TEST HAZARD ANALYSIS REPORT

Date: 01/21/2016
Revision: Basic
Hazard Analysis Of: Valkyrie

Prepared By: Alan Noblitt
Digitally signed by Alan Noblitt
DN: cn=Alan Noblitt, o=Wyle - Safety, Reliability, and Maintainability, ou, email=alan.l.noblitt@nasa.gov, c=US
Date: 2016.03.31 10:29:39 -05'00'

Alan Noblitt, Signature

Organization: Wyle Laboratories

Telephone: 281-204-1570

Concurrence: N/A
TRR Chairperson

Concurrence:
Test Director/Test Article Expert

Approved By: N/A
Quality Engineering

Approved By: N/A
Facility Manger

Approved By: N/A
Test Safety Officer

Approved by: WILLIAM VERDEYEN
WILLIAM VERDEYEN
2016.03.22 10:16:31 -05'00'
Project Management

Approved By: MYRON DIFTLER
Digitally signed by MYRON DIFTLER
DN: c=US, o=U.S. Government, ou=NASA, ou=PIV, cn=MYRON DIFTLER, 0.9.2342.19200300.100.1.1=mdiftler
Date: 2016.03.31 14:50:34 -05'00'
Branch Management

Approved By: CLIFF FARMER
Digitally signed by CLIFF FARMER
DN: c=US, o=U.S. Government, ou=NASA, ou=People, cn=CLIFF FARMER, 0.9.2342.19200300.100.1.1=cfarmer
Date: 2016.03.31 15:07:47 -05'00'
Divison Management

Severity Classes:
I – Catastrophic - A condition that may cause death or permanently disabling injury, facility destruction on the ground.
II – Critical - A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware.
III – Moderate - A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware.
IV – Negligible - A condition that could cause the need for minor first-aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware more than normal wear and tear level.
Probability Codes:
A – Likely to occur
B – Probably will occur
C – May occur
D – Unlikely to occur
E – Improbable

RAC code:	Probability Estimate				
Severity Class	A	B	C	D	E
I	**1**	**1**	**2**	**3**	**4**
II	**1**	**2**	**3**	**4**	**5**
III	**2**	**3**	**4**	**5**	**6**
IV	**3**	**4**	**5**	**6**	**7**

RAC 1 Unacceptable. All operations shall cease immediately until the hazard is corrected, or until temporary controls are in place and permanent controls are in work. A safety or health professional shall stay at the scene at least until temporary controls are in place. RAC 1 hazards have the highest priority for hazard controls. Center Director is authorized to accept the risk with adequate justification in rare cases where critical tests must be done and the risk cannot be reduced.

RAC 2 Undesirable. All operations shall cease immediately until the hazard is corrected or until temporary controls are in place and permanent controls are in work. RAC 2 hazards are next in priority after RAC 1 hazards for control. Program Manager (directorate level), Organizational Director, or equivalent management is authorized to accept the risk with adequate justification.

RAC 3 Acceptable with controls. Division Chief or equivalent management is authorized to accept the risk with adequate justification.

RAC 4-7 Acceptable with controls. Branch Chief or equivalent management is authorized to accept the risk with adequate justification.

SCOPE: NASA is providing a robot shell to universities. The robot will be able to accept umbilical power and will have a software API so that the universities can develop their own software for the system. This hazard assessment assumes that there are no software-based hazard controls.

The universities will perform development work on the robot, and as a result, some of the hazards typically controlled through design or software must be controlled through operational procedures. For the risk of excessive force causing injury to the user, the user must be able to perform activities in close proximity to the system while motor power is on in order to accomplish their development tasks. We therefore instruct the users to have a second person hold and operate the emergency stop during these activities. This does not fully remove the risk of injury since the robot has the potential to move faster than the emergency stop operator can react. We therefore also instruct the users to not place themselves between the system and an immovable surface, like a wall or table, so that if the system does impact the user they will be pushed instead of crushed. With these controls in place, the potential for a catastrophic event is still present, but is considered unlikely.

It is expected that the universities will develop their own control software and safety software for the robots. These hazard reports, along with the likelihoods and controls, are written assuming that there is no safety software in the design. It is possible that the universities will be able to reduce the risk further and potentially relieve some of the operational controls by implementing safety software, but that is beyond the scope of this analysis.

This assessment only addresses hazards that affect the users or the facility. Hazards where the only effect is damage to Valkyrie are not included in this analysis.

No.	Hazard	Cause	Effect	RAC Before Controls	Controls	Verification	Disposition RAC After Controls
1	Mechanical Hazards	Sharp Edges	Personal Injury	III / B / 3	External Surfaces are free of sharp edges. Users are instructed to be cautions when working on the internal components of the Robot as there may be sharp edges, holes, or burrs present.	Inspection of the as-built hardware shows that the external surfaces of the system have no sharp edges or corners. General Operating Procedure shows that the users are instructed to use caution when accessing the internal components of the system	III / C / 4
2	Appendage Entrapment	Pinch Points	Personal Injury	II / B / 2	The users are instructed to keep appendages clear of the robot's joints while motor power is active. All fans are covered with screens or are inaccessible. All motors are inside of the system housing.	General Operating Procedure shows that the users are instructed to keep out of the robot's joints' ranges of motion while motor power is active. Inspection of the as-built system will show that the fans are covered with screens or inaccessible, and that the motors are inaccessible.	II / C / 3
3	Touch Temperature	Accessible components get hot	Personal Injury	III / C / 4	The users are made aware of potential hot spots external to the system. Note: Final temperature and cool down time is implementation-specific. Users are advised to use caution when accessing the system, don PPE, or develop their own characterization of the system.	General Operating Procedure documents the areas that are known to get hot on the external surfaces of the system. Users are instructed to avoid contact with those areas while the system is on.	III / D / 5

No.	Hazard	Cause	Effect	RAC Before Controls	Controls	Verification	Disposition RAC After Controls
4	Fire	Improper Circuit Protection	Personal Injury Hardware Damage	I / C / 2	All wiring is designed by a senior Electrical Engineer and is properly rated for its expected use. NASA will provide a power supply for use with the robot that includes overvoltage and overcurrent protection.	Design verified by senior Electrical Engineer showing that conductors are correctly rated for their expected use, per drawing design.	I / D / 3
5	Electric Shock	Improper Mating/Demating of power cables Improper Grounding Exposed Conductive Surfaces	Personal Injury	I / B / 1	All conductive surfaces accessible to the user have a low impedance path to ground. The positive terminal of the power supply is DC isolated from the chassis and the ground. The negative terminal of the power supply is DC isolated from the chassis and the ground. The power connector is a MIL-SPEC connector. Users are instructed to route the power cables in such a way that they are not in the range of motion of the system. If internal components are being accessed, it is recommended that the user remove power from the system prior to opening the system. If power needs to be applied for maintenance activities, users will avoid contact with conductive surfaces.	Grounding and isolation tests show that the conductive surfaces accessible to the user are grounded, and that the positive and negative terminals are isolated from the chassis and ground. General Operating Procedure shows that the user is instructed to route the power cable out of the range of motion of the robot. General Operating Procedure shows that the user is instructed to remove power from the system when accessing the internal components, or to avoid contact with exposed conductive surfaces.	I / D / 3

No.	Hazard	Cause	Effect	RAC Before Controls	Controls	Verification	Disposition RAC After Controls
6	Electromagnetic Interference	Emitters	Hardware damage	IV / B / 4	Known emitters are identified.	Design Information provided to the users identifies the emitters in the system.	IV / C / 5
7	Non-ionizing radiation	LASERs Radio Frequency Transmitter	Personal Injury	II / C / 3	The MultiSense SL 3D Range Sensor uses a 905nm Class I LASER. Class I LASERs are safe under all conditions of nominal use. The wireless Emergency Stop button uses several radio frequencies. These are all below levels that would create a risk to the operator under normal conditions.	MultiSense SL User Manual shows that the sensor uses a Class I LASER. E-Stop documentation shows the radio frequencies used by the device.	II / E / 5
8	Lift-related injury	Improper Lift	Personal Injury	I / C / 2	Shipping container includes features to facilitate proper lifting (handles, etc.) NASA will provide a lift plan including transportation and assembly.	Inspection of the shipping containers shows that they include handles and wheels to facilitate lifting and moving. NASA Lift Plan	I / D / 3
9	Toxic Materials	Exposure to Capacitor Electrolyte	Personal Injury	II / C / 3	Capacitors are used within their ratings and specifications and are thus unlikely to leak electrolyte.	Design verified by senior Electrical Engineer showing that capacitors are correctly rated for their expected use, per drawing design.	II / D / 4

No.	Hazard	Cause	Effect	RAC Before Controls	Controls	Verification	Disposition RAC After Controls
10	Falling Mass	Failure of Support Structure	Personal Injury Hardware Damage	I / B / 1	The users are instructed to not allow the robot to free-walk. The users will ensure that the supporting structure and cabling/harnesses can support up to 600lbm (weight of the robot plus a 2x factor of safety). Robot attachment points can support up to 600lbm.	General Operating Procedure instructs the uses to not allow free-walking during operations. General Operating Procedure instructs the user to use structure and cabling / harnesses that can support up to 600lbm. Inspection of attachment points shows that they are rated for at minimum 600lbm. Validation test of the as-built system shows that the unit can be supported by the provided attachment points.	I / D / 3
11	Excessive Force	Software Failure Hardware Failure	Personal Injury Hardware Damage	I / C / 2	All activity within the range of motion of the robot while motor power is on will be done with the Emergency Stop Button connected and independently operated. Users are instructed to not place themselves between the robot and an immovable surface within the range of motion of the robot while motor power is on.	General Operating Procedure instructs the users to have the Emergency Stop Button independently operated while activities take place within the range of motion of the robot. General Operating Procedure instructs the users to not place themselves between the robot and an immovable surface while motor power is on. Demonstration of the completed system shows that the Emergency Stop Button will shut off motor power when it is pressed.	I / D / 3

No.	Hazard	Cause	Effect	RAC Before Controls	Controls	Verification	Disposition RAC After Controls
12	Structural Failure	Improper Assembly	Personal Injury	II / A / 1	NASA will provide instructions on proper assembly of the robot.	Reference information provided to the universities which describes the assembly procedure.	II / D / 4