MRV and Robotic Systems Briefing
Introduction
MRV: Vehicle Specs

- Design speed: 64 kph (40 mph)
  - Currently computer limited to 25 kph
- Curb weight: 900 kg (2000 lb)
- Footprint: 2.15 x 1.55 m (7’ x 5’)
- By-wire without mechanical backup
Pedal-by-Wire Design

- Level
- Linear Sensor
- Spring
- Cam profile plates
- Rotation sensor (Prod Part)
- Pedal with force sensor
Wheel Modules
### DFMEA Driven - MRV Scenarios

<table>
<thead>
<tr>
<th>Failure Type (FT)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Power Bus:</td>
<td>All systems go off-line, emergency braking &amp; steering system? Driver's input ignored (HV, 12v)</td>
</tr>
<tr>
<td>2. Hardware Failure:</td>
<td>Motor Failure, Mechanical or mechanism failure</td>
</tr>
<tr>
<td>3. Network Failure:</td>
<td>Network or a portion of network has failed (Node, Wiring, Connector)</td>
</tr>
<tr>
<td>4. Code Failure:</td>
<td>Program code and/or algorithm has failed or frozen</td>
</tr>
<tr>
<td>5. Operator:</td>
<td>Vehicle driver is unfamiliar and or confused in vehicle's operation</td>
</tr>
</tbody>
</table>

**FUNCTION CRITICALITY (FC)**

1. Loss of life or Loss of vehicle control
2. Unable to complete trip or journey, requires immediate attention: stop - repair
3. Unable to complete trip or journey, does not require immediate attention: reduced performance
4. Loss of component or system has no critical effect

**Criticality Definitions from SSP 30234 (Rev F)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Single failure point that could result in loss of Space Station, Orbiter, or loss of flight or ground personnel.</td>
</tr>
<tr>
<td>2</td>
<td>Redundant items, all of which if failed, could result in loss of Space Station or loss of flight or ground personnel. When assigning criticality to an item whose failure results in the use of an emergency system, each safety system functional string shall be considered as redundancy that provides additional protection from a particular failure mode, e.g., a pressure tank is 1R for rupture when a relief valve exists.</td>
</tr>
<tr>
<td>3</td>
<td>A single failure point of the system component designed to provide safety or protection capability against a potentially hazardous condition or event or a single failure point in a safety or hazard monitoring system that causes the system to fail to detect, or operate when needed during the existence of a hazardous condition that could lead to loss of flight or ground personnel or Station (e.g., loss suppression, medical hardware).</td>
</tr>
<tr>
<td>4</td>
<td>A single failure point that is protected by a safety device, whereby the functioning of the safety device, would prevent the hazardous consequences of the failed (protected) component. This criticality category is no longer used as of Revision F of this document, but existing analyses will not be revised.</td>
</tr>
</tbody>
</table>

### MRV FMEA

#### DFMEA Driven - MRV Scenarios

<table>
<thead>
<tr>
<th>Failure Type (FT)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Power Bus:</td>
<td>All systems go off-line, emergency braking &amp; steering system? Driver's input ignored (HV, 12v)</td>
</tr>
<tr>
<td>2. Hardware Failure:</td>
<td>Motor Failure, Mechanical or mechanism failure</td>
</tr>
<tr>
<td>3. Network Failure:</td>
<td>Network or a portion of network has failed (Node, Wiring, Connector)</td>
</tr>
<tr>
<td>4. Code Failure:</td>
<td>Program code and/or algorithm has failed or frozen</td>
</tr>
<tr>
<td>5. Operator:</td>
<td>Vehicle driver is unfamiliar and or confused in vehicle's operation</td>
</tr>
</tbody>
</table>

**FUNCTION CRITICALITY (FC)**

1. Loss of life or Loss of vehicle control
2. Unable to complete trip or journey, requires immediate attention: stop - repair
3. Unable to complete trip or journey, does not require immediate attention: reduced performance
4. Loss of component or system has no critical effect

**Criticality Definitions from SSP 30234 (Rev F)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Single failure point that could result in loss of Space Station, Orbiter, or loss of flight or ground personnel.</td>
</tr>
<tr>
<td>2</td>
<td>Redundant items, all of which if failed, could result in loss of Space Station or loss of flight or ground personnel. When assigning criticality to an item whose failure results in the use of an emergency system, each safety system functional string shall be considered as redundancy that provides additional protection from a particular failure mode, e.g., a pressure tank is 1R for rupture when a relief valve exists.</td>
</tr>
<tr>
<td>3</td>
<td>A single failure point of the system component designed to provide safety or protection capability against a potentially hazardous condition or event or a single failure point in a safety or hazard monitoring system that causes the system to fail to detect, or operate when needed during the existence of a hazardous condition that could lead to loss of flight or ground personnel or Station (e.g., loss suppression, medical hardware).</td>
</tr>
<tr>
<td>4</td>
<td>A single failure point that is protected by a safety device, whereby the functioning of the safety device, would prevent the hazardous consequences of the failed (protected) component. This criticality category is no longer used as of Revision F of this document, but existing analyses will not be revised.</td>
</tr>
</tbody>
</table>

### Supervisory Control Architecture*

#### Steering System

<table>
<thead>
<tr>
<th>IF</th>
<th>FT</th>
<th>FC</th>
<th>CR</th>
<th>Then</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control Freeze - multiple corners (2+)</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>2</td>
<td>Control Loss - multiple corners (2+)</td>
<td>1,2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>3</td>
<td>Angle Sensors Failure - single corner</td>
<td>2</td>
<td>2</td>
<td>1R</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>4</td>
<td>Motor(s) Failure - single corner</td>
<td>2</td>
<td>2</td>
<td>1R</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>5</td>
<td>Erratic operation - single corner</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
</tbody>
</table>

#### Acceleration

<table>
<thead>
<tr>
<th>IF</th>
<th>FT</th>
<th>FC</th>
<th>CR</th>
<th>Then</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control is lost (Runaway)</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>2</td>
<td>Control Lost (Fixed State)</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>3</td>
<td>Control Lost (No Response)</td>
<td>1,2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>4</td>
<td>Control Lost (Erratic)</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
</tbody>
</table>

#### Propulsion

<table>
<thead>
<tr>
<th>IF</th>
<th>FT</th>
<th>FC</th>
<th>CR</th>
<th>Then</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Traction goes offline - multiple corners (3+; No Response)</td>
<td>1,2,3,4</td>
<td>2</td>
<td>2R</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>2</td>
<td>Read Head Failure (Signal Lost)</td>
<td>2</td>
<td>2</td>
<td>2R</td>
<td>Use Remaining Propulsion</td>
</tr>
<tr>
<td>3</td>
<td>System Overheats</td>
<td>2</td>
<td>2</td>
<td>2R</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>4</td>
<td>Traction goes offline - single corner (No Response)</td>
<td>1,2,3,4</td>
<td>3</td>
<td>2R</td>
<td>Use Remaining Propulsion</td>
</tr>
</tbody>
</table>

#### Braking System

<table>
<thead>
<tr>
<th>IF</th>
<th>FT</th>
<th>FC</th>
<th>CR</th>
<th>Then</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control is lost - multiple corners (No Response)</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>2</td>
<td>Control Freeze - single corner (Brakes Locked)</td>
<td>2,3,4</td>
<td>1</td>
<td>1</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>3</td>
<td>Motor(s) Fault - single corner (No Response)</td>
<td>1,2</td>
<td>3</td>
<td>1R</td>
<td>Use remaining brakes</td>
</tr>
</tbody>
</table>

#### Electrical (HV) System

<table>
<thead>
<tr>
<th>IF</th>
<th>FT</th>
<th>FC</th>
<th>CR</th>
<th>Then</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Battery Failure</td>
<td>2</td>
<td>2</td>
<td>2R</td>
<td>Controlled Stop</td>
</tr>
<tr>
<td>2</td>
<td>Battery Maintenance System Failure</td>
<td>2</td>
<td>2</td>
<td>2R</td>
<td>Use Remaining Propulsion</td>
</tr>
<tr>
<td>3</td>
<td>Power Distribution Failure</td>
<td>2</td>
<td>2</td>
<td>2R</td>
<td>Controlled Stop</td>
</tr>
</tbody>
</table>

### Fail Operational Matrix developed for supervisory & local definitions of failure scenarios and controlled reaction scenarios
Power Electronics

• Existing Power Classes
  – 600V (12kV IPM)
    • 75A (MRV)
    • 225A (CG2)

• Rugged IGBT switch technology

• Multi-loop embedded model-based control
  – Current, Velocity, Position

• Modular design enables rapid re-use
MRV Power Electronics Packaging

- Motor controller cold-plate integrated with structure
- Capacitor bank with bus bar connections

Next generation housing design incorporates new thermal design and process. Placement of motor controllers have taken advantage of cooling design efficiencies.
MRV Active Thermal Management

- Pre-cooling strategy
- High max pressure on radiator
- Lower initial temperature will increase heat removed
MRV Electrical Power System

• **Low Voltage PDU**
  – PCM Board
    • Redundant DC-DC conversion from 300V to 24V
    • Fault Detection
  – PCS Board
    • Redundant MCUs
    • Redundant Low Voltage Power Switching
    • Current Sensing
    • Comm via CAN Bus, RS232, I2C

• **High Voltage PDU**
  – HVS Board
    • Redundant High Power Switching
    • Redundant MCUs
    • Fault Detection
    • Pre-charge control
    • HV Current Sensing
    • Comm via CAN Bus, RS232, I2C
MRV Energy Storage

• MRV Battery Capacity – 18 kW hrs
• Cell Architecture - derived from Chariot 1
  • Large format cells
  • 292V nominal, 60 amp hr Lithium ion battery
  • Single series string of cells
  • 80 cells in series
  • Cells purchased from Gaia
• MRV used COTS Battery Management System
  • Manufactured by I+ME
  • Procured through a distributor, Lithium Technologies Corporation, Fairfax, VA
MRV Energy Storage

• Form factor/architecture – modules of 10 cells, easy to carry a module. BMS mounted in MRV, interfaced to each module
• Bus voltage – 292V, varies at the motor
• Thermal control – No thermal control for battery, minimal airflow
• Low capacity backup systems – Original plan in frame was to carry 3 batteries, this would give two fault tolerance. Large batteries ended up winning the day
• Charging
  • Interfaces – High voltage power supplies, constant current, constant voltage
  • Charge rates - nominal 0.2C or 11 amp; maximum 1.0C or 55 amps; to extend life, we’ve been doing < 5 amp
  • Non-mobility loads (HVAC, etc) – computers, pumps
MRV Energy Storage

• 50 amps per wheel, peak up to 60 kW propulsive power
• Static power draw 1.5 kW
• Not optimized for minimum power draw
Battery Design Experience

Space Exploration Vehicle

Centaur 2

MRV

Robonaut 2

Valkyrie

Resource Prospector Rover

PLSS
Battery Management
Design Strategy

- Battery Sizing
- Thermal Design And Analysis
- Cell Screening And Assembly
- Safety Electronics
**Boston Power Lithium ion cells**

- **5300 mAh**
- **207 Wh/kg**
- **>1000 Cycles to 100% Depth of Discharge**

---

### Specifications

<table>
<thead>
<tr>
<th>Nominal capacity</th>
<th>5300 mAh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal energy</td>
<td>19.3 Wh</td>
</tr>
<tr>
<td>Nominal voltage</td>
<td>3.65 V</td>
</tr>
<tr>
<td>Energy density</td>
<td>Gravimetric</td>
</tr>
<tr>
<td></td>
<td>Volumetric 490 Wh/L</td>
</tr>
<tr>
<td>Nominal cell impedance</td>
<td>15.5 mΩ</td>
</tr>
<tr>
<td>Cycle life</td>
<td>100% DOD &gt;1000 cycles</td>
</tr>
<tr>
<td></td>
<td>90% DOD &gt;2000 cycles</td>
</tr>
<tr>
<td></td>
<td>80% DOD &gt;3000 cycles</td>
</tr>
<tr>
<td>Max continuous discharge rate (0%-100% SOC)</td>
<td>13 A</td>
</tr>
<tr>
<td>Allowable 10s pulse capability</td>
<td>1000 W/kg</td>
</tr>
<tr>
<td>Standard charging method</td>
<td>Constant current (CC) 3.7A (0.7C) to 4.2V</td>
</tr>
<tr>
<td></td>
<td>Constant voltage (CV) 4.2V to 50 mA</td>
</tr>
<tr>
<td>Max charge rate (continuous)</td>
<td>10.6 A</td>
</tr>
<tr>
<td>Nominal cell weight</td>
<td>93.5 g</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>Charge -20 to +60 °C</td>
</tr>
<tr>
<td></td>
<td>Discharge -40 to +70 °C</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40 to +60 °C</td>
</tr>
</tbody>
</table>

---

1. Standard discharge 0.2C to 2.75V
2. 50% to 100% SOC

Boston Power Swing 5300 Features

- Small elliptical cell format
- Nordic and Chinese Ecolable certification
- Aluminum Can
  - High heat transfer rate vs cells using steel cans
  - Inherently lower venting pressure
  - Eliminates corrosion issues associated with Fe-containing cans

<table>
<thead>
<tr>
<th>Special separator</th>
<th>CID</th>
<th>Oriented Vent</th>
<th>Rupture</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 layered separator</td>
<td>Current Interruption Device</td>
<td>Directed; redundancy</td>
<td>Less catastrophic</td>
</tr>
</tbody>
</table>

**Mechanism**
- Pores shut down at high temperature
- Pressure fuse
- Non-resettable
- Protect from pressure buildup
- Vent direction controllable
- 2 vents for redundancy
- Aluminum vs. steel for 18650

**Devices Protects Against**
- Overcharge
- Over temperature
- Internal shorts with temperature increase <150 °C
- Overcharge
- Over temperature
- Explosion
- Cascading (cell-to-cell runaway initiation)
- Explosion
R2 Batpack
R2

Cell Configuration: 300 cells in full pack
- 5 Series connected cartridges
- 5 Virtual cells in series per cartridge
  - 12 parallel cells per virtual cell

Energy: 5790 Wh
- Total Pack Assembly Weight = 37.421 kg
- Effective Energy Density = 154.724 Wh/kg

Operating Voltage: 105V – 65V
- Nominal pack voltage: 92.4V

Max Continuous Discharge: 156 A
Valkyrie

Cell Configuration: 96 cells in full pack

- 2 independent batteries for two power busses in one package
- Four 24 cell cartridges
- Low voltage pack is one cartridge
- 8 cell virtual cell
- 3 series connected virtual cells
- High voltage pack is 3 series connected cartridges
- 2 cell virtual cell
- 36 series connected virtual cells

Energy: 1860 Wh

- Runtime: ~1 hour
- Energy Density ~133 Wh/kg

Operating Voltage

- Low Voltage pack (42 Ah)
  - Nominal 10.95V
  - Ranges from 9V to 12.6V
- High Voltage pack (10.6 Ah)
  - Nominal 131.4V
  - Ranges from 108 to 151V

Max Continuous Discharge (HV): 30 A
Max Continuous Discharge (LV): 60 A
Resource Prospector (RP)

- **RP Battery**
  - Utilize Boston Power Swing 5300 cells
  - 12P24S layout consisting of quantity four 12P6S cartridges in series
  - 288 Cells
- **Voltage**
  - Max: 100.8 V
  - Nominal: 87.6 V
  - Min: 72 V
- **Current**
  - Max: 156 A
  - 1C: 64 A
  - 0.1C: 6.4 A
- **Power**
  - Max: 13665 W
  - 1C: 5606 W
  - 0.1C: 560 W
- **Thermal Range (Cells)**
  - Charge: -20 to 60°C
  - Discharge: -40 to 70°C
  - Storage: -40 to 60°C
  - Significant Loss in capacity below 0°C
  - Capacity Increases at higher temperatures
- **Energy**: 5571 Wh (100% DOD)
- **Estimated Weight**: 32 kg (70 lb)
- **Estimated Gravimetric Energy Density**: 174 wh/kg
Battery Safety
Catastrophic Hazards

- Conditions that lead to catastrophic failure (thermal runaway)
  - Overvoltage
  - Charging over discharged cells
  - Overcurrent
  - External heating (system design)
  - Internal Short
Safety Philosophy

- Our safety philosophy is to control against all catastrophic causes with two fault redundancy in detection and mitigation
- Action’s based upon fault detection are flexible by design and vary depending on the application

*Additionally current testing and design efforts include working to prevent cell to cell propagation in the event of a single cell runaway*
Safety Electronics

High Level: Operational Limits

Mid Level: Software/Firmware Limits
- \textit{(Safety Critical Code adds cost and complexity)}

Low Level: Hardware Limits
- \textit{(R2 hardware is 2 fault tolerant without software)}
Modular Battery Management System

BMS Slave Board

- Configurable to up to 12 series cells
- Stackable up to 31 boards (372 series cells)
- Over/Under Voltage Hardware Comparators
- Over/Under Temp Hardware Comparators
- Voltage and Temperature Monitoring
- All hardware safeties trip an interlock signal which can be used by the master as a hardware inhibit

BMS Master Board

- Communicates with slave boards via i2c interface
- Independent stack level Over/Under voltage monitoring
- Over Current Monitoring
- Disengages battery from system during any safety event
Battery Management System Telemetry

- Each Virtual Cell Voltage
- Min/Max/Avg Cell Voltage
- 12x Temp’s/Cartridge
- Stack Voltage
- Current
- Error/Warning Flags
- Error/Warning Counters
- Cell Balancing Status
- BMS state machine state

- Firmware Version
- Hardware Version
- Discrete input states
- Discrete output states
- ADC Sample Counters
- Local Power Supply Voltages
- Charger Control Parameters
Thermal Runaway Propagation

- Investigating materials for unique thermal properties
- Testing at the cell and pack level for propagation tolerance
- Coordinating with parallel NASA Engineering Safety Council and Space Suit Battery team work
- Developing thermal abuse models to aid with design of mitigation features
MRV Battery Power Estimation

- Estimated Vehicle Power Requirements based on NYCC Drive Cycle
- Assumptions:
  - 4 e-Corners
  - Vehicle mass: 862Kg
  - Hotel power load: ~1500W
  - Acceleration: 0.3g
  - Deceleration: 0.3g (-1.0g emergency)
  - CD: 1.0

**Power Profile with CD of 1.0**

**Power Profile with CD of 0.3**

April 19th 2012
Hybrid Battery/Capacitor bank options

- NASA has investigated this approach for previous mobility system projects
- Looked at different convertors, approaches for connecting the capacitor to the batteries
- Initial architecture explored was large battery and large capacitor bank
  - This approach was influenced by size of Chariot rover design concept
- NASA bought a custom built bi-directional DC-DC converter device from US Hybrid for evaluation
- Initial evaluation was to send current back and forth between two batteries
- Goal was to charge one electric vehicle with another vehicle
- Other hybrid battery architectures explored involve pairing up a battery and a capacitor.
MRV Energy Transfer between Batteries

- Implemented bi-directional DC-DC Converter
- Directly applicable to Hybrid power systems
- Demonstrated power transfer in both directions
  - HV battery balancing
  - “Empty” one battery into the other in contingency
  - Arbitrary voltage and current setpoints (0-600V)
Power Management

• Low voltage “flavors” – many voltages used in MRV
• 24V - motor controller logic voltage, power thermal system, computers
• 12V – common for automotive systems
• Familiar with down conversion to lower voltages for many systems
• Dual redundant power systems in MRV
Power Electronics Modules

- Good success with COTS power modules
- R2 uses MS Kennedy, high reliability power electronics for military and aerospace. PowerEX also used, US manufacturer of power modules, relationship with Mitsubishi. R2 uses PowerEX in legs
- Sizing - expanding the top end range of power through the motor drives. Valkyrie fingers is smallest. Chariot 2 wheel module is largest power use, as implemented can accept 600V, deliver 225 amps
- De-rating – numbers above are derated 50%. Vendors recommend establishing limits through testing. Motorcycle dyno testing used for MRV.
- Supercar calls for lots of power, derating through modeling. Look to vendors for the models, we plug in our usage.
- For MRV and Chariot Gen 2, Mitsubishi has a model that shows loss value. Testing was very successful in establishing derating levels
- Commonality across subsystems – applied where feasible
Regenerative Braking

• NASA first implemented this with Chariot
• NASA implementation for MRV is a blending of mechanical and regenerative braking
• NASA sought motor which both a good motor as well as a good generator
• Design requirements of accelerating at 0.3 g, decelerating at 1 g were set for MRV. Acceleration requirement was accomplished in design, design for deceleration achieved 0.5g
• Regen power goes directly into MRV battery
• For battery/supercap architecture, trade study needed to determine what regen power goes to battery vs supercap
Regenerative Braking

- Shunting when fully charged - needed for systems with no large energy reservoir
- Robonaut 2 needed shunting
- Chariot has shunt regulator
- Our approach is to manage this operationally (don’t charge it up all the way)
MRV Regeneration and Mechanical Braking Contributions

Desired Braking Torque

Percent Braking Torque

Regen
Mech