TITLE: The Dynamic Balancer Electrical Safety Systems

AUTHOR(S): Herbert Konkel

SUBMITTED TO: Programmatic Distribution

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.
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.
DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.
The Dynamic Balancer Electrical Safety Systems

Herbert Konkel
Probabilistic Risk and Hazard Analysis Group
Technology and Safety Assessment Division
Los Alamos National Laboratory

December 1997
# CONTENTS

<table>
<thead>
<tr>
<th>Abstract</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>2.0. GENERAL SYSTEM DESCRIPTION</td>
<td>2</td>
</tr>
<tr>
<td>2.1. Dynamic Balancer System Layout</td>
<td>3</td>
</tr>
<tr>
<td>2.2. Control Room</td>
<td>3</td>
</tr>
<tr>
<td>2.3. General Electric DC Motor</td>
<td>4</td>
</tr>
<tr>
<td>2.4. Test Turntable</td>
<td>5</td>
</tr>
<tr>
<td>2.5. Hydraulic Plant</td>
<td>5</td>
</tr>
<tr>
<td>2.6. Safety Interlocks</td>
<td>5</td>
</tr>
<tr>
<td>3.0. PRIMARY SAFETY CONCERNS</td>
<td>5</td>
</tr>
<tr>
<td>3.1. Turntable Over-Speed</td>
<td>5</td>
</tr>
<tr>
<td>3.2. Turntable Rapid Deceleration</td>
<td>8</td>
</tr>
<tr>
<td>3.3. Bay-Wall Voltage Resulting from a Lightning Discharge</td>
<td>8</td>
</tr>
<tr>
<td>4.0. NORMAL OPERATION PARAMETERS AND HISTORICAL CONTROLLER SETTINGS</td>
<td>8</td>
</tr>
<tr>
<td>5.0. DYNAMIC BALANCER ELECTRICAL SAFETY SYSTEMS</td>
<td>13</td>
</tr>
<tr>
<td>5.1. Shunt Field Current Monitor</td>
<td>13</td>
</tr>
<tr>
<td>5.2. Motor Armature Over-Voltage Control Module</td>
<td>13</td>
</tr>
<tr>
<td>5.3. Hydraulic Pressure Auto Shutdown</td>
<td>14</td>
</tr>
<tr>
<td>5.4. Case Vibration Shutoff (Moment of Inertia)</td>
<td>14</td>
</tr>
<tr>
<td>5.5. Operator Emergency Shutdown</td>
<td>14</td>
</tr>
<tr>
<td>5.6. Equipment Grounding</td>
<td>15</td>
</tr>
<tr>
<td>5.7. Case Vibration Shutoff (Center of Gravity)</td>
<td>15</td>
</tr>
<tr>
<td>5.8. Circuits in Moviport to Limit Speed</td>
<td>15</td>
</tr>
<tr>
<td>5.9. Motor Over-Current Protective Circuit</td>
<td>16</td>
</tr>
<tr>
<td>5.10. Motor Armature Over-Voltage Control (Over-Speed)</td>
<td>16</td>
</tr>
<tr>
<td>5.11. In-Line Fuses in the Armature and Controller</td>
<td>16</td>
</tr>
<tr>
<td>5.12. Controller Tachometer Feedback Speed Control</td>
<td>16</td>
</tr>
<tr>
<td>6.0. GENERAL SAFETY DISCUSSION</td>
<td>16</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>17</td>
</tr>
<tr>
<td>APPENDIX: Fault-Tree Analysis for Direct-Current Motor Over-Speed Conditions</td>
<td>A-1</td>
</tr>
</tbody>
</table>
THE DYNAMIC BALANCER ELECTRICAL SAFETY SYSTEMS

Herbert Konkel
Probabilistic Risk and Hazard Analysis Group
Technology and Safety Assessment Division
Los Alamos National Laboratory

Abstract

This study was conducted at the request of the US Department of Energy/Albuquerque Operations Office (USDOE/AL) Dynamic Balancer Project Team to identify the electrical conditions required for motor over-speed to occur and to discuss the functions of the various electrical protective features associated with the Dynamic Balancer (DB). As is shown through the development of a fault tree, numerous electrical and human failures are required for over-speed conditions to occur. As directed by the Project Team, no effort was made to develop detailed fault trees for all electrical systems, to quantify basic events in the fault tree, or to develop accident scenarios leading to or resulting from over-speed.

The Pantex Building 12-60, Bay 2, facility electrical circuits and grounding are described, and potential hazards are discussed. DB motor over-speed is a safety concern, and therefore, the controls that limit this condition are described and discussed in detail. Other safety-significant electrical circuits are discussed as well. These safety systems also are described in the facility Basis for Interim Operation (Mason and Hanger, 1997). A potential for a motor over-speed that is not sensed by the standard safety protective systems does exist. This fault pathway is discussed, and recommendations to mitigate its effect are made.

1.0. INTRODUCTION

This report discusses an analysis of the Pantex Plant Dynamic Balancer (DB) electrical safety systems and associated controls. The DB is used to identify physical imbalance in some weapon systems and, because of its potential hazards, requires safety circuits to ensure that the system remains within its expected operational parameters. Bill Peters (SNL, Electrical Engineer), Mark Johnson (Pantex DB facility, Electrical Engineer) and Herb Konkel (LANL, Hazard Analyst and Electrical Engineer) met at Pantex on September 18, 1997, to review the existing DB safety systems and controls and compare them with those discussed in the draft DB Facility Basis of Interim Operation (BIO) (Mason and Hanger, 1997). For some systems, changes were necessary to provide the ability for periodic tests of their safety systems and verify that the safety systems function. Based on this meeting, the engineers recommended that Pantex implement these changes and add components to improve the system's safety. Safety systems require verifiable controls to ensure they are able to perform their safety function.

The September meeting included a discussion of the options for the location and application of the controls, including concerns for nuclear, worker, and equipment safety. The agreed-on goal was that any changes in the electrical circuits should (1) improve safety, (2) have little effect on the present circuits, and (3) attempt to be independent of the existing circuits. Control discussions included methods for the Pantex Calibration and Test Program to periodically test the safety-significant circuits' safety function to verify their proper operation. The equipment and control changes meet the requirements for the safety-significant class designation that some of the electrical safety systems carry in the facility BIO. The recommended modifications from the September meeting have been implemented and are discussed below as part of the safety system.
2.0. GENERAL SYSTEM DESCRIPTION

The DB is located primarily in two adjacent rooms in Building 12-60: a control room and Test Bay 2 (Mason and Hanger, no date). The rooms are separated by earth fill. Bay 1 contains similar DB equipment, but the equipment is unused and the bay is used for other testing activities. Bays 1 and 3 through 6 of Building 12-60 are not relevant to this analysis. The DB facility layout is shown in Fig. 1, which also shows Bay 2 with the electrical conduit connection to the control room and supporting electrical equipment room. This expanded layout will be important later in the discussion on equipment and system grounding.

Figure 2 is a top view of Test Bay 2. The bay is a 21-ft x 21-ft square and contains an approximately 10-ft-square, 3-ft-deep pit. A rack containing the hydraulic plant mounts on the concrete floor at the edge of the pit. A fixture alignment pole mounts in the pit and extends 78 in. above the pit grate cover. A 4/0 copper ground wire attached to the facility ground is attached to the inside perimeter of the bay wall. Metal work tables are provided to hold tools and equipment for the process. The operator uses the wall-mounted TV camera for remote test monitoring.

Fig. 1. Part of Bldg. 12-60, general facility layout and power and instrumentation runs.
2.1. Dynamic Balancer System Layout

The Bay 2 pit area, the control room, and their interconnection are shown in Fig. 3. The pit area contains the dc motor, the drive system for the table, and a 4/0 grounding cable that grounds all pit area metallic components to the facility ground. The illustration shows the dc drive motor and belt linkage to the turntable, the hydraulic plant mounted to the bay floor, and the fixture alignment pole. Metallic grating covers the pit. The grates remain in place until pit access is required. The rotation table on which the rotating fixture is mounted is above the grating.

Three electrical conduits link the test bay to its control room. Electrical power circuits, transducer circuits, and electrical grounds are mixed in the conduits. Power circuits include 480-V ac, three-phase circuits for high-pressure oil pump motors on the hydraulic plant rack; up to 680-V dc for turntable drive motor operation; and lower voltage transducer and control circuits.

2.2. Control Room

The control room measures 8 ft x 8 ft and has an operator console and a chair inside its door area. The console contains a computer to calculate and plot the imbalance and the motor controller and interrupt relays for both the alternating current (ac) and direct current (dc) systems. The 480-V ac, three-phase electrical supply enters the control room and terminates in a disconnect switch panel mounted on the wall to the left of the door. From this switch, the power circuit runs along the wall and enters the control console. The control room has two operator-activated emergency shutdown switches: a red button on the left side of the front panel and a disconnect switch on the wall behind the operator's chair.

The console contains a number of high-voltage circuits. The 480-V ac circuit is protected by 30-amp interrupters in the equipment room. After conversion to dc, the voltage magnitude can be as high as 680 V dc. The 300-V dc supply for the motor field, the 120-V ac supplies for control relays and instrumentation, and numerous other lower voltage supplies are also inside the console.
The circuit that grounds the control console to the facility ground is locally floating (Konkel, 1997a) but connects to the facility ground in the equipment room and at the DB pit. The control console is not grounded locally but is grounded through conductors that run with the 480-Vac power circuits back to the electrical panel in the equipment room and with the power conductors that run to the pit area. This causes a worker safety concern because of the potential voltage difference between the console and of the conductive metallic wall surfaces within the control room. An electrical fault or transient conditions in the pit area or the equipment room can cause a transient voltage on the console surface, subjecting the worker to an electrical hazard. Bonding the control room metallic components to a ground within the control room would eliminate this hazard.

2.3. General Electric DC Motor

A General Electric (GE) dc, shunt-wound, Type CD2110AT electric motor drives the rotating table. The motor has a 7.5-hp rating at 500 Vdc with a rated armature current of 12.5 amp and a rated speed of 1750 rpm. The voltage and current ratings for the field are 300 Vdc and 0.8 amp, respectively. This motor is totally enclosed and fan-cooled and has a National Electrical Code (National Fire Protection Association) Class I, Group D, rating. (National Electrical Code Class I, Group D establishes design requirements for electrical equipment operating in flammable gas atmospheres.) Electrical equipment in the test bay requires special-rated components because of the potential hazards in the bay. A thermostat in the motor has normally closed contacts with 600-Vac and 0.5-amp ratings with higher current rating at lower voltages. The motor also contains a tachometer with output dc voltage proportional to motor speed.
2.4. Test Turntable

The DB turntable is turned by a drive belt that is run through a power train. The power train includes a bevel gearbox for speed reduction and direction change and the dc shunt motor. The drive belt has an automatic tensioning wheel that adjusts to provide constant belt tension. The drive shaft has a series electrical isolation device to isolate the table electrically from the motor. This belt linkage provides a 2.8:1 turning rotation reduction between the motor and table and limits the mechanical acceleration or deceleration of the table through belt slippage.

2.5. Hydraulic Plant

A rack is connected to the floor close to one edge of the pit on which the high-pressure hydraulic system is mounted. The rack includes temperature and pressure sensors for the system and two high-pressure hydraulic pumps and their respective 480-Vac drive motors. The hydraulic system contains 160 L of hydraulic oil, and a heat exchanger is used for oil cooling.

2.6. Safety Interlocks

To prevent an inadvertent start of the DB, the bay and bay doors have interlock switches linked to the control relay circuits. Both bay entry doors have interlocks that open the interlock circuit when the respective door opens. A third interlock switch, located on the wall of the bay, opens the DB motor control circuit. Pantex Nuclear Explosive Operating Procedures (NEOPs) require that the wall-mounted interlock switch be in the “off” (open) position while the bay is occupied. This switch prevents the motor from starting when it is in the “off” position. The physical lockout capability of this switch is unknown. Before a test, the last person leaving the bay returns the interlock switch to the “on” (closed) position.

3.0. PRIMARY SAFETY CONCERNS

Two primary safety concerns are turntable over-speed and turntable rapid deceleration. A lesser issue is the voltage buildup on the bay wall from lightning discharge to it. Turntable over-speed can occur only if the motor over-speeds. Because the motor speed is proportional to the armature voltage and inversely proportional to field current, both of these motor parameters require protective measures and associated controls. Appendix A provides a detailed discussion of the conditions for motor over-speed and the associated safety circuits.

3.1. Turntable Over-Speed

Turntable over-speed can occur only if the motor over-speeds. GE Industrial Systems was asked for the over-speed characteristics for the turntable dc motor (GE Model 5BY454A74) (Konkel; Konkel, 1997d; Krivonak**). The GE engineer said the maximum speed for this motor is about 4500 rpm based on the assumption that all controls fail and an infinite supply of electrical power is available. GE also said this is an older motor (1985 manufacture) and lacks a number of safety features found in current motors. Two parameters will limit motor speed to 4500 rpm: (1) the rotational physical limits of the cooling fan and (2) the electrical commutation limits of the motor [Konkel, 1997d(a); Konkel, 1997d(b)]. At high motor speeds, the motor cooling fan will physically rip apart, causing shrapnel in the immediate area. Motor commutation problems such as sparking and flashover limit motor over-speed.

Pantex performed several tests (Weaver, no date) to determine the DB system’s maximum speed capability from available console adjustments. For the table load, the test used a fixture without a unit mounted. Several data points from this test are shown in Table 1. The test data showed that a motor speed of 2184 rpm could be achieved with 637 Vdc applied to the armature and the field current constant. Lower motor rpm’s occurred with lower armature voltage.

Using the standard linear rated voltage and motor-speed ratio for 680 V, the motor and table speed are 2380 and 850 rpm, respectively. From tests with a measured 680 Vdc on the armature, the table speed reading was about

---


800 rpm, which corresponds to a motor speed of 2240 rpm. Possible beginnings of turntable speed limits and electrical limits of the supply may explain the difference between the theoretical and actual rpm. This test showed the speed capability of the DB system without the field current being changed.

**TABLE 1**

**MOTOR ELECTRICAL TEST DATA UNDER LOAD**

<table>
<thead>
<tr>
<th>Motor RPM</th>
<th>Armature I Amperes</th>
<th>Field Volts</th>
<th>Table RPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1652</td>
<td>490 5</td>
<td>284</td>
<td>590</td>
</tr>
<tr>
<td>1854</td>
<td>552 5</td>
<td>282</td>
<td>662</td>
</tr>
<tr>
<td>2164</td>
<td>637 6</td>
<td>284</td>
<td>773</td>
</tr>
<tr>
<td>2184</td>
<td>637 6</td>
<td>281.8</td>
<td>780</td>
</tr>
</tbody>
</table>

GE engineers were asked about changes in motor characteristics as the field current changes with constant armature voltage (Agnew*). Beginning with a rated field current of about 0.83 amp, Fig. 4 shows how unloaded motor speed theoretically increases and torque decreases as the field current decreases with a constant armature voltage of 500 Vdc. The field current was increased by a factor of 10, for convenience, to plot both the torque and field current on a common scale. This graph shows that a theoretical speed of 4450 rpm occurs if the field current drops to 280 ma at an armature voltage of 500 Vdc. Again, using a linear armature voltage ratio for motor speed, the theoretical field current at 680 Vdc and 4500 rpm would be 420 ma.

Figure 5 shows the relationship between motor torque and the motor speed, and the relationship between the motor armature power and the motor speed in rpm. The lines in Fig. 5 reflect the present DB system controller settings and dc motor characteristics. The dotted curve “A” and the heavy solid curve “B” plot relationships between the torque and motor speed as the field current is varied or held constant. The dashed curve “C” and the solid line “D” plot the relationships between the power and the motor speed.

Line “A” plots the motor torque in Newton-meters vs the motor speed as the field current decreases. Line “A” is generated from calculated values with the present electrical protection limits of the controller and fuses. Point “A1” is the maximum motor torque at the desired motor speed of 770 rpm. Point “A2” shows the motor torque and speed when the field current is decreased to half of the rated value. Thus, line “A” shows that as the field current decreases, the speed increases and the torque values decrease.

Line “B” shows the increase in torque required for various motor speeds resulting from increasing armature voltage. Thus, line “B” shows the increased motor torque required to overcome rotational losses and maintain a given motor speed. The data points B1 through B4 reflect the test data in Table 1, which were obtained from tests conducted before the power restrictions on the controller. As line “A” approaches and crosses line “B”, the torque requirements limit the motor speed to approximately 1500 rpm.

Line “C” plots the power in watts required for various motor speeds. The data points C1 through C4 also reflect the test data in Table 1, which were obtained from tests conducted before the present power restrictions on the controller. Thus, greater motor armature power is required to achieve higher speeds.

The horizontal line “D” is the maximum power currently available from the controller. Thus, the point where “C” crosses the horizontal line is the maximum motor speed with the power constraints of the controller. Note that both the maximum motor speed because of the controller power constraints and the maximum motor speed because of the torque limitations occur at approximately 1650 rpm.

---

Fig. 4. Motor speed and torque as the motor field current decreases.

Fig. 5. Motor torque and power for various speeds.
Much higher motor speeds can be expected if the converter drive circuits fail and allow high voltage to be applied to the armature circuit. If this scenario occurs, over-speed protection is provided by the over-voltage monitor relay, VM1, which would provide an interrupt to the K101 relay and deenergize the motor circuit.

Appendix A provides a detailed discussion of the conditions required for motor over-speed to occur. These conditions are as follows.

1. The controller drive circuits would have to provide full-on energy to the converter circuits.
2. The controller/regulator over speed circuits would have to fail to sense over speed.
3. The independent dc armature voltage monitor would have to fail to detect high dc armature voltage or fail to interrupt the K101 relay when the high dc voltage was detected.
4. The operator would have to ignore or misinterpret the high speed indication on the control panel readout. The control panel readout could also fail to indicate the high speed condition.
5. The dc fuses would have to fail to interrupt the dc armature current.

A high-impedance fault pathway in the motor field current could lead to a reduction in field current resulting in motor over-speed. This issue also is discussed in Appendix A.

3.2. Turntable Rapid Deceleration

The turntable can decelerate rapidly if the mechanical system seizes. Low oil pressure or loss of oil could result in seizure of the spindle shaft and turntable. Thus, the hydraulic system is a safety concern requiring positive measures and associated controls. This issue is not discussed here but is discussed in a companion report by Bott (1997).

3.3. Bay-Wall Voltage Resulting from a Lightning Discharge

The BIO discusses a recent Sandia National Laboratories lightning report that stated the need to maintain a 1-ft separation between the unit and the wall because of the high voltage potential on the wall from a lightning discharge to the bay. Between the unit and wall, the 1-ft separation distance is subsumed in the explosive safety manual's required 3-ft wall separation. (The 3-ft separation is required because of wall spalling from explosion outside the bay, not because of grounding.) However, because the metallic components in, around, and over the DB pit are grounded to this same wall, the 1-ft separation may apply to the metallic components around the pit area. Pantex has upgraded the grounding for the electrical conduit and metallic runs into the bay, which lowers the voltage potentials that occur from lightning conditions. However, high voltage exists on the bay wall from lightning conditions and within the pit area from grounding to facility ground. This potential high voltage will occur in the bay working area around the pit during lightning discharges to the facility.

4.0. MOTOR CONTROLLER OPERATION AND HISTORICAL CONTROLLER SETTINGS

Figure 6 shows the relationship between the motor controller and its ac and dc power circuits and their control relays. This figure shows some of the positive measures listed in Table 2. The 480-Vac, three-phase circuit (L1, L2, and L3) has 30-amp protection and supplies the DB system from the facility equipment room (see Fig. 1). Transformer T2 reduces 480 Vac to about 220 Vac for the field voltage converter to provide a 300-Vdc source to the motor field. Transformer T1 provides 120 Vac for the DB system's control relay power.

Safety features shown in Fig. 6 are the “D1 Test Breaker,” the special fuses, and the VM1 over-voltage relay across the armature circuit (Konkel', 1997a). The D1 Test Breaker is a large breaker capable of interrupting high dc voltage circuits. The D1 Test Breaker’s multicontacts are wired in series to achieve dc high-voltage interruption. This breaker is used to interrupt the motor’s field circuit, which tests the controller’s “loss of field current” safety circuits that de-energizes the DB system.

Figure 6 shows a 480-Vac, three-phase power circuit supplying the converters for the dc voltage to the armature circuit. This circuit has 10-amp fuses to limit current magnitude to the motor and is a positive measure limiting motor over-speed. A fuse in the second dc pole of the motor power circuit provides redundancy for over-current

*Discussions between H. Konkel (LANL), W. Peters (SNL), and M. Johnson (Pantex) in 1997.
Fig. 6. Power and control circuits feeding the controller.

A second interrupter (K101) isolates the controller circuit during field circuit testing and provides redundancy (to the K5 relay) and independence for armature over-voltage condition interrupts.

A primary requirement for motor over-speed to occur is high armature voltage. The VM1 relay was installed to monitor over-voltage across the armature and is independent of the controller. Upon over-voltage detection, a horn alerts the operator, and the power circuit is interrupted by the K101 relay. The threshold level of the over-voltage relay is adjustable, and the calibration technician can use this adjustment to test the relay periodically.

Motor external speed and acceleration limits are set with potentiometers at the control console. Comparator threshold levels can be adjusted in the controller by a controller manufacturer’s representative for over-speed and over-current. The K100 relay uses the built-in features of the controller to provide an interrupt when preset limits for over-speed and over-current are exceeded.

The DB electrical controller and regulator equipment have a much higher current supply rating than the 12.8-amp motor-rated load they control in the DB. Until recently, the controller limit settings that monitored and protected the regulator were well above the current values needed for the actual load. The settings allowed the motor to rotate so that the table speed was almost 800 rpm, which is far higher than the 275-rpm desired load rotation. Recently, Bill Peters had the controller manufacturer representative adjust the motor controller parameter settings to the expected load electrical parameters, then reset the sensors to the lower parameter limits. The lower values will limit table speed to a maximum rotation speed of about 275 rpm for normal operation.

Because armature voltage is directly proportional to the motor speed, limiting the armature circuit voltage magnitude will limit motor rotation speed. This characteristic is used for monitoring the conditions for motor over-speed.
<table>
<thead>
<tr>
<th>Control/Feature</th>
<th>Location</th>
<th>Type</th>
<th>Description Control/Feature</th>
<th>Setting (if known)</th>
<th>Purpose/Basis</th>
<th>Surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shunt Field Monitor</td>
<td>Brown Boveri Controller</td>
<td>SS</td>
<td>When a drop in the current below a set point is detected, a relay is opened and initiates an automatic interrupt to the power circuit.</td>
<td>Relay interrupts with a drop of 15% to 25% in normal field current of 0.8 amps or about 0.6 amps.</td>
<td>Ensures the integrity of the shunt field circuitry. Prevents overspeed.</td>
<td>Monitor circuit and interrupt relay logic tested every 6 months during DB calibration.</td>
</tr>
<tr>
<td>Motor Armature Over-Voltage Control Module</td>
<td>Schenck Console</td>
<td>SS</td>
<td>Uses secondary contractor and activates an alarm and auto shutdown. Provides independent over-speed protection.</td>
<td>Over-voltage monitor set to just above 275 Vdc.</td>
<td>Prevents over-speed. Limits the motor armature voltage. Initiates shutdown through relays that are independent from normal shutdown path.</td>
<td>Monitor and interrupt circuit checked and tested every 6 months during DB calibration.</td>
</tr>
<tr>
<td>Hydraulic Pressure Auto Shutdown</td>
<td>Schenck Console</td>
<td>SS</td>
<td>Interrupts drive motor circuit if hydraulic pressures on radial or axial bearings are lower than lower limit.</td>
<td>15 bars</td>
<td>Protects spindle/ bearing assemblies in the event of hydraulic system failure. Provides an indication of hydraulic fluid loss.</td>
<td>Hydraulic pressure monitor tested and calibrated during DB calibration.</td>
</tr>
<tr>
<td>Case Vibration Shutoff (Moment)</td>
<td>Schenck Console</td>
<td>SS</td>
<td>Moment determination that initiates shutdown of the drive motor if a limit setting is exceeded.</td>
<td>300 N-m limit setting</td>
<td>Protects the drive system against imbalances. Initiates shut down.</td>
<td>Checked during DB calibration during emergency shut-off verification. Also checked during operational procedures.</td>
</tr>
<tr>
<td>Operator Emergency Shutoff</td>
<td>Schenck Console</td>
<td>SS</td>
<td>Removes power from the DB.</td>
<td>Operator interrupt.</td>
<td>Protects against over-speed and other unforeseen circumstances.</td>
<td>Checked during DB calibration during emergency shut-off verification. Also checked during operational procedures.</td>
</tr>
<tr>
<td>Control/Feature</td>
<td>Location</td>
<td>Type</td>
<td>Description Control/Feature</td>
<td>Setting (if known)</td>
<td>Purpose/Basis</td>
<td>Surveillance</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Equipment Balancer Grounding</td>
<td>Balancer Spindle</td>
<td>DiD</td>
<td>Conductive brushes are in contact with the lower portion of the spindle.</td>
<td>N/A</td>
<td>Prevents static buildup on the fixture and the unit under test.</td>
<td>During DB calibration during system ground verification.</td>
</tr>
<tr>
<td>Case Vibration Shutoff (CG)</td>
<td>Schenck Console</td>
<td>DiD</td>
<td>Center of gravity interrupts drive if off-set limit is detected.</td>
<td>Offset greater than 1000 N.</td>
<td>Protects the drive system against imbalances. Initiates drive interrupt.</td>
<td>None. Functionality of this feature cannot be conclusively demonstrated.</td>
</tr>
<tr>
<td>Circuits in Moviport to Limit Speed</td>
<td>Moviport Chassis Within Schneck Console</td>
<td>DiD</td>
<td>The chassis produces desired speed and ramp rates by providing a control voltage to the controller.</td>
<td>300 rpm maximum</td>
<td>Limits face-plate rpm. Provides protection against intentional acts.</td>
<td>None. Functionality of this feature cannot be conclusively demonstrated. Power supply value and 300-rpm limit checked during 6-month DB calibration cycle.</td>
</tr>
<tr>
<td>Motor Over-Current Protective Circuit (Over-Current at Current Limit)</td>
<td>Brown Boveri Controller</td>
<td>DiD</td>
<td>Circuit limits armature current. Controller read-adjusted to low level. Operator adjustments restricted to a narrow speed range.</td>
<td>Controller limit setting restricted to 275 Vdc to limit speed to 300 rpm.</td>
<td>Limits power available to the drive by limiting current to the armature. Prevents over-speed by initiating auto interrupt if over-current occurs</td>
<td>None. Monitor and interrupt circuit have been tested. Control adjustment available to the operator.</td>
</tr>
<tr>
<td>Motor Armature Over-Voltage Control (Over-Speed)</td>
<td>Brown Boveri Controller</td>
<td>DiD</td>
<td>Monitors speed by monitoring armature voltage. Controller limit setting restricted to 275 Vdc to limit speed to 300 rpm.</td>
<td>Controller limit setting restricted to 275 Vdc to limit speed to 300 rpm.</td>
<td>Limits power available to the drive by limiting voltage to the armature. Limits face-plate speed by initiating auto interrupt if over-voltage occurs.</td>
<td>None. Auto interrupt because of over-speed was tested by Brown Boveri. Auto interrupt not verified during calibration per Brown Boveri recommendation.</td>
</tr>
<tr>
<td>Control/Feature</td>
<td>Location</td>
<td>Type</td>
<td>Description Control/Feature</td>
<td>Setting (If known)</td>
<td>Purpose/Basis</td>
<td>Surveillance</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>In-Line Fuses in Armature (2) and Controller (3)</td>
<td>Schneck Console</td>
<td>DiD for fuses in armature</td>
<td>Limits over-current to the controller and to the motor armature.</td>
<td>Fuses in the ac controller (3) and in the dc armature (2) circuits have 10-amp ratings.</td>
<td>Limits controller input and output power. Limits motor to currents necessary for application. Provides motor protection.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Controller Tachometer Feedback Speed Control</td>
<td>Brown Boveri Controller and Motor</td>
<td>Operational control</td>
<td>GE BC42 tachometer provides voltage proportional to shaft speed.</td>
<td>N/A.</td>
<td>Maintains set speed for a wide range of loads. Limits the faceplate speed (rpm) by reducing the current applied to the motor if speed increases.</td>
<td>Tachometer output levels checked in the DB calibration during the controller operability test after other safety checks to ensure proper operation.</td>
</tr>
</tbody>
</table>
5.0. DYNAMIC BALANCER ELECTRICAL SAFETY SYSTEMS

Because motor over-speed is a potential nuclear safety concern, additional emphasis is placed on the controls of the positive measures guarding against this hazard. It is not sufficient to have safety devices or circuits (positive measures) that limit the system to safe operations if those systems are not tested periodically to ensure that they perform their safety function. The periodic tests of the safety systems are considered controls. In addition to the controller, the electrical safety circuits include independent sensors that monitor armature voltage and current.

The DB electrical safety circuits, associated positive features, and controls are summarized (Konkel, 1997c; Mason and Hanger, 1997b) in Table 2. The first column lists the identified DB safety system positive feature. Column 2 lists the location of the positive feature, and column 3 identifies the class of control: safety significant (SS) or defense in depth (DiD). Column 4 describes its safety function, and the test setting is listed in column 5. Columns 6 and 7 describe the purpose of each positive measure and periodic tests performed to ensure its safety function performance, respectively.

The identified controls depend on the Pantex Calibration Program to periodically (6-month cycle) test each safety circuit for its operation and to set threshold levels for interrupts or alarms. Some potential hazards exist in this calibration. For example, what ensures that the proper set points are set into the safety threshold circuits, and what ensures the system is ready for operation after the test is complete?

Sections 5.1 through 5.12 discuss each electrical control feature and its safety function.

5.1. Shunt-Field Current Monitor

The shunt-field current monitor is a safety feature that monitors for a drop in field current, thereby avoiding motor over-speeds by initiating a power circuit interrupt to the K5 relay. The monitor initiates an interrupt when the field current drops below a set point of approximately 75% of the 0.8-amp motor field current rating with a 300-V supply. The interrupt de-energizes the ac electrical circuit feeding the controller and motor circuits. Although the shunt field current monitor is part of the existing circuit, it was not possible to test its functionality. Therefore, the “D1 Test Breaker” was added to the field circuit. When the breaker is opened (only during testing), it drops the field current to zero (which is below the set point), causing the interrupt of the K5 armature circuit relay and a loss of power to the motor.

To perform the motor shunt-field current monitor test, the technician first interrupts the K101 relay, which isolates the controller and motor circuit and eliminates the possibility of motor operation should power energize the console and field controller/regulator circuit. After the power circuit is isolated by the K101 relay, the technician opens the field circuit using the D1 Test Breaker. The controller senses the loss of field current and initiates a system shutdown by disabling the K5 relay circuit.

This test is performed during a calibration cycle without energizing the motor armature circuit because the K101 relay is open. During the test, there is no unit in the bay, and therefore, there is no nuclear safety concern. To operate the D1 Test Breaker, the technician reaches into the rear of the console, which has a number of high-voltage circuits. The control room is small restricting access to the rear of the control console, presenting potential worker safety hazards.

5.2. Motor Armature Over-Voltage Control Module

A safety feature to monitor motor armature dc voltage is an over-voltage control module identified as VM1. Because the armature voltage is directly proportional to motor speed, an automatic shutdown can be initiated through monitoring the armature voltage, thus avoiding the motor over-speed condition. The module consists of a voltage monitor relay across the terminals of the controller dc output to the motor armature. The over-voltage relay detects dc voltage on the armature circuit and initiates an interrupt when the voltage exceeds a threshold preset level (currently about 300 Vdc). The over-voltage relay interrupt trips the K101 relay, isolating the armature circuit from the 480-Vac source and automatically shutting down the motor.
The motor armature over-voltage control module has a set point that is checked during each calibration and maintenance period. The set points are checked by reducing a set point to below 250 Vdc and then ramping the armature voltage through the set point, causing the K101 relay to interrupt. After verifying that the motor shut down, the technician readjusts the set point back to the threshold value.

There is no unit in the bay during the test; therefore, there is no nuclear safety concern. There are worker safety concerns associated with exposure to hazardous high voltage. Because the over-voltage relay set point is readjusted for testing, the technician may fail to return the set point back to the desired level, causing the over-voltage circuit to have an improper setting when operations are resumed.

5.3. Hydraulic Pressure Auto Shutdown

The hydraulic pressure auto shutdown system monitors the hydraulic pressure supplied to the radial and axial bearings and initiates an automatic shutdown when low hydraulic pressure is detected. The K5 relay trips upon detection of low pressure, initiating an interrupt to the motor circuit and shutting down the motor.

The hydraulic pressure test is part of the calibration cycle for the DB equipment. The test is used to verify the accuracy of the two pressure transducers and the hydraulic plant gauges. As in the shunt-field current monitor test, the technician isolates the armature circuit by disabling the K101 relay. The transducers and gauges are checked by applying a variable pressure source to the lines monitored by the transducer at the hydraulic plant. The K5 relay is tripped when the applied pressure drops below the transducer threshold, deenergizing the motor circuit. Fittings are installed on the gauges to allow them to be calibrated, and the gauges are included in the plant calibration program.

The test is performed without the motor armature circuit energized and without a unit in the bay; therefore, there is no nuclear or worker safety concern. However, because of the high hydraulic pressures, worker safety concerns may arise and potential equipment damage may occur if the fittings are misinstalled or are damaged.

5.4. Case-Vibration Shutoff (Moment of Inertia)

The case-vibration shutoff monitors the moment of inertia by calculating it from displacement measurements of the spindle. The displacement measurements are supplied by the vibro control (VC2000) module of the controller. If the limit setting of 300 Nm is exceeded for three consecutive seconds, a shutdown is initiated by sending interrupts to the K3 and K4 relays, which in turn send interrupts to the K5 relay and cause the motor to shut down. These and the other DB system control relays are shown in Fig. 7.

The case-vibration shutoff is tested during the DB equipment calibration cycle. The test uses a fixed imbalance on the fixture attached to the turntable. The imbalance is detected upon start-up, which initiates a motor circuit interrupt. The test is performed with the motor armature circuit energized but without a unit in the bay, so therefore, there is no nuclear or worker safety concern.

5.5. Manual Emergency Shutdown

The manual emergency shutdown is used when the operator detects a motor over-speed or other unforeseen event. The operator activates the emergency shutdown circuit by pushing the red "Emergency Shutdown" button on the control panel. An operator-initiated emergency stop interrupts the K3 relay, which deenergizes the power circuit of the motor when the K5 relay interrupts.

The operator-initiated emergency shutdown is tested during DB calibration and during bay setup procedures. While the motor is operating at a low speed (approximately 30 rpm), the operator performs the emergency shutdown test by activating the red panel button. If the circuit operates properly, the DB system shuts down. Because the operator performs the test at low motor speed, without a fixture on the rotating table, and without a unit in the bay, there is no nuclear or worker safety issue.
5.6. Equipment Grounding

To prevent static buildup on the fixture and the unit under test, conductive brushes are in contact with the lower portion of the balancer spindle. These brushes drain any static buildup to facility ground. Static charge occurs with charge transfer from the rotation of the fixture in air and the belt drive. These brushes keep the unit at the facility potential.

During the DB calibration, equipment grounding is verified during the system ground verification test by measuring the resistance between the table and facility ground. There are no nuclear or worker safety concerns with this test.

5.7. Case Vibration Shutoff (Center of Gravity)

The center-of-gravity monitor detects case vibration offset. A system shutdown is initiated when an offset greater than 1000 N is detected. This circuit is part of the VC2000 module, and its system interrupt is similar to the interrupt described in Sec. 5.4. Because of the high threshold magnitude of the sensors, this feature cannot be demonstrated conclusively; therefore, no surveillance or associated test is performed.

5.8. Circuits in Moviport to Limit Speed

The circuits in the Moviport chassis in the DB console control the voltage and thus produce the desired speed and ramp (de)acceleration rates. The controller operating and safety circuits recently were readjusted to the expected application speed. Limits set within the controller restrict its operation range to a very narrow operating window. These parameters include a maximum operating table speed of 275 rpm and an armature voltage of 300 Vdc.

Individual circuits, such as over-speed, can be tested during set-up by setting the speed adjustment to the maximum position, which is very close to the 275-rpm limit. A second test measures the maximum armature voltage, which currently is set at about 300 V. A higher armature voltage would indicate a potential for higher motor
speed. These tests are performed during the DB calibration. Because of their functionality, these controller features cannot be demonstrated conclusively, so no surveillance or associated test is performed.

5.9. Motor Over-Current Protective Circuit

The motor over-current protective circuit in the controller limits armature current and thereby limits the power available to the motor. The motor over-current protective circuit prevents over-speed by sensing an over-current and initiating an auto shutdown. The motor over-current protective circuit is not part of a surveillance program. However, the monitor and shutdown circuit were verified in previous tests.

5.10. Motor Armature Over-Voltage Control (Over-Speed)

The motor armature over-voltage control monitors armature voltage and limits the motor speed by limiting the voltage available to the armature (Brown Boveri, 1984; Brown Boveri, no date). The armature voltage interrupt level is set to 275 Vdc (below the 300-Vdc setting of the over-voltage VM1 relay). When an over-voltage is sensed, an automatic shutdown is initiated through the K3 relay. At the recommendation of the controller manufacture, Brown Boveri, the automatic shutdown is not verified during calibration.

5.11. In-Line Fuses in the Armature and Controller

There are two special in-line 10-amp fuses in the dc armature circuit and three special in-line 10-amp fuses in the ac phases of the converter input. These fuses limit the current to the converter and motor armature. An increase in armature current above normal operation causes the fuse to interrupt the motor circuit. The fuses are sized to just above the DB normal operating range for the expected load. There are no nondestructive tests for the fuses; therefore, they are not tested during the calibration cycle.

5.12. Controller Tachometer Feedback Speed Control

The controller tachometer feedback speed control compares the electrical output of a tachometer [a GE BC42 tachometer (General Electric, no date)] mechanically linked to the motor with a set point equivalent to a rotation table speed of around 275 rpm. If the tachometer value exceeds the set point, a relay contact within the controller opens the K3 relay, shutting down the DB system. This safety feature is tested during the DB calibration cycle by adjusting the turntable speed to over 275 rpm and observing the system shutdown.

6. GENERAL SAFETY DISCUSSION

The recent addition of controls that verify the operability of the safety-significant electrical systems should improve the safety and reliability of the DB equipment. The DB system level of safety improved significantly after the controller safety parameters were adjusted for the application rather than the much higher parameters used for equipment protection. Present settings restrict the controller to a very narrow window of operation. A chance of over-speed still exists but at very low torque levels that provide slow acceleration. An operator should be able to detect turntable speeds above normal and initiate an emergency interrupt before the rotation reached hazardous levels.

However, as discussed in Appendix A, there is one potential fault condition that could cause motor over-speed with the DB system electrical parameters remaining within their normal operating range. In this situation, the over-speed condition could go undetected by the electrical safety systems. A high-impedance fault that diverts current from the field circuit could cause motor over-speed and remain undetected. This fault creates a parallel path to the field circuit, diverting current around the field circuit. The effect is a reduction in field current without detection by the field monitoring circuit or other electrical sensors. Because all other electrical parameters would remain within their operating ranges, the standard safety protection systems would not sense any change. The only circuit that would detect an over-speed condition would be the speed comparator circuit, which compares the tachometer output with a value equivalent to about 275-rpm table revolutions. In normal operation, the controller would cause the K3 relay to trip when the speed exceeds the preset level. However, if that circuit fails to detect over-speed, the only interrupt would be by operator activation of the emergency stop. If the operator fails to detect the abnormal operation, high motor over-speed may occur.
The present calibration program does not include impedance checking of the field circuit. Because of the high 300 Vdc in the field circuit, dielectric breakdown could go undetected for a long time. Several hundred milliamps diverted from the field circuit could have a significant effect on the motor speed. Pantex may want to consider a method to periodically check the impedance of the field circuit from the controller to the motor.

Protective feature failures required to allow maximum over-speed are modeled graphically in the fault tree and discussed in Appendix A. The fault tree shows the redundancy and diversity of the over-speed protection. The cut sets of the fault tree include several failure events, including the initiating events that produce high voltage at the dc motor. Based on a qualitative evaluation of the over-speed fault tree, the likelihood of turntable over-speed is very small.

REFERENCES


Brown Boveri Co.. No date. DC Controller Operating Instructions, Publication No. D HS 251881 E.

General Electric. No date. Instructions for Explosion Proof Direct Current Motors and Generators, Publication GEH-4200C.


National Fire Protection Association. No date. NEPA 70, National Electric Code (Batterymarch Park, Quincy, Massachusetts).

Weaver, S. No date. Pantex Test Configuration and Summary Sheets from DB Tests.
Introduction

Motor over-speed is considered to be a primary initiating event for Dynamic Balancer (DB) accidents. Thus, the DB design includes a number of key controls to prevent over-speed conditions. A direct current (dc) shunt-field wound motor drives the DB turntable. The conditions needed for motor over speed include a reduction in field current or an increase in armature voltage. Abnormal conditions in both parameters have a significant effect on motor over-speed. Most of the controls that sense abnormal conditions depend on the motor controller. Controls that monitor abnormal conditions and provide interrupts and whose safety function can be verified are considered safety significant. Other controls whose operation is not verified periodically are considered defense-in-depth protection. This latter class includes special circuit fuses to interrupt the motor power circuit on motor over-current and controller circuits that monitor armature current, motor speed, and other parameter settings.

Analysis

A fault tree that identifies potential paths leading to motor over speed is developed in Figs. 1–7. The top event, shown in Fig. 1 shows conditions required for motor over-speed. These conditions are a reduction in motor field current or high dc voltage applied to the motor armature circuit, failure of the operator to sense over-speed, and a protection system failure allowing over-speed conditions. The first condition is a reduction in field current, which is developed in Fig. 2. High armature voltage also causes motor over-speed, and the high-voltage conditions are shown in Fig. 3. The portion of the tree identifying the failure of the protection circuits to interrupt is developed in Fig. 4.
To monitor for over-speed conditions, the operator views the test operation by remote television and has a
tachometer speed display on the console. With any abnormal condition, the operator can initiate an emergency
shutdown by depressing a large red button on the front panel. This emergency circuit is not part of the controller but
contains contacts in series with other safety circuit contacts that will interrupt control relays, including the motor
circuit. The emergency shutdown switch is considered safety significant and is tested before each operation.

The fault tree developed in Fig. 2 reflects possible failure that could lead to a reduction in motor field current.
As shown in the fault tree, field current reduction occurs with an open field circuit, a high-impedance fault that
provides a parallel path to the motor field circuit (thus reducing the current through the field), or a fault in the field
circuit outside of the motor. The motor circuit controller includes controls to monitor the field current and interrupt
the motor circuit if the field current drops below about 75% of its rated value. This field current monitor would
detect an open circuit. However, the field current monitor would not detect high-impedance faults or pathways that
bypass the motor field circuit.

The events that could lead to an increase of motor armature voltage are developed in Fig. 3. The DB system can
supply about 680 Vdc to the armature under abnormal conditions—well above the motor’s 500-Vdc rated armature
voltage. For high voltage in the armature motor circuit to occur, the controller would have to misoperate because of
spurious signals and provide a broader drive signal to the converter gate circuits. For maximum voltage, the
misoperation would have to occur with each of the six converter gates in the circuit. A misoperation affecting fewer
than the six gates would result in a lower armature voltage.

Failure of the SCR control module could result in high dc voltage applied to the motor armature circuit. The
motor speed varies proportionally with the armature voltage. To limit the voltage to the armature, Pantex adjusted
the controller operation point to about 275 Vdc maximum. Because of the complexity of the motor controller
settings, the controller operating point is not adjusted periodically but is verified by system performance during
operation and calibration.

A circuit independent of the controller also monitors the armature circuit voltage. This circuit is discussed later,
and its fault tree is shown in Fig. 7.

---

Fig. 2. Tree showing conditions for low field current.
High dc voltage applied to motor armature

Spurious signal fires the SCR

Failure of the SCR control module

Fig. 3. Conditions for high armature voltage.

Figure 4 shows the numerous protection circuits both within the controller and independent of the controller that could lead to over speed. All protection circuits shown in Figure 4 would have to fail to allow motor over speed. There are special fuses on both the alternating current (ac) and dc sides of the motor converter module. Interruption by any one of the ac fuses would limit energy available for over-speed, whereas any one fuse operation in the dc circuit would interrupt power flow to the motor circuit. A controller failure would not detect differences in signals between the speed set by the operator and the actual speed from a tachometer attached to the mechanical motor drive. A speed marginally greater than the value set by the operator normally would cause motor circuit interruption by the controller with the K5 relay. For the motor to continue its over-speed condition, the armature isolation relays (K5 or K101) would have to fail to interrupt the ac power to the motor converter circuit. The K5 relay is the primary interrupt, three-pole relay in the ac circuit. A second relay (K101) in series with the K5 relay isolates the motor circuit during some DB tests and provides an independent circuit interruption for high armature voltage detected by the VM1 over-voltage relay. The fault tree for each of these protection circuits is discussed below.

Figure 5 shows the conditions required for circuit interruption by the special protective fuses caused by over-current in the motor’s ac and dc circuits. The fuses are considered special because their size depends on the normal electrical load of the controller. Pantex recently replaced the motor over-current protection fuses with fuses having much lower current interrupt ratings; these fuses will interrupt at currents levels a margin above the load requirement. The present fuses are rated at 10 amp and replace the much larger 30-amp fuses. The fuses are in the motor circuit on both the ac side and dc sides of the converter. Each ac phase circuit has its own fuse and is independent of the other phase fuses. Interrupting only one of the three ac phases will reduce the power to the motor and, if available, should trigger a power source interruption because of phase current imbalance. The dc armature circuit has a fuse in each pole, and they will interrupt independently of each other.

The fault tree in Fig. 6 shows the controller circuits that must fail for the controller to fail to interrupt the motor power circuit because of abnormal conditions. This controller includes monitor circuits that will cause an interruption of the ac converter power circuit K5 relay for dc motor armature circuit over-current, over-voltage or abnormal over-speed conditions. Separate modules within the controller monitor electrical parameters supplying the motor. These modules have relays that open on a detected abnormal condition. The system designer connects the contacts of these relays in series with the electrical control circuits of the system. If a module within the controller detects an abnormal condition, the module relay contacts open, which interrupts the control circuit relay, usually leading to an alarm and system shutdown.
Protection system failure allows over speed

AND

DC fuses fail to open as required
Special AC phase fuses fail to open as required
DC motor controller fault
Armature isolation interrupt fails to function on demand

D
E
F
G

Fig. 4. Tree showing the over-speed protection from protection circuits.

Fig. 5. Fuse protection tree for the ac and dc motor circuits.
A number of protective circuits are built within the controller. Failure in any of these circuits can cause a controller fault and lead to possible motor over-speed. These faults may be in the motor acceleration (ramping) circuits, the circuits that compare desired with actual motor speed, or the circuits that supply the speed comparator. This type of fault would cause an invalid signal to the converter drive circuit and could cause the SCRs to supply high voltage to the motor armature circuit, resulting in motor over-speed. A fault in the converter circuit also could cause this condition. Any condition that causes or leads to a longer SCR turn-on time results in higher voltage applied to the armature circuit, thereby increasing motor speed.

Under certain abnormal conditions, a stuck interrupt contact within one of these modules could prolong the application of ac voltage to the converter and could result in motor over-speed.

If high voltage is applied to the armature and if the controller fails to detect this over-voltage, an over-voltage relay (VM1) circuit independent of the controller relay will sense and interrupt the ac motor circuit by interrupting the K101 relay. The fault tree for this circuit is shown in Fig. 7. This circuit is set to interrupt with armature voltages above 300 Vdc. The circuit could fail to interrupt from a fault in the VM1 sense relay or if the K101 relay contact sticks.
Conclusion

A fault-tree analysis for over-speed conditions shows that over-speed can occur from high-impedance faults in the field circuit. Although there are a large number of safety circuits and controls in the DB system, it is possible for motor over-speed to occur from high-impedance faults in the field circuit. These faults create a parallel path to the field circuit, thereby diverting current around the field circuit. The effect is a reduction in field current without detection by the field monitoring circuit. Because all other electrical parameters are within their operating range, the standard protection systems would not sense any change. The only circuit that would detect an over-speed condition would be the speed comparator circuit, which compares the tachometer output with a value equivalent to about 275 rpm table revolutions. In normal operation, the controller would cause the K3 relay to trip when the speed exceeds the preset level. However, if that circuit fails to detect over-speed, the only interrupt would be by operator activation of the emergency stop. If the operator fails to detect the abnormal operation, high motor over-speed may occur.

The current calibration program does not include impedance checking of the field circuit. Because of the high 300 Vdc in the field circuit, dielectric breakdown could go undetected for a long time. Several hundred milliamps diverted from the field circuit could have a significant effect on the motor speed. Pantex should consider a method to check the impedance of the field circuit from the controller to the motor periodically.

The fault tree illustrates the redundancy in the over-speed protection. The cut sets of the fault tree all include several failure events, including the initiating events that produce high voltage at the dc motor. In a system with high redundancy, common-cause failures may defeat the multiplicity of safety features. For example, the DB safety system has multiple fuses that are subject to common-use failures. This failure could result of fuses replaced en masse, and hence a faulty batch of fuses could result in all the fuses in the system being faulty at the same time. The DB safety system includes diverse protection from circuit breakers and the motor controls; therefore, even the failure of all the fuses is not sufficient to defeat the safety features.

Another possible common-cause fault that could disable several parts of the DB safety system is improper setting of the set point parameters in the control equipment during calibration. The probability of this common-cause
failure could be reduced if calibration procedures include assurance that the system is set properly before returning the equipment to operation.

Finally, aside from the high-impedance fault pathway in the motor field circuit discussed above, the following conditions would have to be present for motor over-speed to occur.

1. The controller drive circuits would have to provide full-on energy to the converter circuits.
2. The controller/regulator over-speed circuits would have to fail to sense over-speed.
3. The independent dc armature voltage monitor would have to fail to detect high dc armature voltage or fail to interrupt the K101 relay when the high dc voltage was detected.
4. The operator would have to ignore or misinterpret the high-speed indication on the control panel readout. The control panel readout also could fail to indicate the high-speed condition.
5. The DC fuses would have to fail to interrupt the DC armature current.

Because all of these conditions need to be present, the motor over-speed scenario is very unlikely.