



Ride Motion Simulator Safety Assessment Report

Test Report No.: 2013-MBT-SAR-RMS

Issued: 7/1/2013

Prepared By:

Victor J. Paul

Research Electrical Engineer, Motion Base
Technologies team

Reviewed and Approved By:

Harry Zywiol

Team Leader, Motion Base Technologies team



TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 JUL 2013		2. REPORT TYPE		3. DATES COVERED	
4. TITLE AND SUBTITLE Ride Motion Simulator Safety Assessment Report			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Victor Paul			5d. PROJECT NUMBER 2013-MBT-SAR-RMS		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army TARDEC, 6501 East Eleven Mile Rd, Warren, MI, 48397-5000			8. PERFORMING ORGANIZATION REPORT NUMBER #23990		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The Ride Motion Simulator (RMS), located at the U.S. Army Tank Automotive Research, Development and Engineering Center's (TARDEC) Ground Vehicle Simulation Laboratory (GVSL) in Warren, Michigan, is a high-performance, six degree-of-freedom (DOF), single occupant motion base designed to recreate the "ride" of nearly any ground vehicle with high precision and accuracy. The simulator has two vehicle cabs that are essentially space frames that allow for a variety of vehicle configurations. The simulator was specifically designed for crew station and human-in-the-loop experiments. The RMS has a much higher bandwidth than most traditional driving simulators enabling it to recreate the high-frequency vibration often found in military vehicles traversing rough, cross-country terrains. The RMS was previously safety certified by both the U.S. Army Tank-automotive and Armaments Command (TACOM) and U.S. Army Developmental Test Command Safety Offices and was originally man-rated for operator-in-the-loop experiments. It has been used in a number of research and engineering studies including the characterization of warfighter body/seat dynamics, vehicle inceptor comparisons, warfighter-machine interface development and soldier task-load and cognition research.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 37	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

NOTICE:

Reference herein to any specific commercial company, 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 the Department of the Army (DoA). The opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government or the DoA, and shall not be used for advertising or product endorsement purposes.

DISPOSITION INSTRUCTIONS

This document shall not be reproduced except in its entirety. Destroy this document when no longer needed. Do not return document to its originator.

Permission to further disseminate this proposal must be obtained by Motion Base Technologies, TARDEC.

TABLE OF CONTENTS

1.0	Introduction.....	4
2.0	Objectives	4
3.0	Conclusions.....	4
4.0	Recommendations.....	4
5.0	Discussion.....	4
5.1	SYSTEM DESCRIPTION.....	5
5.2	SYSTEM PERFORMANCE	6
5.2.1	MAXIMUM SYSTEM ACCELERATION/DECELERATION	8
5.3	RMS HAZARD EVALUATION.....	9
5.4	SAFETY ANALYSIS OF EACH SUBSYSTEM	10
5.4.1	HEXAPOD SAFETY ANALYSIS.....	10
5.4.1.1	HEXAPOD DESCRIPTION.....	10
5.4.1.2	HEXAPOD STRUCTURAL INTEGRITY	12
5.4.1.3	HYDRAULIC FAILURES RELATING TO THE HEXAPOD	13
5.4.1.4	ELECTRICAL FAILURES RELATING TO THE HEXAPOD	14
5.4.2	HYDRAULIC SUPPLY AND DISTRIBUTION SAFETY ANALYSIS	14
5.4.2.1	HYDRAULIC SUBSYSTEM DESCRIPTION.....	14
5.4.2.2	HYDRAULIC FAILURES	16
5.4.3	ELECTRONIC CONTROLS AND SAFETY ANALYSIS	17
5.4.3.1	ELECTRONIC CONTROL DESCRIPTION	17
5.4.3.1.1	Real-Time Computer.....	18
5.4.3.1.2	PILZ Safety PLC.....	20
5.4.3.1.3	Servo Control Unit and Analog I/O Chassis	21
5.4.3.1.4	Operator Computer	22
5.4.3.1.5	Simulation Host Computer.....	23
5.4.3.2	CONTROLLER SOFTWARE.....	23
5.4.3.2.1	Controller Software Safety Features	23
5.4.3.3	CONTROLLER ELECTRICAL FAILURES	24
5.4.3.4	TRANSDUCER FAILURES	25
5.4.4	System failure response	25
5.5	SYSTEM HAZARD ANALYSIS TABLE.....	32
6.0	References.....	37

1.0 Introduction

The Ride Motion Simulator (RMS), located at the U.S. Army Tank Automotive Research, Development and Engineering Center's (TARDEC) Ground Vehicle Simulation Laboratory (GVSL) in Warren, Michigan, is a high-performance, six degree-of-freedom (DOF), single occupant motion base designed to recreate the "ride" of nearly any ground vehicle with high precision and accuracy. The simulator has two vehicle cabs that are essentially space frames that allow for a variety of vehicle configurations. The simulator was specifically designed for crew station and human-in-the-loop experiments. The RMS has a much higher bandwidth than most traditional driving simulators enabling it to recreate the high-frequency vibration often found in military vehicles traversing rough, cross-country terrains. The RMS was previously safety certified by both the U.S. Army Tank-automotive and Armaments Command (TACOM) and U.S. Army Developmental Test Command Safety Offices and was originally man-rated for operator-in-the-loop experiments [1]. It has been used in a number of research and engineering studies including the characterization of warfighter body/seat dynamics, vehicle inceptor comparisons, warfighter-machine interface development and soldier task-load and cognition research.

In the mid-1990's, TARDEC contracted with MTS Systems (Eden Prairie, MN) to build and install the Ride Motion Simulator with "Man-Rated" status granted in 1998 (See original Safety Assessment Report Dated December, 1998 [2]). The writing of this report marks the replacement of the simulator's electronic controller with a custom Moog Test Controller for the simulator to improve performance and maintainability.

This report documents the analysis of the new motion controller for the RMS designed, built and installed for TARDEC by Moog, Inc. (East Aurora, NY). It provides system and component descriptions and a specific hazard analysis of the entire system. While this effort only replaces the electronic controls of the simulator, all simulator system and component descriptions are presented here for completeness.

The scope of this analysis is the systematic assessment of the real and potential hazards associated with the RMS. This report is an attempt to identify hazards and to discuss the elimination or control of the identified hazards.

2.0 Objectives

The objective of this report is to provide documentation that ensures that the RMS is safe for human-in-the-loop operations with the new controller upgrade. This document can also significantly supplement and support a safety confirmation release for the RMS by Army safety leadership.

3.0 Conclusions

All known safety hazards have been evaluated throughout the analysis of the RMS. The design features and safety devices for the RMS, when used in conjunction with test specific operating procedures, will reduce the probability of injury to occupant or damage to equipment to a satisfactory level sufficient to certify it for Human-in-the-loop experiments.

4.0 Recommendations

Because of the changes in the RMS controller, software and new User Interface (UI), it is recommended that TARDEC's Motion Base Technologies team update the previously developed simulator checklists

(LQP-14-2-W102) and Standard Operating Procedure (LQSOP-14-2-2) that it uses for Operator in the loop testing. In addition, it is recommended that the Motion Base Technologies team Quality Coordinator conduct a systematic review of the current ISO17025 documentation to reflect the new controller. Furthermore, it is also recommended that the RMS be approved for Human-in-the-loop operation based upon the findings described throughout this report.

5.0 Discussion

5.1 SYSTEM DESCRIPTION

The Ride Motion Simulator is based upon the Stewart platform style of motion platform design. This mechanism, also commonly referred to as a hexapod, uses six linear actuators to connect a triangular fixed base with a triangular motion platform. The six actuators, the base and the platform form a near octahedral structure. Through control of the six actuators, this mechanism provides for independent or simultaneous motion of the platform in the six natural degrees-of-freedom.

The RMS is composed of the following major subsystems:

- Hexapod
- Hydraulic Supply and Distribution
- Electronic Controls
- Controller Software

Figures 5-1 and 5-2 are photographs of the RMS and its new electronic controller.

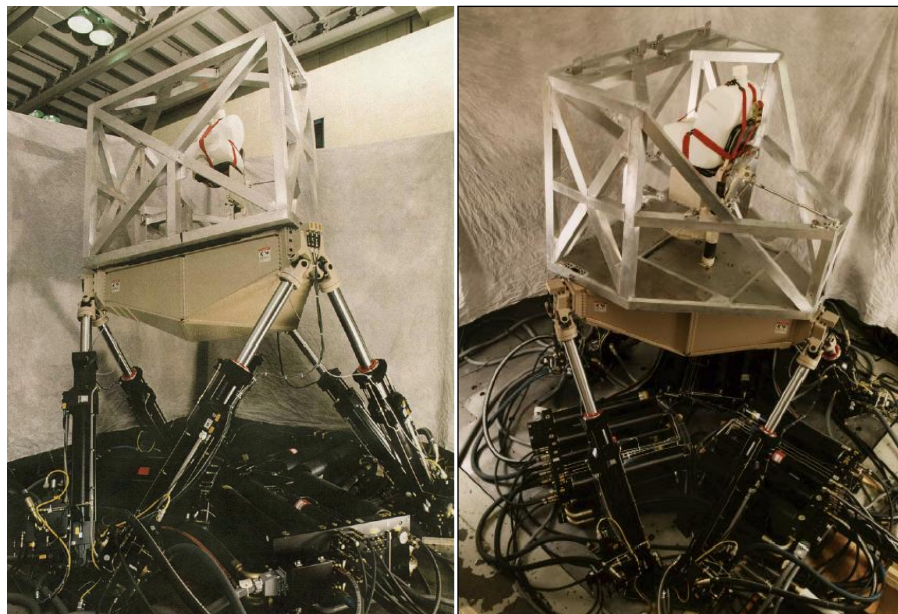


Figure 5- 1 Ride Motion Simulator (RMS)



Figure 5-2 *New Ride Motion Simulator Control Cabinet*

5.2 SYSTEM PERFORMANCE

The original specifications for the actuators and platform of the RMS motion platform are summarized below:

- Payload: 0 to 1500 lb
- Performance capability per axis (maximum independent, transient motion):

Axis	Displacement		Velocity		Acceleration	
X (longitudinal)	± 20 in	± 0.51 m	± 30 in/s	± 0.76 m/s	± 1.0 g	± 9.81 m/s ²
Y (lateral)	± 20 in	± 0.51 m	± 30 in/s	± 0.76 m/s	± 1.0 g	± 9.81 m/s ²
Z (vertical)	± 20 in	± 0.51 m	± 50 in/s	± 1.27 m/s	± 2.0 g	± 19.61 m/s ²
Roll (about X)	± 20 °		± 70 °/s		± 1146 °/s ²	
Pitch (about Y)	± 20 °		± 70 °/s		± 1146 °/s ²	
Yaw (about Z)	± 20 °		± 90 °/s		± 1146 °/s ²	

Table 5- 1 *RMS Performance Capability*

The following figures provide examples of the current system performance of the simulator.

Figure 5-3 is a plot of the transfer function between the Z-axis acceleration command and feedback showing the vibration capacity of the system.

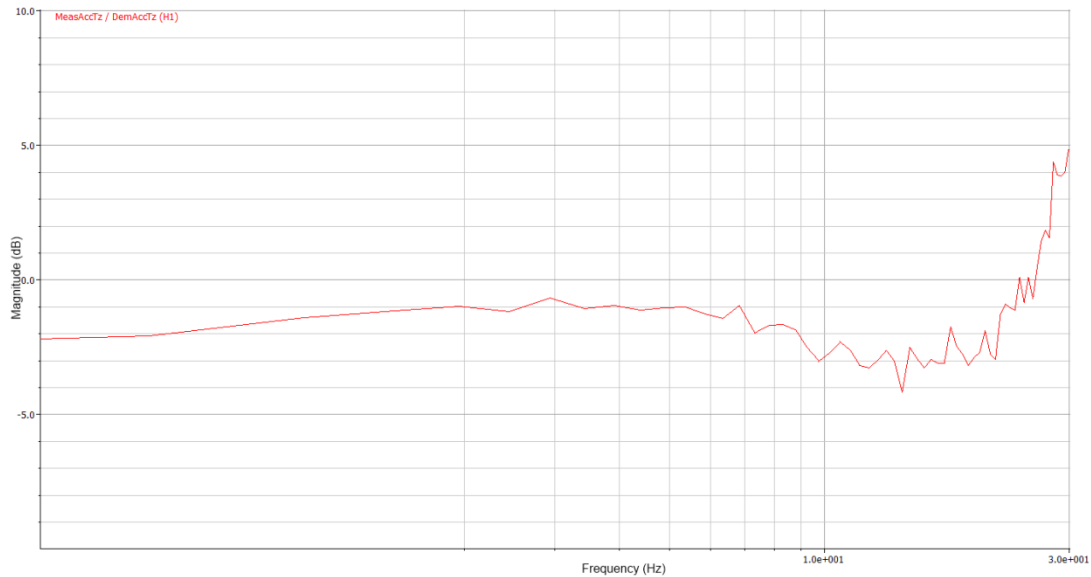


Figure 5-3 *Closed Loop, Z-Axis Acceleration Frequency Response Plot*

Figure 5-4 shows a Z-axis time history of the simulator command vs. feedback while playing a drivefile. The data represents the heave of a simulated military vehicle traversing a rough cross-country test course and has been used in many seat comfort tests in the laboratory.

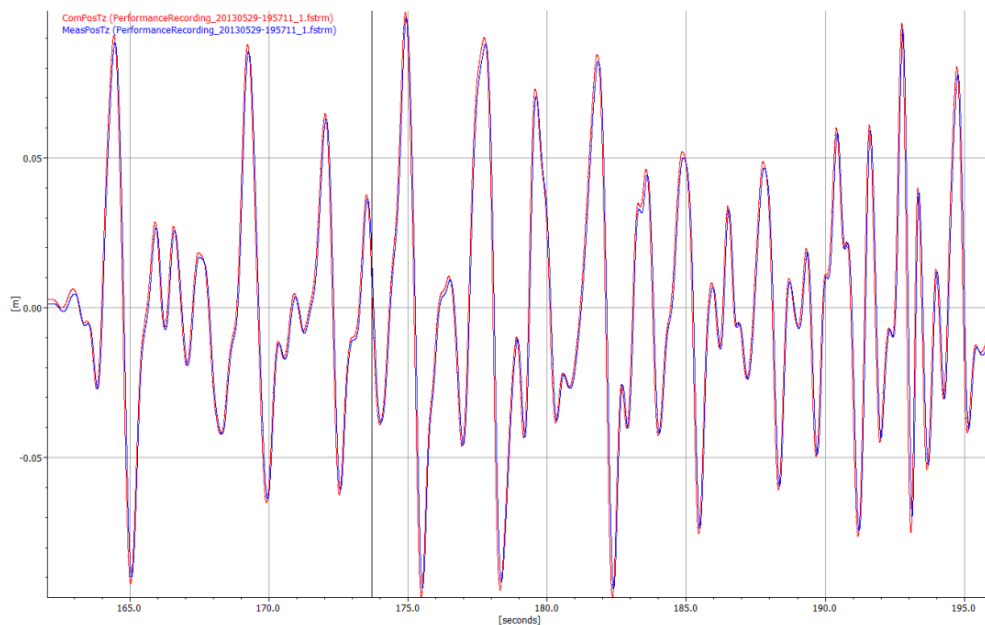


Figure 5-4 *Z-axis position command vs. feedback during playback of a drive file*

5.2.1 MAXIMUM SYSTEM ACCELERATION/DECELERATION

Maximum acceleration/deceleration tests were originally conducted at the initial manufacturer's facility in the mid-1990s. These tests were conducted in such a manner as to command the simulator at full velocity and acceleration in a given direction into the actuator cushions (depending on the direction, some actuators will become fully extended/retracted before others) with all electronic and software safety features disabled. Because these tests cannot be recreated today without risking damage to the simulator, the original test data presented in the MTS Technical Report, entitled "Ride Motion Simulator Safety Assessment Report" [2], remains the best account of the maximum acceleration/deceleration capacity of the simulator and is re-presented below.

From Section 5.2.1, MAXIMUM SYSTEM ACCELERATION AND DECELERATION, page 10 of the 1998 MTS report [2]:

"A number of tests were performed on the RMS to experimentally verify the performance as well as document the maximum acceleration and deceleration capability for a nominally configured payload. These tests were conducted with all electronic and software safety features disabled. The recorded data is presented in the table below. Due to the number of degrees of freedom and high cross-coupling inherent with the hexapod, along with the flexibility allowed for both cab payload and controller, it cannot be stated that these maximums are absolute. It can be stated that the data presented below is a best account of the maximum acceleration and deceleration capacity of the RMS for the conditions of this test."

Motion	Acceleration	Deceleration
<i>Along + Z axis into retract cushions</i>	<i>+ 10 g</i>	<i>- 10 g</i>
<i>Along - Z axis into retract cushions</i>	<i>- 8 g</i>	<i>+ 4 g</i>
<i>Along +X axis into actuator 1 & 6 cushions</i>	<i>+ 3 g</i>	<i>- 4 g</i>
<i>Along +X axis into actuator 2 & 5 cushions</i>	<i>+ 3 g</i>	<i>- 4 g</i>
<i>About +Y axis (pitching):</i> <i>actuator 1, 2, 5 & 6 into extend cushions</i> <i>actuator 3 & 4 into retract cushions</i>	<i>+2300 °/s²</i>	<i>- 5700 °/s²</i>
<i>Actuator 5 open-loop into retract cushion,</i> <i>all other actuators commanded to hold</i>	<i>max. translation:</i> <i>X = -3 g</i> <i>Max. rotation:</i> <i>roll = 1700 °/s²</i>	<i>max. translation:</i> <i>Z = - 4 g</i> <i>Max. rotation:</i> <i>roll = 2300 °/s²</i>

“An example of the test data from which the above table was generated is shown in Figure 5-6. For this experiment, the RMS was positioned at 10 inches above the home position for the start of the test. It was then given a position command of maximum acceleration to full velocity in the positive Z direction (downward) and along the vertical Z axis until all motion was fully arrested by the six actuator cushions. This data describes a worst case scenario because all six actuators maintain a driving force through the cushion, and all actuators enter their cushions almost simultaneously. The operating pressure for Figure 5-6 was 1,200 psi. However, during integration and tuning on site at TARDEC, the HPS pressure was adjusted to 600 psi. This was done to increase the safety while still meeting all system performance specifications. Therefore, the minimum and maximum acceleration and deceleration curve results in less severe motion.”

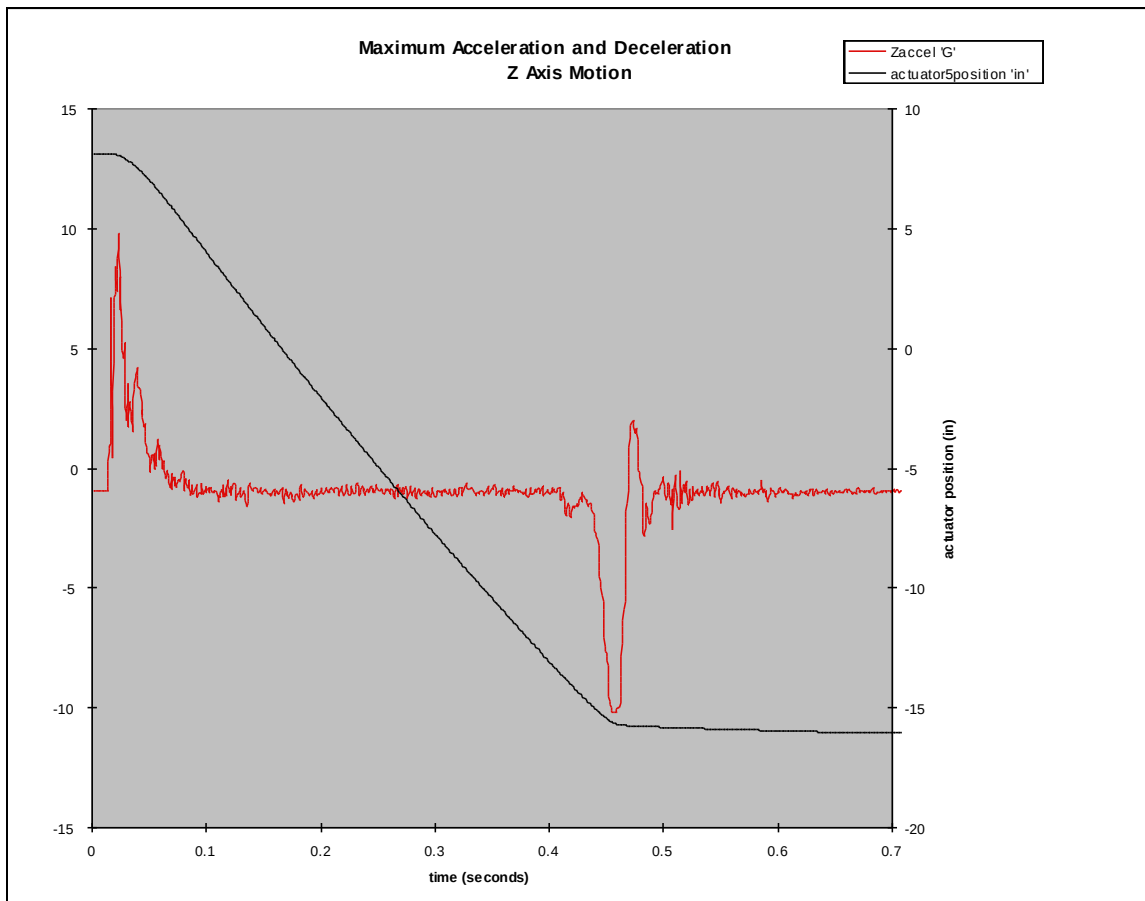


Figure 5-6. Maximum Acceleration and Deceleration - Z Axis Motion

5.3 RMS HAZARD EVALUATION

The analysis results presented on the following pages address the hazard potential to the Ride Motion Simulator should there be a failure in any of the RMS subsystems.

The hazard assessment is divided into two parts as follows:

- A general safety analysis for each RMS subsystem (Section 5.4)

- An analysis of each possible hazard, failure probability and backup system presented in table format (Section 5.5)

5.4 SAFETY ANALYSIS OF EACH SUBSYSTEM

This section provides a safety analysis of each of the following RMS subsystems:

- Hexapod (Subsection 5.4.1)
- Hydraulic Supply and Distribution (Subsection 5.4.2)
- Electronic Controls (Subsection 5.4.3)
- Controller Software (Subsection 5.4.3.2)

Each subsection provides a description of the subsystem, a structural integrity overview (if applicable), and an analysis of subsystem failures that may occur. It should be again noted that for this effort, only the Electronic Controls and Controller software have been modified therefore the sections on the Hexapod (Section 5.4.1) and Hydraulic Supply and Distribution (Section 5.4.2) remain valid and are taken directly from the 1998 MTS Report [2].

5.4.1 HEXAPOD SAFETY ANALYSIS

5.4.1.1 HEXAPOD DESCRIPTION

The hexapod is composed of the following mechanical components:

- *hydraulic actuators and swivels*
- *actuator drain sump pump*
- *platform*
- *isolation mass*

Each of these components is described in detail as follows.

Hydraulic Actuators and Swivels

The six hydraulic actuators are the active links, or legs, supporting the motion platform. The actuators are connected to the system at each end with a swivel. The base swivel attaches the fixed bottom end of the actuator to the isolation mass. The table swivel attaches the moving top end of the actuator to the motion platform. The swivels allow the actuator to rotate about the base and table without imposing constraint to motion. The actuator is composed of a piston/cylinder of equal acting area and a control manifold. The piston/cylinder incorporates hydrostatic bearings for low friction performance and hydraulic cushions to limit deceleration at the limits of stroke. The actuator control manifolds house safety and control devices for regulating pressure in the cylinder. The principle functions designed into actuator control manifolds are summarized below:

- *three-stage servo valves provide regulation of hydraulic flow to the cylinder during normal operation*
- *blocking valves isolate the cylinder from the servovalve and main oil supply when electrical power is removed from the enable/abort solenoid valve*
- *pressure relief valves limit the maximum load pressure (delta-pressure) which can be applied to the actuator piston*
- *pairs of pressure relief valves are employed for redundancy*
- *pressure dump valves provide an escape path for cylinder pressure and an entrance path for retract accumulator oil; the dump valves operate in parallel with the blocking valves, they open when electrical power is removed from the enable/abort solenoid valve*
- *the settling orifice restricts the flow of oil out of the cylinder limiting platform velocity when the table moves to the park position after E-Stop*

Safety Features

- *a separate pilot supply for the three-stage servovalve and safety valves increases system predictability and safety during aggressive E-Stop shutdown events*
- *pilot controlled three-stage servovalves provide the second redundant means of isolating the main source of hydraulic power from the actuator*
- *solenoid controlled blocking valves provide the third redundant means of isolating the main source of hydraulic power from the actuator*
- *pressure relief valves limit maximum acceleration of the motion platform*
- *solenoid controlled pressure dump valves further attenuate platform acceleration after invoking an E-Stop*
- *actuator hydraulic cushions limit platform deceleration at the limits of stroke*
- *the abort/retract accumulator, pressure dump valve, and settling orifice function together to smoothly return the motion platform to the parked position after E-Stop or after hydraulic pressure is removed and the motion platform is not in the parked position*
- *pressure transducers allow software limits to be applied to the load pressure (delta-pressure) generated by each actuator and thus provide a redundant means of limiting maximum acceleration of the motion platform*

Actuator Drain Sump Pump

The actuator drain sump pump provides a near zero back pressure drain system for the RMS actuators. Drain flow from the six actuators is directed to the sump reservoir located below floor level and directly below the center of the RMS. Float level switches detect oil level inside the reservoir and a

motor/hydraulic pump unit built into the reservoir pumps oil back to the hydraulic service manifolds (HSM) where it joins return flow back to the hydraulic power unit (HPU).

Safety Features

- a flood level switch detects reservoir oil level above the normal high level sensor and is provided as an input to the controller; software limit configuration determines simulator response to a reservoir flood level condition*

Platform

The triangular shaped platform is the moving structure to which actuator swivels and simulator cab are attached. The table is of all aluminum riveted construction in order to minimize mass and maximize stiffness and fatigue resistance.

Safety Features

- accelerometers attached to the platform allow software limits to be applied to each of the six degrees of world acceleration and thus provide further redundancy for detecting and limiting maximum acceleration of the motion platform*

Isolation Mass

The isolation mass, to which the base of the RMS attaches serves to minimize the amount of vibration disturbance transmitted to the surrounding laboratory. The total weight of the isolation mass is approximately 230,000 lb. It is constructed of steel reinforced concrete and rests on compacted soil. Anchor plates and tie rods built into the structure provide the mechanical interface for the RMS actuator base swivels at the top surface of the isolation mass.

5.4.1.2 HEXAPOD STRUCTURAL INTEGRITY

The major load carrying elements of the RMS motion platform are the actuators, swivels, platform, and isolation mass. To mitigate risk of injury or damage to the simulator, the RMS employs three engineering approaches in the design of these structural elements:

- The first approach is to design structural elements such that stress level at maximum loading condition is not greater than 25% of the material ultimate strength. It is important to recognize that the maximum load for a given structural element is unique. It is a function of local sub-system structure and simulator attitude and acceleration.*
- The second approach is to provide redundant load paths whenever possible, each of which is capable of handling the maximum loading condition. The riveted aluminum table is an excellent example of a structure which employs redundant load paths. Each joint of the table is composed of at least two structural elements which are connected by numerous rivets. In many cases, the table could easily survive maximum loading conditions even if 50% of the rivets were removed from the joint.*
- The third approach employed is to neglect both mechanical and software acceleration limiting safety functions when computing maximum loading conditions for a given structural element. For example,*

the actuator pressure relief valves will limit the maximum vertical acceleration, but if the pressure relief valves are removed, the simulator is capable of accelerating at significantly higher rates.

Nevertheless, the RMS contains structural elements which in the event of failure could result in injury. The following table summarizes these critical, non-redundant load paths, elements of the structure and describes the design approach employed to mitigate the risk of failure.

Subsystem	Load Path Element	Risk Mitigating Design Features
actuator	piston rod	• fatigue resistant base material • design safety factor >> 4
swivel	casting pivot pins	<i>a prototype of the swivel design was built and the following design verification tests were performed prior to construction of the swivels installed on the RMS:</i> • 10M cycle durability test, normal operating loads • 10K cycle durability test, maximum loads • fatigue resistant base material • design safety factor >> 4 • complete X-ray inspection of every casting (ref. MIL STD 2175, Grade B, Class 1) • fatigue resistant base material • design safety factor >> 4 • redundant attachment fasteners
platform	Seat attach plate	• high strength aluminum base material • monolithic construction • design safety factor >> 4 • near optimal attachment joint configuration
isolation mass	base swivel mount	• design safety factor >> 4

5.4.1.3 HYDRAULIC FAILURES RELATING TO THE HEXAPOD

Hose and Fitting Failure

The greatest hazard related to hydraulic power is the potential for a hose or fitting failure near the cab. The loss of control due to even a large hose failure is only a minor hazard. The major hazard is with the potential for discharging a large amount of hydraulic oil vapor into the laboratory environment. Also of concern is the possibility of imparting a dense cloud of high velocity oil vapor in the direction of the test subject or a nearby observer.

To mitigate the risk of hydraulic hose failure, RMS supply pressure hoses are rated for 3000 psi working pressure. Since the burst pressure of these hoses is 12,000 psi, a design safety factor of four, based on ultimate, is inherent in the hose working pressure rating. Since the RMS system pressure is 600 psi, this

increases the inherent design safety factor of hoses by 5 times, raising the overall safety factor of RMS pressure hoses to 20. A parallel argument can be made regarding hydraulic fittings used on the RMS.

Subsystem Failure

Hydraulic pressure related failures are also a concern with the RMS HSM, actuator, and accumulator subsystems. Experience shows that catastrophic failure at the subsystem level is highly unlikely. The more likely scenario is a confined single component failure which results in loss of system performance and/or a quantity of oil being discharged into the environment. An example of such a failure would be a blown actuator seal or a crack developing in a manifold. In both of these cases, the resulting oil leak would become apparent either during simulator operation or upon pre-operating inspection.

To mitigate the risk of subsystem hydraulic failure, additional safety factors were engineered into components and proof pressure testing was conducted for each sub-assembly. For example, all accumulators installed on the RMS are fatigue rated for 3000 psi working pressure while their burst pressure is rated at 12,000 psi. Since they normally operate at 600 psi maximum system pressure, the result is an overall design safety factor of 20 based on ultimate pressure.

Upon completion of assembly and hydraulic tests, all hydraulic subassemblies of the RMS were subjected to a proof pressure test of 1.5 times the system pressure. This pressure was applied and held for five minutes for all internal circuits and vessels of each subassembly which operate at system pressure.

It is important to remember that after a hydraulic failure has occurred and all motion has stopped, the significant remaining hazard is the possibility of injury related to slipping on an oily surface.

5.4.1.4 ELECTRICAL FAILURES RELATING TO THE HEXAPOD

If the sump pump unit fails to pump oil out of the reservoir, a flood level switch which detects reservoir oil level above the normal high level sensor is provided as an input to the controller. A software limit can be programmed to notify the operator and/or shutdown the system.

5.4.2 HYDRAULIC SUPPLY AND DISTRIBUTION SAFETY ANALYSIS

5.4.2.1 HYDRAULIC SUBSYSTEM DESCRIPTION

The hydraulic supply and distribution subsystem is composed of the following components:

- hydraulic power unit (HPU)
- hydraulic service manifold (HSM)
- hydraulic distribution manifolds

Each of these components is described in detail below. To aid in understanding overall system and subsystem functionality, refer to MTS Hydraulic Schematic - Ride Motion Simulator (MTS part number 527212-01).

Hydraulic Power Unit

The hydraulic power unit (HPU) is the source of hydraulic power to the RMS actuators. The HPU is capable of delivering up to 200 gpm at a pressure of 1200 psi. The HPU is located in a separate room from the RMS and supplies hydraulic power to the RMS via pressure, return and drain piping. The piping is sized to limit the pressure drop between the HPU and RMS to an acceptable level. The RMS controller monitors HPS status and controls the operating mode of the HPS. Hydraulic Power On and Off are the principal operating modes and are controlled by RMS electronics and software.

Safety Features

- All high pressure components are designed for 3000 psi of continuous pressure with a minimum safety factor of 4 (12,000 psi burst) and the pumps are rated for 5000 psi. An maximum operating pressure of 1200 psi allows for a safety factor of at least 10.
- An over-temperature switch and a low-level switch protect the system from abnormal operating conditions. Shutdown of the HPU is delayed 2 seconds to give advanced warning to remote control devices.
- The main pressure piping is rated to 5000 psi for continuous pressure with a minimum 4:1 safety factor (20,000 psi burst). Operation of the system at 1200 psi or below allows for a safety factor of approximately 8.

Hydraulic Service Manifold

The hydraulic service manifold (HSM) is located in a trench next to the RMS. It provides for local control of the main hydraulic power supply to the RMS while also providing filtration features. The HSM is also the location where hydraulic power from the HPU is divided into pilot pressure and main pressure sources for the RMS. Pilot pressure provides hydraulic power to actuator safety functions and pilot servovalves and cannot be interrupted by the HSM controls. Pilot pressure is always ON whenever the HPU is ON. The main source of hydraulic pressure to the RMS which enables motion is controlled at the HSM and there are three operational states: OFF, LOW, and HIGH pressure. In the HSM OFF state, only pilot pressure is supplied to the RMS. In the HSM LOW state, the main source of hydraulic pressure to the RMS is regulated to 200 psi. In the HSM HIGH state, the main source of hydraulic pressure to the RMS is regulated to 600 psi. The HSM is connected to the HPU and hydraulic distribution manifolds via hydraulic piping and hose and to the RMS controller via electrical control cables. Note, the HSM only enables the system main hydraulic supply to reach the actuator control manifolds. Platform motion is not possible until safety features built into actuator control manifolds are disengaged.

Safety Features

- the HSM inherently increases system safety since it provides a means of isolating the main source of hydraulic power from the actuator
- a separate pilot supply increases servovalve stability and predictability during system startup and shutdown

- *a separate pilot supply ensures safety functions can be engaged before main pressure is turned on*
- *the ability to operate the system at LOW HSM pressure setting (200 psi) with a low maximum velocity*
- *operating the simulator at LOW HSM pressure setting (200 psi) greatly reduces the maximum platform velocity making it possible to more safely test and evaluate new simulator features and configurations*
- *HSM filtration increases system safety since it protects hydraulic control elements from damaging particles*
- *when the HSM is switched to LOW or OFF the HSM dumps downstream pressure including pressure stored in the main pressure accumulators*
- *an hydraulic pressure switch installed on the HSM and set at 1400 psi will detect if the supply pressure has been increased; since increased supply pressure will increase the simulator acceleration and velocity capability, controller software limits are configured to prohibit simulator operation if this switch is triggered*

Hydraulic Distribution Manifolds

Three hydraulic distribution manifolds located directly below the RMS distribute hydraulic power to the six hexapod actuators. The principle feature of the distribution system is storage of hydraulic energy through the use of accumulators. Each distribution manifold incorporates four main supply pressure accumulators, two main return pressure accumulators, one pilot pressure accumulator, and one abort/retract pressure accumulator. With the exception of the abort/retract function, all accumulators act inline with their respective sources to smooth out pressure peaks or valleys resulting from varying flow demand.

Safety Features

- *The abort/retract accumulator and associated controls maintain an isolated volume of pressurized oil which will gently move the simulator into the park position immediately following an E-stop. The function is entirely passive, no electronics or control signals are required other than to initiate the loss of pressure at the main supply pressure via E-stop, HSM or HPU shutdown. The abort/retract accumulators will fully discharge through the actuator control manifolds regardless of initial actuator position.*
- *Pilot pressure supply to the pilot pressure accumulator is checked upstream at the HSM outlet. This design provides the actuator pilot stage servovalves and safety valves with a limited supply of oil in the event the HSM or HPU output pressure is lost.*

5.4.2.2 HYDRAULIC FAILURES

Hydraulic failures include hydraulic hose failure, loss of hydraulic power, an increase in hydraulic pressure, and hydraulic oil problems.

To mitigate the risk of hydraulic hose failure, RMS supply pressure hoses are rated for 3000 psi working pressure. Since the burst pressure of these hoses is 12,000 psi, a design safety factor of four, based on ultimate, is inherent in the hose working pressure rating. Since the maximum system pressure of the RMS is 1200 psi, this increases the inherent design safety factor of hoses by 2.5 times, raising the overall safety factor of RMS pressure hoses to 10. A parallel argument can be made regarding hydraulic fittings used on the RMS.

The RMS controller monitors HPS status and controls the operating mode of the HPS. The controller will shut down the system if abnormal hydraulic conditions occur.

- Unexpected loss of hydraulic power will cause the controller to shutdown the system.*
- An over-temperature switch and a low-level switch protect the system from abnormal operating conditions. These signals feedback to software limit detectors.*
- A hydraulic pressure switch installed on the HSM and set at 1400 psi will detect if the supply pressure has been increased; since increased supply pressure will increase the simulator acceleration and velocity capability, controller software limits are configured to prohibit simulator operation if this switch is triggered.*
- Pilot pressure supply to the pilot pressure accumulator is checked upstream at the HSM outlet. This design provides the actuator pilot stage servo valves and safety valves with a limited supply of oil in the event the HSM or HPU output pressure is lost.*

5.4.3 ELECTRONIC CONTROLS AND SAFETY ANALYSIS

The scope of this current upgrade covers the simulator control system and electronic controls. The following sections detail the composition and the safety analysis of that upgrade. While this report is being written by TARDEC personnel, much of the information in the sections below was provided by Moog with regards to their controller.

5.4.3.1 ELECTRONIC CONTROL DESCRIPTION

The Moog Test Controller is made up of many sub-systems that work in conjunction to move the RMS in a safe and controlled manner in order to replicate the motion of military ground vehicles traversing a wide range of terrains. The simulator controller not only controls the servo-hydraulic valves that, in turn, control how the actuators move but is constantly monitoring critical safety parameters and the health of all of its subsystems in order to ensure that the simulator does not produce any motions that would be unsafe. The Moog Test Controller, which is shown in block diagram form in Figure 5- 5, is made up of the following subsystems which are detailed in the subsequent paragraphs below:

- Real-Time Computer
- PILZ Safety PLC
- Servo Control Unit Chassis
- Analog I/O Chassis
- SeTAC ISO-2631 monitoring device

- Operator Computer
- Simulation Host Interface

5.4.3.1.1 *Real-Time Computer*

The Real-time computer is a standard Industrial PC computer running a real-time Linux operating system. CueingMiddleware is the name for the software application running on the real-time pc for simulator control. The software is responsible for:

- Servo valve control loop.
- Safeguarding of the system
- Transform 6-DOF platform commands to actuator commands.
- Manage system states
- Communication with the Simulation and Operator computers
- Communication with the I/O system
- Communication with the PILZ Safety system

If the software or real-time computer fails, the PILZ safety system will perform an immediate shutdown of the motion platform. A full description of the system's response to faults/failures can be found in section 5.4.3.5.

Describe below are many features that the CueingMiddleware has to further protect against un-intended motions being introduced to the simulator occupant.

PVA Limiter

The controller has a software feature called the PVA Limiter. This algorithm ensures safety in a human rated system by attenuating the position, velocity and acceleration commands of the simulator to values which are within a safe range given the current velocity, acceleration and position within the movement envelope. This is done both at the platform and actuator level.

The limiting concept of the PVA limiter is based on limiting (or clipping) the acceleration signal. The limited acceleration signal is then integrated twice to get matching velocity and position. Even if the velocity or position exceed the maximum value, first the acceleration is limited then the accompanying velocity and position are computed. In this way, a synchronized or matching PVA signal is ensured.

The outcome of the PVA limiter is to make sure that external commands smoothly and safely limit the motion of the system to ensure the human occupants never reach the limits of the motion envelope with any significant velocity.

Onset Limiter

An onset limiter is used to provide a ramp transition if the instantaneous rate of change of an input signal is above a pre-set value. If the onset (dy/dt) is greater than a specified value, the commanded value is attenuated to a value that provides a safe acceleration level.

Position Loop Filter

The goal of the position filter is to prevent high accelerations. Therefore the position signal is low-pass filtered.

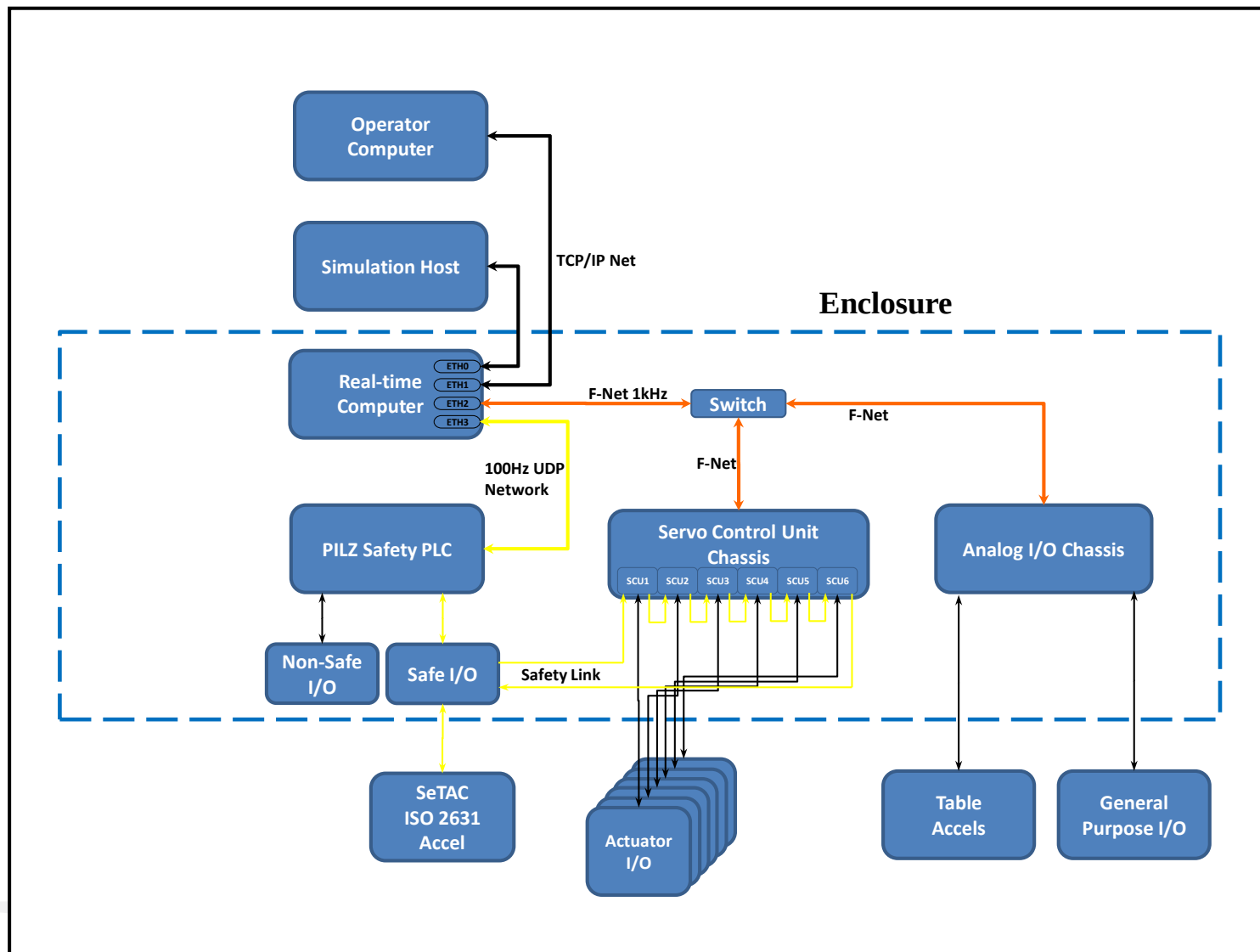


Figure 5- 5 Moog Test Controller Block Diagram

Acceleration Loop Filter

The goal of the acceleration loop filter is to prevent signals that would lead to positions beyond the position envelope. Low frequency accelerations require a long stroke. Since the stroke of a simulator is limited, the acceleration signals are high-pass filtered.

Velocity Loop Filter

The goal of the velocity signal is to prevent out of stroke signals and high accelerations. Therefore a band-pass filter is used.

5.4.3.1.2 PILZ Safety PLC

The PILZ Safety Programmable Logic Controller (PLC) is a specially designed COTS PLC to enhance the security and safety of the motion control system. The PILZ system meets the requirements of IEC/EN 61508 [3] up to SIL3 and EN 13849-1 [4] up to Category 4.

The PILZ PSS4000 Safety PLC consists of a main module which is expandable with a wide range of IO modules for standard as well as 'safe' operation. The safe operation of the PILZ PSS4000 is completely independent of the motion controller. To make optimal use of the PILZ PSS4000 functions, there is a standard Ethernet based interface between the motion controller and PILZ PSS4000. This allows the motion controller to:

- Request hydraulic pressure, which is controlled and monitored by the PILZ PSS4000
- Request hydraulic temperature which is monitored by the PILZ PSS4000
- View values of PILZ PSS4000 IO and its modules
- Receive error events when detected by the PILZ

The Safety PLC's power module integrated into the system monitors system functions and provides the following diagnostic data:

- Start-up error
- Configuration error
- FS Communication error
- Bus termination error
- Over Temperature error
- Test Pulse Error
- Input error

5.4.3.1.2.1 Use of Redundant Wiring with Safety PLC

To take advantage of the inherent safety features of the certified Safety PLC, additional control and wiring support the 'safe' digital I/O feature. The redundant wiring and monitoring of the dual circuit insures the proper operation of all safety circuits if needed.

Redundant wiring is used for all Emergency Stop (ESTOP) 'safe' circuits. Specifically, there are multiple independent contacts on each Emergency Stop Button and all switch contacts are 'failsafed'. Therefore, the contacts are normally closed and are opened when the ESTOP button is pressed.

The redundant wiring is continually tested by the PILZ Safety PLC to insure each circuit is in proper working order. There are 2 test pulse outputs that use different test pulses to differentiate one circuit from

the other. Any failure of a safety circuit either from normal activation of the ESTOP circuit or a failure detected by the Safety PLC Monitoring function will cause an emergency shutdown to occur.

5.4.3.1.3 *Servo Control Unit and Analog I/O Chassis*

The Servo Control Unit and Analog I/O chassis are both a standard 19" rack chassis that contains a PC architecture processor module running a real-time operating system and all required interface modules for either Servo Control or Analog I/O. The Servo Control Unit Chassis contains the SCU modules for servo control and the Analog I/O Chassis contains SAI modules for interfacing to the analog I/O (Accelerometers and General purpose Analog I/O). Both chassis communicate with the Real-time computer via Ethernet running the F-Net protocol.

The SMC rack could fail due to loss of electrical power, electronic module failure or a communication link failure. The reaction to any of the above failures is for the system will shut down immediately as it does with an ESTOP shutdown.

5.4.3.1.3.1 *SeTAC ISO-2631 Monitoring Device*

The Sequoia Tri-axial Accelerometer Computer (SeTAC) ISO-2631 Monitoring Device is one of two primary safety features that control and monitor human exposure to vibration. This device consists of two redundant, independent systems which continuously supervise accelerations of the platform when the simulator is in the human-rated mode.



Figure 5- 6 *Sequoia Tri-axial Accelerometer Computer (SeTAC)*

The goal of the tri-axial accelerometers is to ensure that the simulation table will be stopped when the movements of the platform overrun the limits depicted in the ISO 2631-1 [5] and ISO 13090-1 [6] norms. According to the guidelines given in these ISO norms, the 1 second-RMS value of the acceleration will be safeguarded through the tri-axial accelerometer computer connected to the PILZ Safety PLC's 'safe' circuit and the safety shutdown relay will be activated if vibrations beyond the specification are measured. The independent monitor calculates the average acceleration in real time and compares the result to the ISO 2631 standard and will stop the test, via the normal safety PLC shut down mechanism in the event that a 1-second RMS acceleration (lat, long or vertical) above 1G (acceleration due to gravity) or instantaneous acceleration above 2Gs absolute is encountered.

This entire safety concept has been developed in order to be compliant with the ISO norms 2631-1 and ISO 13090-1 relative to the exposure of human beings to vibration and to be compliant with the CE safety machinery directives. This safety concept has its root in the 25 years of experience of Moog in simulators.

5.4.3.1.4 Operator Computer

The Operator Computer is a standard office grade PC computer and is used by the system operator to Control the system. The office computer is connected to the Real-Time Computer via Ethernet.

The Operator Computer has 3 software packages installed to facilitate the control of the Motion Control system. They are:

- Moog Replication Software
- Moog Explorer Software
- RTI Custom GUI software

The software packages provide the ability to start the system, control the system activities, display current data and status and shut down the system. The software can run simultaneously and the system can be started and shut down from any of the three software packages. The primary function of each the three software packages are:

- The RTI Custom GUI software is considered the ‘Basic’ Operator interface package and Moog Explorer is used for the more advanced operator.
- The Moog Explorer software is intended primarily for maintenance and troubleshooting use and therefore requires an experienced operator for safe operation.
- Moog Replication software is an advanced software package that provides features for drive file development and playback as well as test sequence development and playback.

In general, the motion control system is a slave to external commands. This implies that the motion system is always waiting for the next command from the GUI. Therefore, if a higher level computer system stops sending information or if the PC or the communication link fails, the motion system will wait at its current state for the next command.

For example, if the current operation is ‘Sequence playback’ from Moog replication, the controller will continue playing out the active sequence until completion or the point where additional information is needed from the Replication software system.

This operation applies to Moog Replication, Moog Explorer and any GUI connected through the Moog SDK.

The Operator PC is NOT a part of any active safety system.

5.4.3.1.4.1 Evaluate Human Exposure of Iterated Target Signal

The Moog Replication software provides the capability to evaluate whether an iterated target signal is suitable for human exposure, as defined in the ISO 2631-1 and 2631-2 standards. This is the second of two primary safety features that control and monitor human exposure to vibration. If the target file meets standards it is marked as OK to use in a human rated scenario. Once the files have been validated, the system preferences, within Replication, can be set to only allow 2631 validated files to be played out to the simulator.

5.4.3.1.5 *Simulation Host Computer*

The Simulation Host Computer is responsible for sending a continuous stream of commands to the motion controller that provides movement synchronized with a simulation scenario controlled by the same Host Computer. The Simulation computer is connected to the Real-Time Computer via Ethernet.

The stream of data contains a watchdog value that is monitored in both directions. If the PC fails or if the Ethernet communication link fails, the watchdog mechanism built into the communication scheme will cause 'HostCommunication Lost' to be triggered and the system will settle to a neutral position.

5.4.3.2 **CONTROLLER SOFTWARE**

The Real-time Motion Control software, referred to as the Cueing Middleware, contains the control loop for the Hexapod system. The primary system control loop is at the actuator level and is fundamentally a position control loop. There is a control loop for each actuator and the primary real-time monitoring is performed on the difference between the position command and the actual position.

The system can execute in Position Limiter mode or PVA Limiter mode. The primary difference is PVA mode will actively limit Position, Velocity and Acceleration based upon an algorithm that 'clamps' the demanded acceleration, velocity and position to be within safe limits. The limits are system properties and are adjustable through the Moog Explorer maintenance software interface.

Since the fundamental control loop is position control, the shutdown limits are based upon position error. There are two primary safeguarding limits that will cause an immediate shutdown.

1. Actuator Position errors (Guard_MaxPosError Per Actuator)
2. PVA Errors (MaxBrakeAcc Error and Pva_MaxPos Error)

If the controller cannot keep up with the commanded signals the above errors will be encountered.

The control loop exhibits the following features:

- Hexapod forward and backward kinematics w/ PVA command
- Actuator control loop contains PIDF position control loop w/delta-P stabilization gain (via pseudo channel)
- Servo-valve (3-stage) control loop utilizes a standard PID control loop (integrator is used for multiple 3-stage valves)
- Dither (max 400 Hz, max 10 mA amplitude)
- Servo valve offset (max +/-10 mA)

Although the servo control loop is closed at the actuator level, a feed forward compensator at the platform, i.e. with respect to the DOF reference frame is provided for platform level control based on the payload's inertias and center-of-gravity (CG).

5.4.3.2.1 *Controller Software Safety Features*

The system safety concept has been chosen in such a way that hardware and software components check each other. The real-time controller software monitors the status of each actuator by comparing the

measured actuator response with the calculated actuator response. In addition to the actuators, the real-time controller software checks the system interlocks and auxiliary components. The safety hardware monitors the correct functioning of the servo drives.

The Safety implementation is a combination of hardware and software designed to provide human safety as a primary goal and as such, the shutdown needs to be handed by hardware or a certified safety device such as the PILZ safety PLC. The items considered to be “Safety Critical” for the Moog Test Controller are:

- E-Stop buttons
- SeTAC accelerometer monitored items
 - RMS (root-mean-square) acceleration monitor
 - Peak acceleration monitor
 - SeTAC properly functioning
- Pressure lost

There are additional items that are not considered “Safety Critical” items due to the fact that computer software is involved in the determination of the fault. These items include:

- Digital and analog Interlocks connected directly to the PILZ
- Controller limits
- Feedback limits
- Actuator command limits

All of the above items produce a configured safety behavior as described below in section 5.4.3.5.

5.4.3.3 CONTROLLER ELECTRICAL FAILURES

All of the cards and chassis within the Moog Test Controller are manufactured to their applicable standards and are utilized on other industrial projects throughout the world. Each individual chassis within the Moog Test Controller contain their own power supplies and are connected to the cabinet Uninterruptable Power Supply (UPS). This de-centralization of power supplies reduces the risk of a single point power failure.

Since all components are manufactured for use in industrial environments, the chance of individual failure is minimal. Since failures can occur, and we must control the manner in which the system reacts to all possible errors, the software and hardware is designed to continuously monitor all signals.

There are two basic methods employed to mitigate error or failures within the system. The first is the constant monitoring of all input channels. This includes comparing the incoming signal to predefined min/max absolute limits and min/max error limits (both position and acceleration). This software monitoring can initiate either a controlled shutdown of the system or an Emergency Stop (E-Stop) shutdown. The second method is a hardwired E-Stop chain which monitors the consent switches, watchdog timers, and several E-Stop buttons. The E-Stop chain will initiate a mechanical protection reaction to bleed down the actuator pressure without exerting undue forces to the occupant of the simulator.

Control console and/or control cabinet fire is a possibility; however it is minimized by using only industrial rated devices operating within their rated capacity. Further, the installation of the control console and cabinet equipment is carried out in accordance with best practice. The system's control console and controller cabinet are located in an environmentally controlled room. This room has both fire monitoring, alarm and suppression equipment. In addition, the control cabinet is equipped with both smoke and heat detection devices, both of which can initiate an Emergency Stop. In the event a fire should occur in the pit area, manually operated fire extinguishers rated for Class A and Class B & C should be available in the immediate area.

5.4.3.4 TRANSDUCER FAILURES

All electrical transducers located in the pit are of industrial quality and benefit from the regulations governing the safety of such equipment. The equipment functions normally even when wet with oil. The low operating temperature of the working fluid and its low volatility lessen the fire hazard.

If a transducer fails, the Moog Test Controller will react to a position velocity or acceleration software limit. The controller will then proceed with an E-Stop procedure. With regular maintenance, calibration, safety startups and dynamic pretests the likelihood of a transducer fault is minimal.

5.4.3.5 SYSTEM FAILURE RESPONSE

All possible failures that can occur during system operation are categorized as either Class 1 or Class 2 failures. Depending on the class of the failure, the failure results into a specific system behavior. In the following table the system behavior and response to Class 1 and Class 2 failures are listed.

The safety behaviors are shown below.

Class 1 Fault: CONTROLLED STOP - Example (Smoke detector cabinet)

- Sequence (application) fade out
- System settles (with remaining hydraulic energy for healthy actuator)
- Pressure shutdown

Class 2 Fault: IMMEDIATE STOP - Examples (E-stop, limit exceeded)

- Pressure shutdown
- Sequence (application) fade out
- System settles (with remaining hydraulic energy (for healthy actuators))
-

As can be seen the primary difference is that the system pressure is removed immediately during an 'Immediate Stop' or Class 2 fault. In a Class 1 fault, the system exhibits a controlled shutdown with the pressure removed after the system has settled.

The following table describes the fault conditions:

	Class 1 Fault Messages	Fault Description	Fault Type
1	Crew Consent Not Removed	The “Motion Consent” button in the Crew Cab is still pressed in and activated.	Crew “Consent” Button
2	Operator Consent Not Removed	The “Motion Consent” button on the Operator Console is still pressed in and activated.	Operator Console “Consent” Button
3	Smoke Detector Alarm	The smoke detector in the controller cabinet has detected smoke	Smoke Detector in Controller
4	Heat Detector Alarm	The heat detector in the controller cabinet has detected a high temp.	Heat Detector in Controller
	Class 2 Fault Messages	Fault Description	Fault Type
1	Hydraulic EStop	The “Hydraulic Emergency Stop” on side safety rail has been activated	Safe Emergency Stop Button
2	Crew EStop	The “Crew Emergency Stop” in the crew cab has been activated	Safe Emergency Stop Button
3	Facility EStop	The “Facility Emergency Stop” on the back wall has been activated	Safe Emergency Stop Button
4	Console EStop	The “Console Emergency Stop” on the operator console has been activated	Safe Emergency Stop Button
5	Access Platform Not Retracted	The access platform is no longer in the ‘Retracted’ position	Switch contact on Access Platform
6	Crane Not Retracted	The Crane is no longer in the ‘Retracted’ position	Switch contact on Crane support
7	SafetyPLC Heartbeat Lost	The Watchdog between MRC and the Safety PLC (PILZ) has been lost	MRC Software Detected Failure
8	Host Communication Lost	The Watchdog between MRC and the Host computer has been lost	MRC Software Detected Failure
9	NaN in Host Data	A data error was encountered in the MRC	MRC Software Detected Failure
10	Overrun Detected	A data error was encountered in the MRC	MRC Software Detected Failure
11	SMC FNet Node 1 Lost	The communication link between MRC and the SMC Rack #1 has been lost	MRC Software Detected Failure
12	SMC FNet Node 2 Lost	The communication link between MRC and the SMC Rack #2 has been lost	MRC Software Detected Failure
13	Hardware.Acu1: Position Error Too High	The difference between the commanded position and actual position for Actuator 1 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure
14	Hardware.Acu1: Scu Card Failure	The a failure in SCU #1 was detected	MRC Software Detected Failure
15	Hardware.Acu2: Position Error Too High	The difference between the commanded position and actual position for Actuator 2 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure
16	Hardware.Acu2: Scu Card Failure	The a failure in SCU #2 was detected	MRC Software Detected Failure
17	Hardware.Acu3: Position Error Too High	The difference between the commanded position and actual position for Actuator 3 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure
18	Hardware.Acu3: Scu Card Failure	The a failure in SCU #3 was detected	MRC Software Detected Failure
19	Hardware.Acu4: Position Error Too High	The difference between the commanded position and actual position for Actuator 4 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure

20	Hardware.Acu4: Scu Card Failure	The a failure in SCU #4 was detected	MRC Software Detected Failure
21	Hardware.Acu5: Position Error Too High	The difference between the commanded position and actual position for Actuator 5 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure
22	Hardware.Acu5: Scu Card Failure	The a failure in SCU #5 was detected	MRC Software Detected Failure
23	Hardware.Acu6: Position Error Too High	The difference between the commanded position and actual position for Actuator 6 is too large. (Guard_MaxPosError limit error)	MRC Software Detected Failure
24	Hardware.Acu6: Scu Card Failure	The a failure in SCU #6 was detected	MRC Software Detected Failure
25	Hydraulics: Timeout	A timer in the PILZ hydraulic sequencer has expired	MRC Software Detected Failure
26	Pos_MaxBrake error	The acceleration commanded will cause the platform to exceed the position envelope. (Pos_MaxBrakeAcc error)	MRC Software Detected Failure
27	Pva_MaxBrakeAcc Error	The acceleration commanded will cause the platform to exceed the PVA Limiter ability to stop envelope.	MRC Software Detected Failure
28	Pva_MaxPos Error	The difference from the current position to the PVA Limiter commanded position is too large.	MRC Software Detected Failure

Table 5- 2 Moog Test Controller Fault Conditions

Many of these faults were tested during the Moog Test Controller Site Acceptance Testing conducted at TARDEC in May of 2013. The results of those tests are presented below in Table 5- 3 *RMS Failure and Effect Table*.

**Ride Motion Simulator
Failure and Effect Table**

Failure/Switch	Moog ATP Section	Effect on RMS	Action Taken	Verified (initials)
<u>Emergency Stop Buttons</u>				
Emergency Stop buttons on console (Left and Right Side)	5.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset E-Stop. Reset interlock and re-start system.	VJP 5/14/2013
Emergency Stop button on I-beam	5.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset E-Stop. Reset interlock and re-start system.	VJP 5/14/2013
HPU and Simulator Emergency Stop button on railing	5.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset E-Stop. Reset interlock and re-start system.	VJP 5/14/2013
Crew Emergency Stop button	5.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset E-Stop. Reset interlock and re-start system.	VJP 5/14/2013
HPU Emergency Stop button (pump)	5.2	Simulator E-Stop initiated when pressure drops below minimum allowed value. Hydraulic pressure removed and simulator comes down to rest.	Restore proper HPU operation. Reset interlock and re-start system.	VJP 5/15/2013
<u>Safety Critical Interlocks</u>				
Access Platform Lowered	5.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Raise Access Platform. Reset interlock and re-start system.	VJP 5/14/2013
Crane moved out of park position	5.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Move crane back to park position. Reset interlock and re-start system.	VJP 5/14/2013
Sump Overflow fault	5.3	E-Stop initiated. HPU shutdown and simulator comes down to rest.	Re-establish Sump Pump operation. Reset interlock and re-start system.	VJP 5/14/2013
HPU Tank-Low Level fault	5.3	E-Stop initiated. HPU shutdown and simulator comes down to rest.	Restore HPU oil level. Reset interlock and re-start system.	VJP 5/14/2013
SeTAC fault	5.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore proper SeTAC operation. Reset interlock and re-start system.	VJP 5/14/2013

Table 5- 3 RMS Failure and Effect Table

**Ride Motion Simulator
Failure and Effect Table Continued**

Failure/Switch	Moog ATP Section	Effect on RMS	Action Taken	Verified (initials)
<u>Communication Interlocks</u>				
Loss of communication between Operator PC and Real-Time Controller (RTC)	5.5.1	No effect on the simulator.	Stop simulator. Restore communication. Reset interlock and re-start sys.	VJP 5/14/2013
Loss of communication between RTC and SMC Rack	5.5.2	Moderate simulator jerk. E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore communication. Reset interlock and re-start sys.	VJP 5/14/2013
Loss of communication between RTC and PILZ Safety PLC	5.5.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore communication. Reset interlock and re-start sys.	VJP 5/14/2013
Loss of communication between RTC and Simulation Host	5.5.4	Simulator stops at last position. Comes down to rest and turns off.	Restore communication. Reset interlock and re-start sys.	VJP 5/15/2013
<u>Actuator Controller</u>				
Act. Position Limit exceeded	5.6.1	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset interlock and re-start sys.	VJP 5/15/2013
Act. Control Error too high	5.6.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset interlock and re-start system.	VJP 5/15/2013
<u>Motion Cabinet Safety</u>				
Control Cabinet power loss	5.7.1	Moderate simulator jerk. Hydraulic pressure removed and simulator comes down to rest.	Restore cabinet power. Reset interlock and re-start system.	VJP 5/14/2013
RTC power loss	5.7.2	Simulator jerks. E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore RTC power. Reset interlock and re-start system.	VJP 5/14/2013
PILZ Safety PLC power loss	5.7.3	Moderate simulator jerk. E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore Safety PLC power. Reset interlock and re-start system.	VJP 5/15/2013

Table 5- 5 Continued RMS Failure and Effect Table

**Ride Motion Simulator
Failure and Effect Table Continued**

Failure/Switch	Moog ATP Section	Effect on RMS	Action Taken	Verified (initials)
<u>Motion Cabinet Safety Cont.</u>				
Control Cabinet Smoke Detection	5.7.4	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Resolve cabinet smoke problem. Reset interlock and re-start system.	VJP 5/15/2013
Control Cabinet Heat Detection	5.7.5	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Resolve cabinet heating problem. Reset interlock and re-start system.	VJP 5/15/2013
<u>SeTAC Operational Test</u>				
SeTAC limit exceeded during drive profile	7.1.1	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset interlock and re-start system.	VJP 5/15/2013
<u>PILZ Pressure/Temp Test</u>				
Hydraulic Pressure fault	7.1.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Restore HPU Pressure. Reset interlock and re-start system.	VJP 5/15/2013
Hydraulic Temperature fault	7.1.3	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reduce Hydraulic Oil temp. Reset interlock and re-start sys.	VJP 5/15/2013
<u>Safeguarding Limits</u>				
Translational (X, Y or Z) Axis Acceleration Limit exceeded	7.1.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset interlock and re-start system.	VJP 5/15/2013
Rotational (R, P or Yw) Axis Acceleration Limit exceeded	7.1.2	E-Stop initiated. Hydraulic pressure removed and simulator comes down to rest.	Reset interlock and re-start system.	VJP 5/15/2013

Table 5- 5 Continued RMS Failure and Effect Table

**Ride Motion Simulator
Failure and Effect Table Continued**

Failure/Switch	Moog ATP Section	Effect on RMS	Action Taken	Verified (initials)
<u>TARDEC Specific Tests</u>				
Simulate operator error on Operator PC (i.e. close controller application)		No effect on the simulator.	Push E-Stop to stop simulator. Restart application. Reset interlock and re-start system.	VJP 5/15/2013
High to low pressure change in pump room		Simulator E-Stop initiated when pressure drops below minimum allowed value. Hydraulic pressure removed and simulator comes down to rest.	Restore proper HPU operation. Reset interlock and re-start system.	VJP 5/15/2013
UPS input voltage lost (Uninterruptible Power Supply)		No effect on simulator. UPS beeps to notify a loss of line power.	Shutdown simulator. Restore UPS input power. Reset interlock and re-start system.	VJP 5/15/2013
Human Rated/Full Performance Key Switch on console turned.		Simulator E-Stop initiated. Simulator comes down to rest. Hydraulic pressure removed.	Restore performance mode. Reset interlock and re-start sys.	VJP 5/15/2013
Human Rated/Full Performance Key Switch in cab turned.		Simulator E-Stop initiated. Simulator comes down to rest. Hydraulic pressure removed.	Restore performance mode. Reset interlock and re-start sys.	VJP 5/15/2013
Test Motion Consent Switch on console (latched to unlatched)		Simulator E-Stop initiated. Simulator comes down to rest. Hydraulic pressure removed.	Restore consent. Reset interlock and re-start system.	VJP 5/15/2013
Test Motion Consent Switch in cab (latched to unlatched)		Simulator E-Stop initiated. Simulator comes down to rest. Hydraulic pressure removed.	Restore consent. Reset interlock and re-start system.	VJP 5/15/2013
Temposonics III Error		Moderate simulator jerk. E-Stop initiated. Simulator comes down to rest. Hydraulic pressure removed.	Restore proper Temposonics functionality. Reset interlock and re-start system.	VJP 5/15/2013

Table 5- 5 Continued RMS Failure and Effect Table

5.5 SYSTEM HAZARD ANALYSIS TABLE

The accompanying analysis sheets contain hazard severity levels and hazard probability levels from MIL-STD-882E [7]. These hazard levels allow system damage and personal injury to be included in the definition and reflected in the hazard assessment.

HAZARD SEVERITY LEVELS

SEVERITY CATEGORIES		
Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding \$10M.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding \$1M but less than \$10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding \$100K but less than \$1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than \$100K.

HAZARD PROBABILITY LEVELS

PROBABILITY LEVELS			
Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Will occur several times in the life of an item.	Continuously experienced.
Probable	B	Will occur several times in the life of an item.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	F	Incapable of occurrence.	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.

SYSTEM HAZARD ANALYSIS TABLE

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS
					CORRECTIVE ACTION/MINIMIZING PROVISIONS
Impact/Crushing Physical Injury	Structural failure of hexapod platform, swivels, actuators, reaction base	Possible severe damage to the RMS depending on the locations and severity of structural damage	2	E	Since a hexapod mechanism becomes unconstrained if one actuator is removed, the worst case hazard is that an actuator completely breaks away at one end and the remaining structure topples over. If such an event would occur, multiple controller limits would be violated thus triggering emergency shutdown. To mitigate this hazard, major load carrying elements of the RMS were designed with: a minimum safety factor of 4, redundant load paths whenever possible and conservative limit load specifications for each degree-of-freedom. Mandatory use of seat belts during any motion of system should be enforced. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of hazard.
	Structural failure of cab structure or components	Possible damage to the RMS, possible severe damage to the cab	2	E	Critical cab structure elements concerning human safety are the seat support and the monitor support. Failure of these elements could result in structural members impacting the test subject. To mitigate this hazard, cab structural elements were designed with: a minimum safety factor of 4, redundant load paths whenever possible, and conservative limit load specifications for each degree-of-freedom. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of hazard.
	Person entering pit area during test run	Possible physical injury to person	2	E	Access to pit area limited to experience maintenance personnel. All personnel should have proper training before entering pit area.
Electrical shock	Wear or severing of power cables to actuator drain sump pump and actuator solenoids	Electrical shock to personnel	2	E	Design is based on industry standards National Electrical Code. Actuator drain sump pump voltage (460 V) is conduit enclosed per National Electrical code. Solenoid voltage (24 Vdc) is not a hazard.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Chemical Exposure	Burst in hose or rupture in manifold resulting in large scale oil leakage	Power to the RMS will end, release of hydraulic oil into room	4	E	The exact location of the failure and the equipment wetted by the escaping oil determines the severity of the hazard. The hazard to personnel varies with the amount and velocity of oil delivered and point of impact. Burn hazard is non-existent based on the maximum oil temperature being limited to 140 °F. Immediate control of the hazard depends on system shutdown by the operator or controller limits. Using an industry standard petroleum based hydraulic fluid (refer to the MSDS for Mobil DTE25 in Appendix A). A good preventative maintenance program and periodic inspection of equipment keeps the probability of occurrence remote.
Fire and Smoke Exposure	Ignition of oil from spark or open flame	Possible severe damage depending on the extensiveness of the fire	2	E	Using an industry standard petroleum based hydraulic fluid (refer to the MSDS for Mobil DTE25 in Appendix A). It is highly unlikely that the hydraulic fluid could burn since it has a flash point of 395 °F. However, pressurized oil from a leak or spray has a greater probability of combustion if it comes into contact with a flame or spark. The main pump motor is of drip-proof construction. Banning any open flames or smoking materials from the area will reduce the chance of fire to almost zero.
Sustained Physical Acceleration	Hardware or software failure or setup error which causes control instability	high acceleration and deceleration possible over a broad band of frequency before controller invokes shutdown	3	D	Worst case scenario implies sinusoidal motion at the performance limits of the machine. Multiple feedback parameter out-of-bound conditions will be detected by controller limits thus triggering emergency shutdown. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs, head or body resonance also unpredictable. The RMS operator can stop the test by pressing one of several Emergency- stop buttons located throughout the laboratory, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.
	Actuator and DOF limits disabled	large acceleration, velocity, and displacements are possible over a broad band of frequency	3	D	If Actuator and DOF limits are disabled, controller triggered emergency shutdown will still be triggered by the SeTAC monitoring accelerometer if the system is in Human-rated mode. If the system is in Full-Performance mode, an emergency shutdown will not occur and the machine will follow the motion commands to the extent of performance limits. Worst case scenario #1 implies maximum acceleration and velocity followed by maximum deceleration at actuator extreme positions (position commands go outside of machine displacement limits). Worst case scenario #2 implies random or periodic motion imparting sustained maximum acceleration/deceleration to the test subject (position commands remain within bounds of machine displacement limits). Following a pre-test checklist will reduce both the possibility of limit detectors being disabled and the system being run in Full Performance mode while a human is aboard.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
High Physical Acceleration	Loss of controller hardware, servo-valve failure, valve driver failure, feedback transducer, cable, or conditioner failure	high acceleration possible before complete shutdown	3	D	Worst case scenario implies high velocity near displacement limits concurrent with controller loss; established kinetic energy and trajectory could result in multiple actuator cushion impact before controller shutdown can arrest motion. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs or head also unpredictable. The RMS operator can stop the test by pressing one of several Emergency- stop buttons located throughout the laboratory, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.
	Data file error	high acceleration and deceleration possible before controller invokes shutdown	3	D	Worst case scenario implies high velocity through set displacement limits; established kinetic energy and trajectory could result in multiple actuator cushion impact before controller shutdown can arrest motion. Most likely system will shutdown fast enough, but this is not guaranteed. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs or head also unpredictable. Data to be simulated should be generated from well proven analytical models. Additionally, all data should be visually inspected and a simulation executed without the test subject in the RMS. The RMS operator can stop the test by pressing one of several Emergency- stop buttons located throughout the laboratory, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.
	Loss of integrity of external input signal to RMS	Invalid signals sent to the RMS from external device	3	D	All output data is filtered using the electronic filters which would smooth over any sudden changes in signal. Invalid signals should be detected in the testing phase before the test subject has boarded the simulator.
	Incorrect electrical connections	Undesirable movement of the simulator. Loss of control.	3	D	Changing the RMS motion electrical connections is unlikely. Pre-simulation testing will reveal incorrect settings of the control modules or incorrect hookups of the input signal. Corrections will then be made. Also, a preliminary dry run each morning will greatly reduce the possibility of this type of hazard.
	Operator or occupant errors resulting in failure to stop test, perhaps placing occupant in danger	Failure to stop test	3	D	Failure of either the operator or occupant to stop a test and cause possible damage to the occupant (and equipment) is prevented by providing both people the ability to stop a test. If neither person acts to stop a test, additional safety is provided through automatic shutdown triggered by the SeTAC monitoring accelerometer which will stop a test when acceleration limits have been exceeded.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Minimal.	Failure of UPS system	Fluctuations in electrical supply power to the RMS	4	D	The UPS (Uninterruptible Power Supply) system will provide power to the entire RMS electrical system. The UPS will regulate voltage, frequency, and remove noise from the input line voltage. It will also provide power if the input line voltage is lost. The UPS guarantees a clean and continuous power supply to the RMS and associated equipment. Failure of the UPS system in itself poses no problem because unregulated line voltage will be available.
	Loss of input line voltage to RMS control electronics and hydraulic pump	Loss of electrical power to RMS control electronics and hydraulic pump	4	D	The UPS system will provide power to the entire RMS electrical system except for the hydraulics. The UPS will provide power for up to 15 minutes if the input line voltage is lost. The UPS guarantees a clean and continuous electrical power supply to the RMS. The hydraulic pump will lose power but the accumulator's discharge will smooth loss of performance at the machine. Eventually feedback parameter out-of-bounds conditions will be detected by controller limits thus triggering emergency shutdown.
	Noise on the power lines (perhaps due to electrical storm)	Input line voltage is no longer at 115 VAC	4	D	The UPS system protects all RMS control electronics from voltage surges except the hydraulic pump. Hydraulic pump motors are insensitive to short duration voltage surges although voltage spikes could result in current spikes which could trip the breakers. Loss of 3-phase power to the hydraulic pump will result in loss of pressure to the RMS, resulting in an E-stop condition.
	Loss of Hydraulic Pressure	Hydraulic power to the RMS decreases or stops	4	D	Loss of system pressure due to loss of pump power, blockage in lines, clogged hydraulic filters, burst in hose or fitting, component failure, etc. implies a decrease in flow volume and hence a rapid decrease in machine performance. The accumulator's discharge will smooth the loss of performance. Eventually feedback parameter out-of-bound conditions will be detected by controller limits thus triggering emergency shutdown. A good preventative maintenance program and periodic inspection of equipment keeps the probability of occurrence remote.
	Hydraulic Pressure Fluctuations	Varying output pressure of hydraulic pump, instead of constant	4	E	HPS pressure controls have a variation of 100-200 psi when controlling to any specific set pressure. Pressure surges and dips can also occur due to many factors: hard-line pressure drop, water hammer, oil separation, pressure control valve dynamic response to changes in required flow, etc. Short duration pressure pulses are dampened by the accumulators. Sudden sustained low pressure would indicate a large leak. Sustained high pressure would indicate a relief valve malfunction. A pressure compensated pump is designed to de-stroke in the face of increased pressure, eventually going to near zero. Pump pressure compensators are quick acting (<100 msec) to limit over and under-pressure surges. A sustained pressure surge to the actuators is only possible by simultaneous failure of the pump relief valve, compensator and pressure switch. A pressure surge does not in itself define an injury situation. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of situation.

6.0 References

- [1] V. J. Paul, A. Berger and H. J. Zywiol, "M2A2 Bradley Fighting Vehicle Traverse Drive Motor Base Line Test on TARDEC's Crew Station/Turret Motion Base Simulator Final Report," Tank Automotive Research, Development and Engineering Center, Warren, MI, 1993.
- [2] MTS Systems, "Ride Motion Simulator Safety Assessment Report," 1998.
- [3] IEC/EN61508, "Functional Safety of Electrical/Electronic/programmable Electronic Safety-related Systems -- Part 1: General Requirements," IEC/EN.
- [4] EN ISO13849-1:2006, "Safety of machinery - Safety-related parts of control systems -- Part 1: General principles for design," EN ISO, 2006.
- [5] ISO2631-1:1997, "Mechanical vibration and shock -- Evaluation of human exposure to whole-body vibration -- Part1: General Requirements," ISO, 1997.
- [6] ISO13090-1:1998, "Mechanical vibration and shock -- Guidance on safety aspects of test and experiments with people -- Part 1: Exposure to whole-body mechanical vibration and repeated shock," ISO, 1998.
- [7] U.S. Department of Defense, *MIL-STD-882E SYSTEM SAFETY*, 2012.