Example Hazard Assessment and Mitigation Plan

Background
The FutureCar Team is working on a single passenger vehicle that will have a top speed of approximately 30 MPH and a performance-oriented propulsion system for good acceleration. The students are designing a hybrid power plant that will utilize a hydrocarbon fuel source to drive an electrical power system. Evaluation of the design will require driving the vehicle over a secure course.

We would like to use the road surface that surrounds the Yale Bowl as a test track during a time of low activity. We do not anticipate using rough or uneven terrain.

Hazard Assessment:
We will proceed with testing under two configurations:

1) Stock proven commercial cart configuration- Baseline testing prior to any functional design modifications
2) Hybrid/modified design configuration

The students will be designing and assembling components and modules that will be capable of producing and transmitting electrical and mechanical power on the order of 20 horsepower. Potential hazards include moving parts, electrical potentials, component failures and driving obstacles. It is anticipated that hazards at this prototype stage of development may be handled by incorporating safety systems in the design, operator training or control of the environment. Specific hazards and mitigation strategies are listed below:

Hazard	**Mitigation/Safety measure(s)**
Loss of control while driving – bystander injury hazards	Use a secure test track. Place marshals around the track to ensure that bystanders and other vehicles do not enter the track. Use radio communications between marshals.
Loss of control while driving – driver injury hazards	Drivers will wear helmets, eye protection and full clothing to cover all parts of the body. Car has a 5 point harness and roll cage that were purchased from a reputable cart manufacturer. Test track will have wide shoulders and runout space over the entire track. Drive testing will be carried out with speed governed to 15 mph before allowing higher speed operation.
Loss of control while driving – throttle malfunction	1) proven standard configuration with mechanical throttle returns, brakes and driver-operated engine shutdown. 2) Hybrid Design: Throttle will use a redundant control sensor so that a single point failure will not result in loss of control. Mechanical brakes will be left intact and capable of overriding propulsion system. E-stop switches will be fitted in multiple locations on the frame

	to ensure that drive system can be disconnected from drive axles. E-stop will require battery activation to enable propulsion system so that any loss of power to relays will interrupt propulsion system.
Driver entrapment	Roll bar / cage for driver protection. Safety Harness has a single release button. Driver must demonstrate ability to exit car in under 4 seconds when car is stopped prior to each test run.
Mechanical failure of transmission component causes component to separate from car	All rotating machinery will have guards. Design will be reviewed by 2 faculty members (Professor Smith & Professor Ivanova) and 3 technical staff (John Ramirez, Ed Chao and Jane Jones) to review design for integrity, strength and electrical safety concerns.
Electrical failure of power electronics causes short circuit	1) Commercial production insulated low voltage design 2) Hybrid Design: Energy sources will have fuse/circuit breaker interrupters to cut off short circuit currents. Electrical components/wires will be insulated.
Electrical potential on frame of car	All high current conductors will be insulated and mounted to avoid chafing. Predrive check list will include a ground check to make sure no continuity exists between power electronics and chassis (SAE requires a "Hypot" test)
Fuel spill creates fire hazard	1) Commercial configuration Guarded central location tank of about 2 gallon capacity/ secure cap with roll over check valve to reduce likelihood of fuel spill 2) Fuel tank fill will be very small to minimize fuel on vehicle to amount needed to perform required testing(1-2 quarts). Fire extinguishers will be placed strategically with selected track marshals.
General injury hazards	Request that first responders from Yale Athletics be made aware of the class activities and be available during the testing period.

Test Preparation Protocol

During testing, we will have a safety vehicle ready to respond to incidents/issues (either following or stationed along side the track)

At the lab, prior to loading car for transport
Test propulsion system on lift
Inspect car per safety checklist (to be based on final design)
Fuel is secured
Electrical systems are disconnected/off

At the Track
Marshals at entry points to course.
Safety vehicle equipment list: radio, fire extinguisher, first aid kit
Inspect car per safety checklist (to be based on final design)

Before car leaves pit
Marshals have radio contact with pit chief
Test car has radio contact with pit chief

While car is on track
Marshals report each time car passes via radio
Pit chief monitors radio contact

Messages:
"Code Green" – track is clear
"All stop" – car operation is stopping – nothing serious is wrong
"Code Yellow" – if any person believes there is something on the track that shouldn't be there
"Code Red" – The car or track is not safe – stop immediately
"Emergency at ____" – there is reason to believe someone is in danger – give the location.

Post test
Fuel is secured
Electrical systems are disconnected/off

Specific support required from Yale organizations

1) Permission from the Yale Bowl facilities manager to use the track surrounding the Yale Bowl as a test driving track. We will need to know what days/times are most appropriate.
2) Support of the trainers at the Yale Bowl to be available should anyone require treatment.