieve it. The null space of the Jacobian, $\dot{\mathbf{q}}$ such that $J\dot{\mathbf{q}} = 0$, corresponds to joint motions which result in no end-effector motion. All redundant manipulators have a nullspace and in general it can be used to alter the manipulator's configuration without affecting the end-effector trajectory.

The Jacobian matrix, like any matrix, can be factored into the form

$$J = U\Sigma V^T \tag{2}$$

using Singular Value Decomposition. The orthogonal matrices U and V are composed of left and right *singular vectors*, respectively, and the matrix

$$\Sigma = \left[\begin{array}{ccc|c} \sigma_1 & & \mathbf{0} & \\ & \ddots & & \mathbf{0} \\ \mathbf{0} & & \sigma_m & \end{array}\right] \in \mathbb{R}^{m\times n} \tag{3}$$

contains non-negative *singular values*, σ_i, along its diagonal. These singular values, which change with the robot's configuration, provide insight into how well joint motions by the robot translate into motions of the end-effector, which is referred to as *dexterity* [17]. If the arm is configured such that all the singular values are large, the end-effector can be moved easily in all directions with small joint velocities and the arm is said to be highly dexterous. However, if the arm is configured such that a singular value is small, the manipulator will have difficulty moving in some directions, even if the joint velocities are high, in which case the arm is said to have low dexterity. If a singular value is zero, then the end-effector is not capable of moving in select directions and the arm is said to be in a singular configuration. Therefore, the smallest singular value of the Jacobian provides a measure of the dexterity of the manipulator and gives an indication of how near the robot is to a singularity.

Highly dexterous configurations are desirable since joint velocities are reduced and singular configurations within the robot's workspace are avoided. Kinematically redundant manipulators can continually optimize their dexterity by adding joint motions, derived from projecting the gradient of the Jacobian's smallest singular value onto the Jacobian's nullspace, to the joint motions necessary to move the manipulator along the commanded trajectory, thus increasing the dexterity without affecting the end-effector trajectory. This technique can be extended to optimize failure tolerance. By determining which locked-joint failure produces the worst-case dexterity and using the gradient of its Jacobian's smallest singular value as described previously, the dexterity of the worst-case failed manipulator can be maximized [18]. The smallest singular value of the worst-case joint failure represents a lower bound on the dexterity of the manipulator following a locked-joint failure and is the kinematic fault-tolerance measure used in this work.

An Illustrative Example

To demonstrate the effectiveness of the failure-tolerance technique, a PUMA 560, equipped with a 13.5 inch tool, was programmed to track a straight, thirty inch trajectory, as illustrated in Figure 3. The robot was restricted to move only in the plane of the image, thus reducing the six DOF spatial manipulator to a three DOF planar manipulator. However, the end-effector task requires only two DOF; therefore, the manipulator is redundant for the task. At 14.5 inches of displacement along the trajectory, joint three was failed and locked in place. Three control strategies were evaluated in this way: (1) Traditional inverse position control, where the robot interpolates between joint angle set points, obtained by solving the manipulator's kinematic equations at various points along the end-effector trajectory. The kinematic equations do not account for joint failures, which results in significant errors between the position of the end-effector and the assigned trajectory, after a failure occurs. This is the inverse kinematic control scheme used in virtually all commercial industrial robots. (2) Inverse velocity control, where the Jacobian equation $\dot{\mathbf{x}} = J\dot{\mathbf{q}}$ is used to compute the joint velocities, $\dot{\mathbf{q}}$, necessary to achieve the desired end-effector velocity, $\dot{\mathbf{x}}$. In the event of a joint failure, the Jacobian is easily modified to account for the changes in the manipulator, a column vector is removed, and the new equation is solved for the desired joint velocities. (3) Failure-tolerant control, where the Jacobian equation is also used. However, nullspace motions which optimize the fault-tolerance measure are added to the solution in anticipation of a joint failure, thereby reducing the impact of the failure and improving the post-failure workspace.

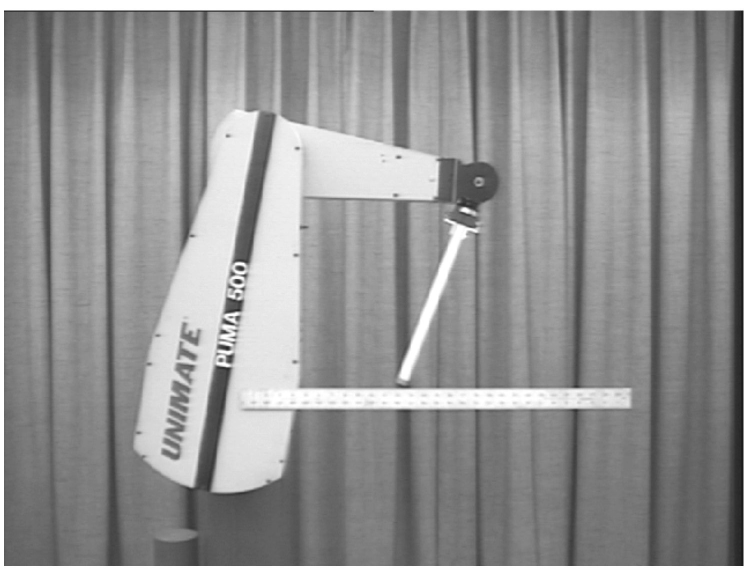

Figure 3: PUMA 560 manipulator tracking a straight line trajectory while restricting motion to the image plane. The manipulator is redundant for the task and fault-tolerant control can be applied.

Figures 4 and 5 illustrate the effects of a joint three failure on the PUMA while using inverse position control. The trajectories of joints one and two are unaffected by the failure of joint three, which drops to zero velocity at the moment of failure. The error in end-effector tracking is given in Figure 10 and is seen to grow quickly after the failure.

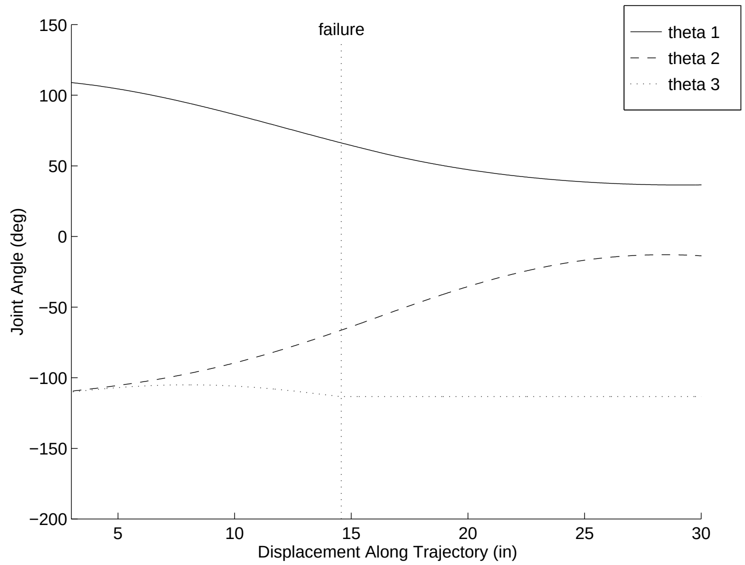

Figure 4: Effects of a joint three failure on joint position while using inverse position control.

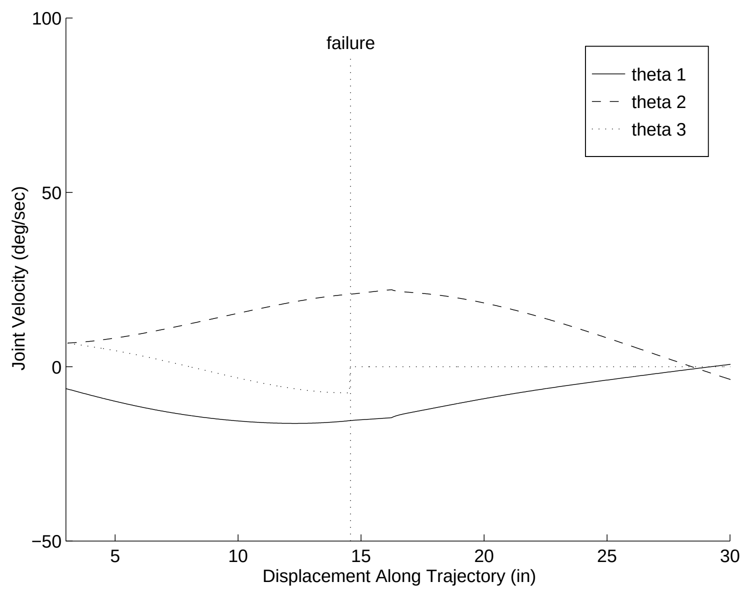

Figure 5: Effects of a joint three failure on joint velocity while using inverse position control.

Figures 6 and 7 illustrate the effects of the joint three failure on the PUMA while using inverse velocity control. At the point of failure, the velocity of joint three drops to zero while large discontinuities are seen to occur in the velocities of joints one and two. A major change in the direction of joints one and two occurs at a displacement of twenty-four inches. This is a result of the failed manipulator reaching the limit of its reach along the path. End-effector error is given in Figure 10 where a significant error is seen at the moment of failure. Because the inverse velocity control method adjusts for failures, the error is quickly reduced back to its nominal value. However, the reach singularity is soon encountered, causing the error to rise out of bounds.

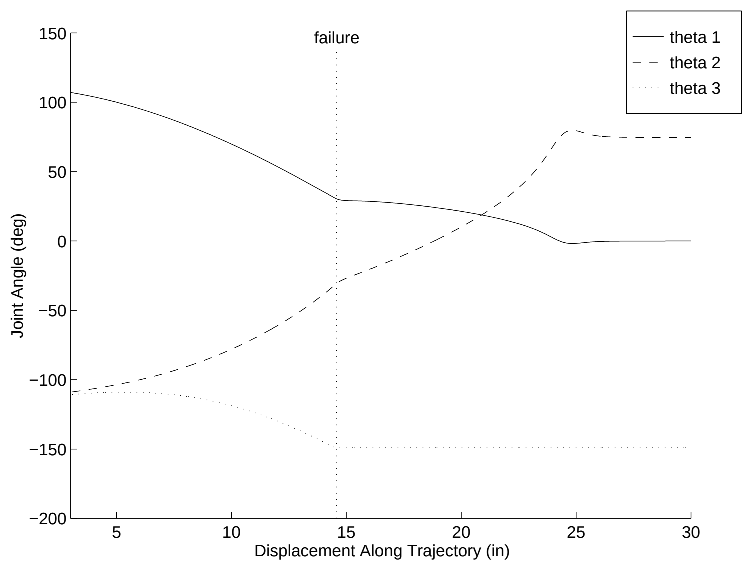

Figure 6: Effects of a joint three failure on joint position while using inverse velocity control.

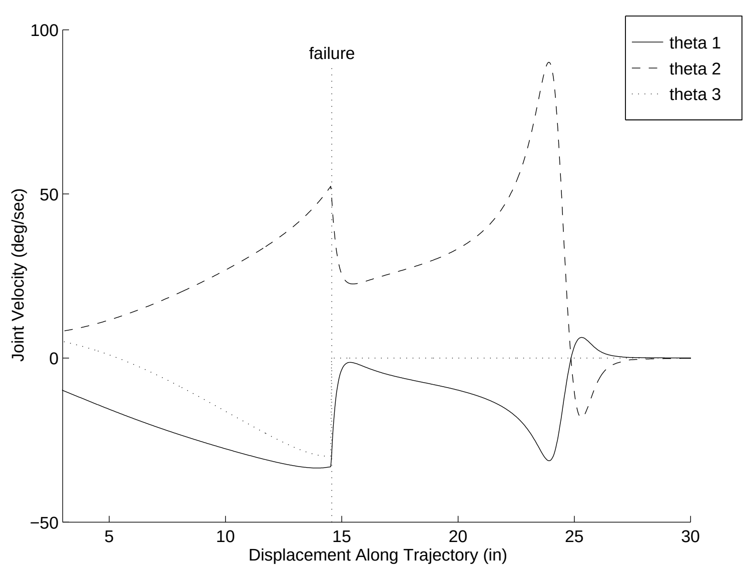

Figure 7: Effects of a joint three failure on joint velocity while using inverse velocity control.

By comparison, Figures 8 and 9 illustrate the effects of a joint three failure while using failure-tolerant control. The discontinuities in joint velocity, at the point of failure, are substantially reduced. End-effector error is also reduced significantly. (Figure 10) Furthermore, sufficient workspace remained after the failure to complete the given task; the reach limit was not encountered.

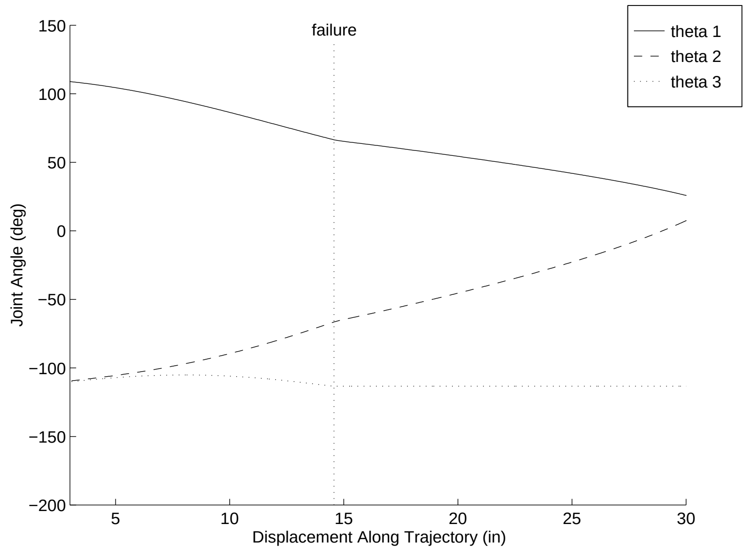

Figure 8: Effects of a joint three failure on joint position while using failure-tolerant control.

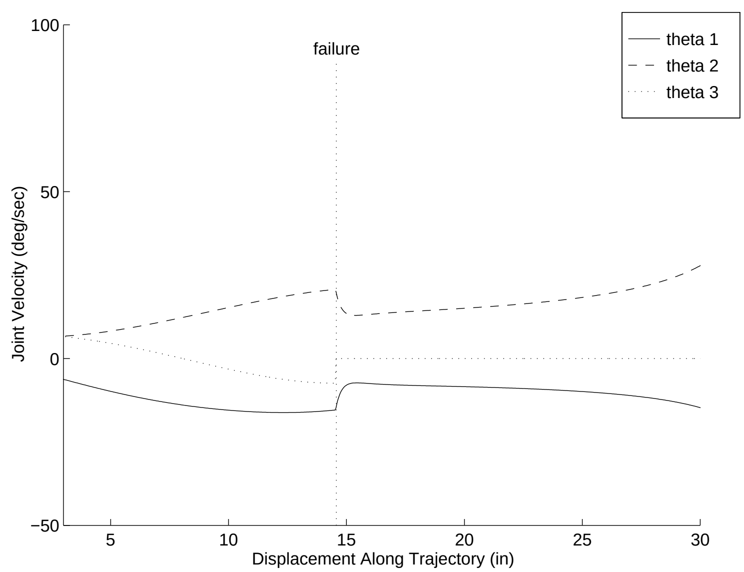

Figure 9: Effects of a joint three failure on joint velocity while using failure-tolerant control.

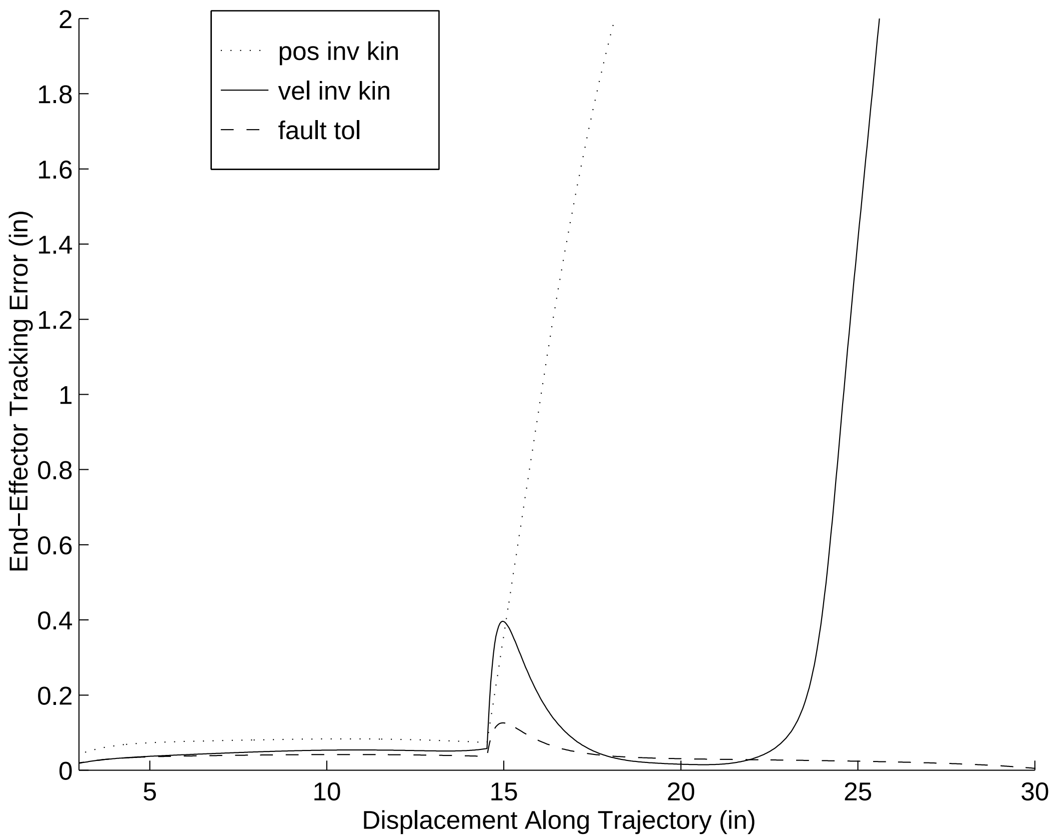

Figure 10: Effects of a joint three failure on end-effector tracking while using inverse postion control, inverse velocity control, and failure-tolerant control.

Conclusions

Industrial robot failures are a statistical certainty. However, because manipulator failures are usually limited to a single joint, kinematically redundant manipulators can often continue a programmed task after a failure by locking the failed joint and compensating with the remaining joints. Maintaining manipulator configurations with a high kinematic fault-tolerance measure prior to failure reduces discontinuities in the joint velocities and end-effector tracking errors at the time of failure. Additionally, the post-failure workspace can be increased.

Acknowledgments

The authors would like to sincerely thank Chris Lewis, of Sandia National Lab, for many useful discussions on this topic. His insights have been a tremendous asset.

References

[1] B S Dhillon. *Robot Reliability and Safety.* Springer-Verlag, New York, 1991.

[2] J. F. Engelberger. Three million hours of robot field experience. *The Industrial Robot*, pages 164–168, June 1974.

[3] Unimation Incorporated. *Unimate Puma Mark II Robot 500 Series Equipment Manual.* Danbury, Connecticut, 1985.

[4] Reliability Analysis Center. *Nonelectronic Parts Reliability Data 1995.* Department of Defense, 201 Mill St., Rome, NY 13440 (315) 337 0900, 1995.

[5] R F Stengel. Intelligent failure-tolerant control. *IEEE Control Systems*, pages 14–23, June 1991.

[6] M L Visinsky, I D Walker, and J R Cavallaro. Layered dynamic fault detection and tolerance for robots. In *1993 International Conference on Robotics and Automation*, pages 180–187, Atlanta, Georgia, May 2-6 1993.

[7] K S Tso, M Hecht, and N Marzwell. Fault-tolerant robotic system for critical applications. In *1993 International Conference on Robotics and Automation*, pages 691–696, Atlanta, Georgia, May 2-6 1993.

[8] M L Visinsky, J R Cavallaro, and I D Walker. Expert system framework for fault detection and fault tolerance in robotics. In *Fourth International Symposium on Robotics and Manufacturing (ISRAM '92)*, pages 793–799, Sante Fe, New Mexico, November 11-13 1992.

[9] Y Ting, S Tosunoglu, and D Tesar. A control structure for fault-tolerant operation of robotic manipulators. In *1993 International Conference on Robotics and Automation*, pages 684–690, Atlanta, Georgia, May 2-6 1993.

[10] Y. Ting, S. Tosunoglu, and B. Fernández. Control algorithms for fault-tolerant robots. In *1994 International Conference on Robotics and Automation*, pages 910–915, San Diego, CA, May 8-13 1994.

[11] D Sreevijayan, S Tosunoglu, and D Tesar. Architectures for fault-tolerant mechanical systems. In *Proceedings of the 7th Mediterranean Electrotechnical Conference*, pages 1029–1033, Antalya, TURKEY, April 12-14 1994.

[12] E Wu, J Hwang, and J Chladek. Fault tolerant joint development for the space shuttle remote manipulator system:Analysis and experiment. In *Fourth International Symposium on Robotics and Manufacturing (ISRAM '92)*, pages 505–510, Sante Fe, New Mexico, November 11-13 1992.

[13] A A Maciejewski. Fault tolerant properties of kinematically redundant manipulators. In *1990 International Conference on Robotics and Automation*, pages 638–642, Cincinnati, OH, May 13-18 1990.

[14] C L Lewis and A A Maciejewski. Optimization of the dynamic performance of redundant robots in the presence of faults. In *Fourth International Symposium on Robotics and Manufacturing (ISRAM '92)*, pages 279–284, Sante Fe, New Mexico, November 11-13 1992.

[15] C. J. J. Paredis, W. K. F. Au, and P. K. Khosla. Kinematic design of fault tolerant manipulators. *Computers and Electrical Engineering: An International Journal*, 20(3):211–220, May 1994.

[16] D E Whitney. Resolved motion rate control of manipulators and human prostheses. *IEEE Transactions on Man-Machine Systems*, MMS-10(2):47–53, June 1969.

[17] C. A. Klein and B. E. Blaho. Dexterity measures for the design and control of kinematically redundant manipulators. *International Journal of Robotics Research*, 6(2):72–83, Summer 1987.

[18] C. L. Lewis. *Fault Tolerance for Kinematically Redundant Manipulators.* PhD thesis, Purdue University, 1994.