A NASA Approach to Safety Considerations for Electric Propulsion Aircraft Testbeds

Kurt V. Papathakis[1] and Alaric M. Sessions[2]
NASA Armstrong Flight Research Center, Edwards, CA, 93523

Phillip A. Burkhardt[3] and David W. Ehmann[4]
Jacobs Technology, Edwards, CA, 93523

Electric, hybrid-electric, and turbo-electric distributed propulsion technologies and concepts are beginning to gain traction in the aircraft design community, as they can provide improvements in operating costs, noise, fuel consumption, and emissions compared to conventional internal combustion or Brayton-cycle powered vehicles. The National Aeronautics and Space Administration (NASA) is building multiple demonstrators and testbeds to buy down airworthiness and flight safety risks for these new technologies, including X-57 Maxwell, Hybrid-Electric Integrated Systems Testbed (HEIST), Airvolt, and NASA Electric Aircraft Testbed (NEAT). This paper addresses the safety system design process used at NASA Armstrong Flight Research Center, specific hazards associated with these new electric propulsion technologies, including an extensive investigation into the emergency-stop system for a HEIST, and other best practices. In general, the best course of action is to actively design out hazards associated with these systems, but when removing these hazards is either impossible or impractical, other safety protocols including keep-out zones, lock-out/tag-out, and other practices should be implemented.

Nomenclature

A	=	amperage
AC	=	alternating current
AC/DC	=	alternating current to direct current (converter)
AFRC	=	Armstrong Flight Research Center
AFSRB	=	airworthiness and flight safety review board
ARMD	=	Aeronautics Research Mission Directorate
BMS	=	battery management system
CANBus	=	controller area network bus
Cat	=	category
CIS	=	cockpit interface system
CRM	=	continuous risk management
CST	=	combined systems test
E-stop	=	emergency stop
EMI	=	electromagnetic interference
FMEA	=	failure modes and effects analysis
HAM	=	hazard action matrix
HEIST	=	Hybrid-Electric Integrated Systems Testbed
HIU	=	hardware interface unit
HR	=	hazard report
HSDR	=	high speed data recorder
LEAPTech	=	Leading Edge Asynchronous Propeller Technology

[1] HEIST Power Architecture, Vehicle Integration & Test Branch, P.O. Box 273/MS4800D, member.
[2] HEIST Hardware/Software Interface, Simulations Engineering Branch, P.O. Box 273/MS4840D, non-member.
[3] HEIST Safety Engineer, Safety of Flight Branch, P.O. Box 273/MS4800, non-member.
[4] HEIST Power Systems, Vehicle Integration & Test Branch, P.O. Box 273/MS4800, non-member.

KOZ	=	keep-out zone
NASA	=	National Aeronautics and Space Administration
NEAT	=	NASA Electric Aircraft Testbed
O&SHA	=	Operations and Support Hazard Analysis
PHA	=	preliminary hazard analysis
PHL	=	preliminary hazard list
PPE	=	personnel protective equipment
RPM	=	revolutions per minute
RX	=	receiver port / receiver
SCRAMNet	=	shared common RAM network
SHA	=	system hazard analysis
SIS	=	simulation interface system
SSHA	=	subsystem hazard analysis
SSP	=	systems safety plan
SSWG	=	systems safety working group
TX	=	transmitter port / transmitter
VAC	=	volts, alternating current
VDC	=	volts, direct current
VFR	=	visual flight rules

I. Introduction

THE National Aeronautics and Space Administration (NASA) Aeronautics Research Mission Directorate (ARMD) has identified reducing energy consumption, emissions, and noise for future aircraft in their Strategic Implementation Plan.[1] In order to accomplish these goals, technology development, simulation, flight demonstration, and ground testing must be performed to mature new concepts and retire electric, hybrid-electric, and turbo-electric propulsion flight risks. NASA is currently developing and testing the X-57 Maxwell (Empirical Systems Aerospace, Inc., Pismo Beach, California) all-electric airplane, the NASA Electric Aircraft Testbed (NEAT) for testing megawatt scale components, the Hybrid-Electric Integrated Systems Testbed (HEIST) for testing flight components with simulation-feedback, the Airvolt test stand, a single highly-instrumented electric motor-propulsor, and others in development. These testbeds represent key capabilities for the X-57 Maxwell airplane and future electric, hybrid-electric, and turbo-electric flying demonstrators. There are numerous electrified aircraft propulsion architectures being proposed, but all have inherent high voltage and current, requiring extensive safety considerations. This paper aims to identify safety hazards and mitigation strategies associated with these architectures. Figure 1 shows the X-57 Maxwell, HEIST, and Airvolt projects, at varying levels of maturity.

Figure 1. NASA electric and hybrid-electric projects: X-57 Maxwell (left), HEIST testbed wing trailer (center), and Airvolt test stand (right).

The X-57 Maxwell demonstrator is NASA's first all-electric, manned X-plane. A Tecnam (Casoria, Italy) P2006T airframe has been mated with an experimental, high-speed cruise wing, and electric motors and batteries. The primary propulsors are two Joby Motors (Santa Cruz, California) JM-X57 motors paired to pitch controlled propellers producing 72 kW max (60 kW continuous) located at the wing tips of the new experimental wing. Twelve additional motors paired to fixed-pitch, folding props will be integrated as part of the final X-57 buildup. The fuel tank and plumbing have been replaced by a 57 kWh battery and a high voltage (461 VDC nominal) bus architecture, designed to be single fault tolerant.[2]

The HEIST at NASA Armstrong Flight Research Center (AFRC) (Edwards, California) is configurable as an all-electric, hybrid-electric, or turbo-electric test stand, and has aerodynamic loading feedback via a network of dynamometers and connectivity to the AFRC simulation labs. The testbed consists of eighteen Joby Motors JM-1 electric motor / propeller propulsors, a Capstone (Chatsworth, California) C-65 Turbogenerator, an AC/DC converter (converting the 480 VAC from the turbogenerator to the DC bus), simulation computer, and all necessary signal and power routing. In order to obtain meaningful aircraft controls research for an electric, hybrid-electric, or turbo-electric configuration, the system must be tied into the simulation computers, allowing controls engineers to manipulate all the propulsors, battery system, and turbo-generator system. The need for direct connectivity of the testbed to the simulations laboratory as well as aircraft hangar regulations at NASA AFRC necessitated a testbed trailer setup, and allowed for testing flexibility while maintaining connectivity to the simulation laboratory.[3]

Airvolt was the first AFRC all-electric demonstration project, designed to be a fully-instrumented, single propulsor test stand in order to better understand and analyze how current from the batteries ultimately produced thrust from the propeller, via the bus architecture, motor controllers, motor, and other equipment. Airvolt is currently being used as a method of acceptance testing for the X-57 Maxwell JM-X57 cruise motors.

NASA is aggressively pursuing multiple all-electric, hybrid-electric, and turbo-electric models, test stands, and flying demonstrators, while endeavoring to maintain high levels of safety throughout the design process and testing. In order for these systems to retire electric, hybrid-electric, and turbo-electric distributed propulsion architecture risks, numerous safety considerations must be implemented, as these systems require high voltage and current, especially for the new megawatt-scale systems being proposed. A safety design is the incorporation of control methods and processes which begins early in the system design to either eliminate a hazard or mitigate risks to human health and safety throughout the lifespan of the platform.

II. Electric, Hybrid-Electric, and Turbo-Electric Testbed Hazards and Mitigations

To help assure mission success for these all-electric, hybrid-electric, and turbo-electric distributed propulsion projects, NASA is leveraging the hazard analysis process from the NASA Hazard Management Procedure[4] to identify, eliminate, or control to an acceptable level the hazards associated with the projects that could affect human safety, damage or loss of assets, or loss of mission during the conduct of operations. NASA AFRC has a stringent hazard identification and mitigation system allowing the Center to self-certify experimental aircraft. This process starts with identifying hazards in preliminary hazard reports, complete with causes, effects, mitigations, and then categorizes the probability and severity for humans and assets. These preliminary hazards are then used to update the system and subsystem requirements. Once the hazards are accepted by the design board or reviewing committee, hazard reports are populated and signed off by the project manager or Center leadership, depending on the hazard severity and probability classification.

The hazard analysis process must be implemented in the early stages of the project so that hazards can either be eliminated or minimized through the design process. This principle is especially critical when dealing with the complexities of new technologies and experimental systems, such as new electric motors, motor controllers, batteries, traction bus equipment, and other systems associated with these new electric / hybrid-electric architectures. Another critical element of the AFRC hazard management process is continuous risk management (CRM). CRM is not a one-time pass through, but a continuous activity where the identification of new risks occur throughout the life cycle of the project.

The hazard analysis process starts with the identification of Center responsibilities for mission success, airworthiness, ground / flight safety, and mishap contingency considerations. The hazard analysis process is usually accomplished by distilling requirements and objectives for the project, determining the required level of system safety support, and designating a system safety engineer to the project. The system safety engineer defines and tailors the project's specific hazard management process through the development of the project's system safety plan (SSP). Following the development of the SSP, the system safety engineer, in conjunction with the project manager and lead engineer, will establish the system safety working group (SSWG).

The SSWG is comprised of personnel from across all project disciplines and skill sets and provides the forum where participants review potential hazards introduced directly or indirectly by the project. This forum creates an atmosphere where formal technical discussions and interactions between team members can take place that are crucial to fully recognize the causes of a hazard, the subsequent effects, and to develop strong mitigation actions.

A mishap is the effect, or outcome, of the hazard. In the event of a mishap, a degree of severity will be assessed. It is that assessment that will drive the level of response to the particular mishap. Mishaps are categorized into 5 categories ranging from catastrophic to close-call. A hazard cause is the condition that contributes to the hazard. It could be an unsafe design, environmental factors, hardware failure, software error, human error, et cetera.

Hazards are described in a scenario-based statement that addresses the cause (source) and effect (outcome); or source, mechanism, and outcome (i.e., consequence) to characterize the potential harm of the hazard. Hazard mitigations are the means by which a hazard can be eliminated completely or the probability and/or severity can be reduced (outcome). An order of precedence has been derived from experience that has shown that eliminating a hazard is the most effective means of preventing a mishap.

The hazard mitigation order of precedence is as follows:

1) Design to eliminate the hazard or to minimize risk (e.g., utilizing "fail-open" contactor relays, so that in the event of an uncontrollable failure, all high-power circuits will not be energized).
2) Incorporate safety features and/or safety devices to minimize risk (e.g., incorporating an emergency-stop system or other inhibit device).
3) Incorporate warning/caution/protective devices to minimize risk (e.g., flashing light with a sign to indicate that there is a radiation hazard present).
4) Use special procedures/training/personal protective equipment to minimize risk (e.g., mission rules/operating limits, test procedures that contain warnings and precautions with regard to test being performed, high pressure systems training, hearing protection, safety glasses, gloves, hard hats, et cetera).
5) Use of placards to minimize risk (e.g., implementing a propeller or audio-threshold keep-out zone with stanchions).

In order to categorize a hazard, both the probability of occurrence and severity must be identified. Probability is the likelihood that an identified hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population. Severity is an assessment of the worst potential consequence, defined by degree of injury, loss of asset, property damage, the cost of an unforeseen event (loss of mission), or loss of data.

The NASA AFRC hazard severity and probability categories in Table 1 are derived from the NASA safety manual,[5] and are communicated by utilizing the NASA Armstrong hazard action matrices (HAM). The purpose of HAMs are to relate human safety hazards and loss of asset/mission in order to identify the associated overall hazard risk. These templates are used to convey the project's residual risk (current category/projected final category) to the Center's airworthiness and flight safety review board (AFSRB) and various project reviews during the course of the project. The purpose of the AFSRB is to ensure that projects are airworthy, safe, comply with Center policies and procedures, and maximize mission success. The AFSRB is comprised of the Center's chief engineer, project management, subject matter experts, pilots, and operations and safety personnel.

Table 1. NASA AFRC hazard severity and probability classification matrices.

	Injury severity classifications				
	A: Frequent	B: Probable	C: Occasional	D: Remote	E: Improbable
I: Catastrophic					
II: Critical					
III: Moderate					
IV: Negligible					

	Asset/mission severity classifications				
	A: Frequent	B: Probable	C: Occasional	D: Remote	E: Improbable
I: Catastrophic					
II: Critical					
III: Moderate					
IV: Negligible					

	Requires Center Director approval and may require approval by a higher authority. These hazards are defined as "Accepted Risks."
	Risk acceptance requires Center Director approval. These hazards are defined as "Accepted Risks."
	Risk acceptance requires Project Manager approval.

After the SSWG has been established, the hazard analysis process is initiated with the development of a preliminary hazard list (PHL); a series of brainstorming sessions where potential hazards are introduced to the team for consideration. All hazards deemed credible by the subject matter experts are documented using the AFRC hazard report (HR), and a preliminary hazard analyses (PHA) is performed.

The HR is the primary tool used to document and track a hazard. A compilation of these forms for all identified hazards associated with a project serves as the primary documentation from the initial PHA through the subsequent analyses that follow, that is system hazard analysis (SHA), subsystem hazard analysis (SSHA), and operations and support hazard analysis (O&SHA) (if deemed applicable by the project). These analyses refine the PHA and identify additional hazards that may become apparent as the understanding of a project's systems and operational requirements mature.

The X-57, HEIST, and Airvolt projects have each undergone the AFRC hazard analysis process, and though the projects differ in overall system complexity, there are still many similarities in regards to design considerations that need to be made to assure overall reliability and safety of the systems. Some of these considerations are, but are not limited to: single fault tolerance, adequate margins (de-rate power systems, et cetera), ruggedization of critical components (thermal/mechanical), fail-safe mechanisms, circuit protection, interlocks, audio/visual alarms, electromagnetic interference (EMI) shielding, emergency manual shutdown, protective enclosures for power systems, et cetera. The full X-57 Maxwell traction bus hazard is shown as an example (Table 2) including hazard causes, effects, severity and probability for both human and asset categories, and mitigations. A full list of the HRs with the severity and probability for both human and asset categories for each project are shown in Table 3.

Table 2. X-57 Maxwell Hazard Report 3 (HR-3) traction bus failure full description.

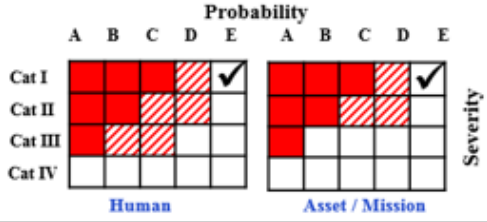
X-57 Maxwell HR-3 traction bus failure	
Causes	**Effects**
A. Electrical short B. Wiring defect C. Design error D. Circuit protection component failure E. Installation error F. External/environmental abuse (thermal/mechanical) G. Grounding isolation fault H. Inadequate grounding I. Operational / procedural error J. Lightning strike	* Loss of essential avionics power * Total loss of aircraft power * Motor failure * Propeller governor failure * Fire * Damage or loss of aircraft * Damage to ground assets * Injury or death to personnel
AFRC hazard action matrices	**Mitigations**
	1 Design avionics bus for single fault tolerance (A,B,C,D,E) 2 Ground test (CST) (A,B,C,D,E,F,G,I) 3 Grounding checks (G,H) 4 Design with margin (de-rate power system) (C,D,F) 5 Quality control process (B,E,I) 6 Peer review of design (C) 7 VFR operations only (J) 8 Perform visual inspection of system components (A,B,D,E,F) 9 Adhere to X-57 operational placards and procedures (E,F,H,I,J)

Table 3. NASA electric and hybrid-electric hazards, and severity/probability classifications.

Project hazard summary	Severity/probability classification	
	Human	Asset
X-57 Maxwell		
HR-1 Aircraft traction battery fire	I D	I D
HR-2 Structural failure of wing	I D	I D
HR-3 Traction bus failure	I E	I E
HR-5 Aircraft damage due to exposure to excessive environmental conditions during ground operations	N/A	III D
HR-7 Wing control surface system failure	I D	I D
HR-9 Inadequate stability control	I D	I D
HR-11 Failure of motor mounts	I E	I E
HR-12 Whirl flutter	I D	I D
HR-13 Symmetric loss of cruise propeller thrust (partial/total)	II E	II E
HR-14 Avionics bus failure	III E	II E
HR-15 Cruise propeller performance degradation and/or separation	I E	I E
HR-17 Battery modules separate from attach points	I E	I E
HR-18 Abrupt asymmetric thrust	I D	I D
HR-19 Electromagnetic interference in flight	N/A	IV D
HR-20 Landing gear structural failure	II D	I D
HR-21 Failure of propulsor system	I E	I E
HR-22 Restricted and/or obstructed crew egress	I E	N/A
HR-23 Cockpit air contamination	I E	I E
HR-24 Inadvertent cruise motor propeller rotation	I E	III E
HR-25 Equipment pallet separates from attach points	I E	III E
HR-26 Personnel exposed to high voltage/current	I E	N/A
HR-27 High lift propeller damage and/or separation	Analysis in work	
HR-28 Classic flutter	I E	N/A
HEIST		
HR-1 Propeller failure	I E	III C
HR-2 Traction battery fire	II E	III D
HR-3 Inadvertent system activation	I E	III E
HR-4 Electrical discharge / shock / arc flash	I E	III E
HR-5 HEIST ground asset collision	I E	II E
HR-6 JM-1 motor failure	I E	IV B
HR-7 Electrical fire	II E	III D
HR-8 Damage to HEIST assets due to environmental factors	N/A	III E
HR-9 Test article support structure failure	I E	III E
HR-10 Excessive noise exposure	II E	N/A
HR-12 Dynamometer system failure	I E	III C
HR-15 Software operation outside of intended parameters	N/A	III C
HR-16 Electromagnetic interference	N/A	IV D
HR-17 Loss of hardware communication link	N/A	IV D
Airvolt		
HR-1: Lithium polymer battery fire	II E	IV E
HR-2: Airvolt test stand structural failure	I E	III E
HR-3: Electrical fire	III D	II E
HR-4: Electrical discharge/shock	I E	III E
HR-5: Propeller / motor failure	I E	IV E
HR-6: Test personnel exposed to excessive noise during system operation	II E	N/A

A primary safety consideration for most aircraft and ground test projects is the use of a testing keep-out zone (KOZ). This keep out zone is in place during all testing activities and includes electric/hybrid-electric-specific considerations, such as: propeller keep-out zone, a motor magnet debonding hazard zone, and an auditory keep-out zone based on O&SHA regulations for excessive noise exposure. The propeller keep-out zone applies when a protective shield is not in use. The propeller keep-out zone is based on the FAR 25.905 dictating a 10% angle from the propeller plane.[6] The keep-out zone distance is a function of the maximum propeller speed, propeller diameter,

and failure mode. While the implementation of a keep-out zone does not reduce the probability of a propeller failure, it does completely mitigate any substantial negative effects to all personnel. The HEIST team has also designed a protective shield, which mitigated both to a propeller failure and a debonded motor magnet. Experience from previous electric propulsion projects, including the Leading Edge Asynchronous Propulsion Technologies (LEAPTech) experiment,[7] suggests that a debonded magnet from an experimental flight-rated electric motor is possible, and the exact effects of a lost magnet are yet unknown. Therefore, a protective shield has been implemented in order to reduce that risk until the full extent of that failure can be identified. Lastly, an auditory keep-out zone and personal protective equipment (PPE) required zone were also implemented, as the turbogenerator and propellers at full speed do exceed the O&SHA 85 dB threshold for long-term exposure. As shown in Fig. 2, the propeller, motor magnet, and audio-threshold KOZ has a circular area for the audio decibel level threshold and motor magnet departure, with extensions in the propeller plane for blade departure. This KOZ is instituted during all testing and any troubleshooting where high speed rotation of the electric motor / propeller propulsors is needed.

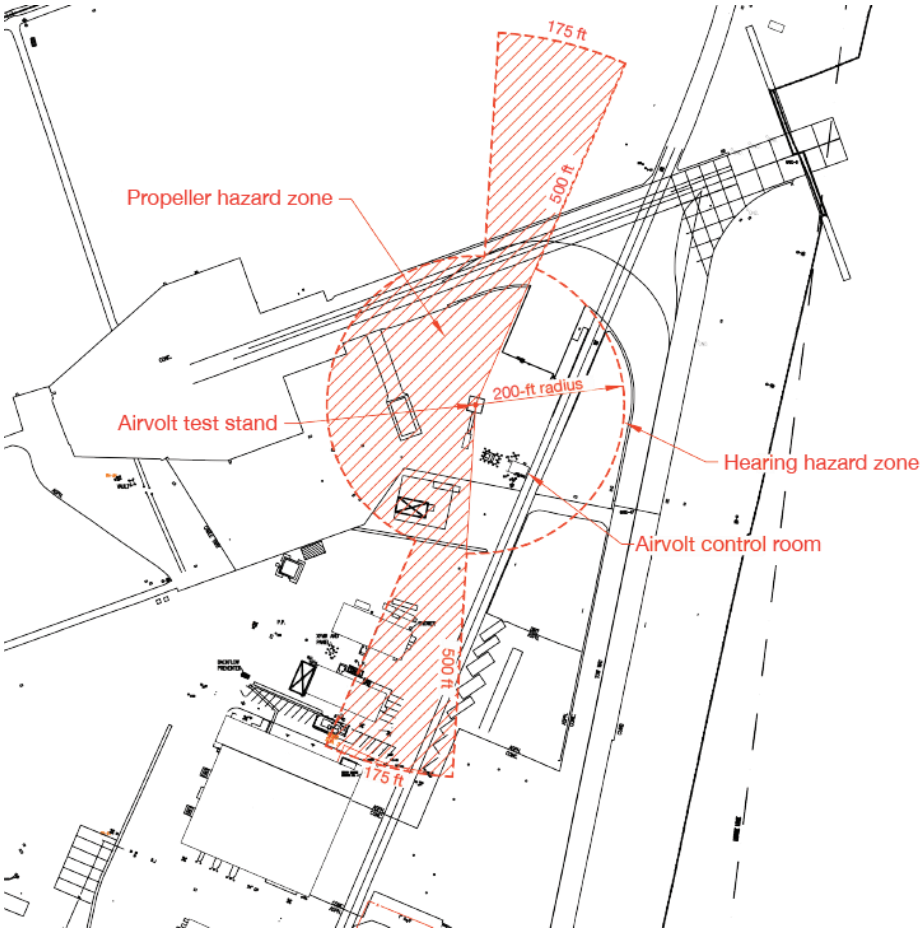


Figure 2. NASA Airvolt propeller, motor magnet, and audio-threshold keep-out zone.

III. NASA HEIST Power Relay and Emergency-Stop Networks

The HEIST testbed is a platform that supports a wide variety of components requiring multiple mitigations for each component and subsystem. One mitigation that was present in multiple HRs was the need for a robust emergency stop (E-stop) system. The definition of an E-stop is a functionality that is intended to prevent or reduce existing hazards to personnel or project assets. The E-stop system is a reactive system that does not prevent an incident from happening, but rather stops the process without creating additional hazards.

This safety strategy began at the concept stage of the design process when initial decisions were made about the overall system layout, component selection, and functional testing requirements for the HEIST testbed and evolved through the life of the project. It is easier and lower cost to eliminate hazards or integrate safety mitigations at the

beginning of the project when everything is on paper rather than modifying the final product at later phases. This safety design included more than just the electrical circuit and physical layout; it required brainstorming potential hazards and design solutions as the testbed was manufactured, transported, set up, torn down, tested, and/or modified.

One of the primary safety designs of E-stop is the network of contactor relays. This safety mitigation strategy directly or partially mitigates a propeller failure, traction battery fire, inadvertent system activation, electric discharge / shock / arc flash, JM-1 motor failure, electric fire, damage to HEIST assets due to environmental factors, test article support structural failure, blowing debris from propeller wash, dynamometer system failure, software operation outside of intended parameters, electromagnetic interference, or loss of hardware communication link. This network removes all high voltage power from all power sources (6 battery banks and turbogenerator) and sinks (all motors and dynamometers). See Fig. 3.

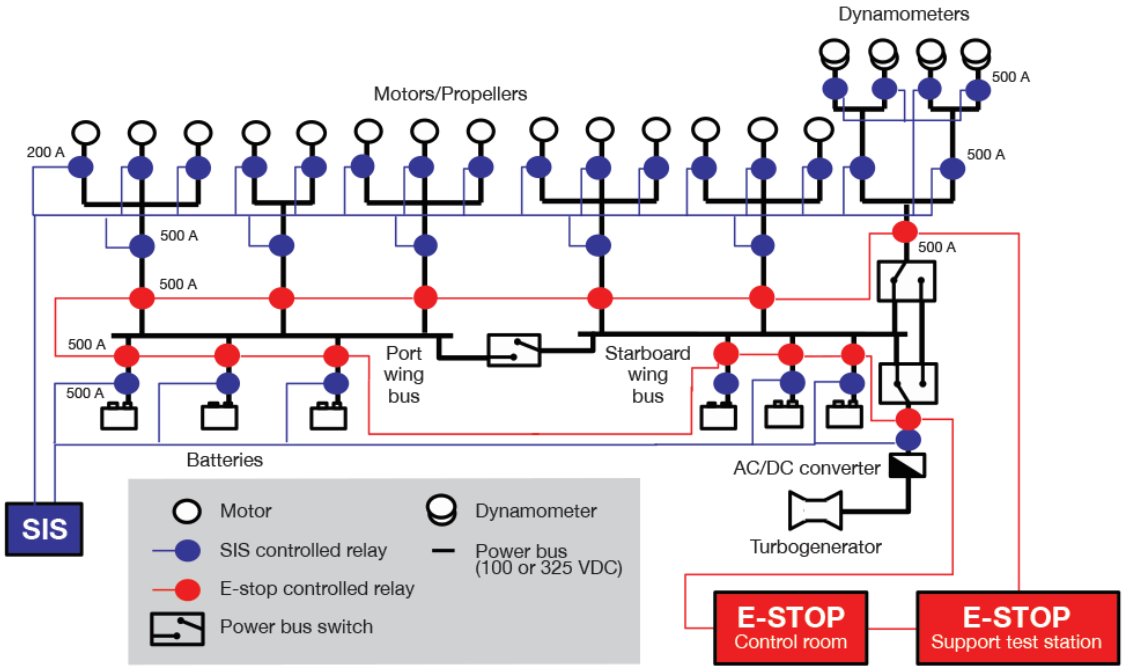


Figure 3. NASA HEIST relay network topology.

The testbed also has software controlled contactors for research purposes shown as the simulation interface system (SIS). The two contactor relay networks are fundamentally separated in order to prevent a software failure inadvertently keeping the system from shutting down during an emergency. The high voltage bus operates at 100 VDC or 325 VDC (during different phases of the HEIST development). Activating the E-stop removes each battery (six 100 VDC sets or two 325 VDC sets, depending on phase of development), the C-65 turbogenerator (via internal shutdown protocol), and the AC/DC converter off of the main power bus. The traction bus is separated into two buses, mimicking port and starboard wing traction power buses. The JM-1 motor / motor controller propulsors are organized into groups of 2 or 3 in order to limit the current flowing in any one contactor as well as provide added research flexibility to the system. An E-stop activation will also remove high voltage power to each motor / motor controller propulsor at the branch and each dynamometer, thereby cutting off all power to all power sinks.

The NASA team decided that the E-stop system on HEIST would only remove the traction power (high voltage and high current) from the system and not the logic power to the motor controllers or the excitation power to the sensors. This decision was driven by the requirement that HEIST be able to work with a variety of components, and not all controllers maintain known states when logic power is removed during operation. In an emergency, human safety is the primary concern, but if the hardware can be salvaged, it can provide important data that may be helpful in determining the condition that led to the emergency, so that it may prevent it in the future. Additionally, the project chose not to remove power from sensors, as the data can provide real time information on the state of the system during a hazard condition.

As a reactive system, the primary function of the E-stop circuit is the ability to safely load-break all power sources and loads operating at maximum power and quickly bring the 100 VDC or 325 VDC power system to an inactive

state. This process must be accomplished with a single human action, not in a series of steps, and it should not impair the effectiveness of other safety devices while being as simple as possible. The more components in the circuit, the more difficulty in troubleshooting, and more points of failure are present.

The HEIST team endeavored to remove all possible single-point failures in the E-stop design, requiring redundancy of the E-stop power contactors, as historically these systems can react in unpredictable ways. The current HEIST configuration is a 200 kW system operating at 100 VDC. In subsequent phases, testing at higher voltages from 325-400 VDC will be completed, and in later phases, there is the possibility of testing AC systems and doubly-fed induction motors which operate at higher frequencies. While these AC systems are not priorities at this moment, the HEIST team has considered them as it is more economical and easier to design in the functionality early than to modify it later. Since HEIST operates at the 100 VDC for the initial phases, the current at 100 VDC will be much higher than during all subsequent phases and operating ranges, therefore the system will get more current margin as the project matures. All component sizing and selections were based on this configuration; however, the physical system layout was designed to allow for quick substitution of various safety devices such as fuses.

The E-stop circuit itself consists of two E-stop buttons in series controlling the excitation power to a contactor. The local E-stop button is a standard red mushroom button connected with copper cable. As HEIST is a mobile testbed potentially hundreds of feet from the control room where HEIST will be controlled, there were concerns of cable length limitations due to voltage drop on the E-stop circuit. To address this issue, the HEIST team incorporated a fiber optic E-stop design which provides greater flexibility in operating locations without compromising safety. The load side of the contactor passes the 24 VDC excitation power to all of the power contactors throughout HEIST from a 24 VDC 100 A power supply that is dedicated to the E-stop circuit and the contactors. When either E-stop button is pressed, the contactor opens and removes all excitation power from the power contactors. While the total power consumption of all contactors and E-stop is less than 40 A, well within the capabilities of the power supply, it was decided that in order to mitigate risk, no non-safety related components would be connected to this circuit. This decision also provided additional benefit for future expansion and ease of troubleshooting. The contactors and E-stop buttons selected are normally open in their non-energized state. This distinction was chosen so that in the event of any failure, from broken wires to damaged coils, the system would not inadvertently activate.

While effective, the E-stop system is not the only hazard mitigation employed. The HEIST testbed also includes manual disconnects to physically disconnect motors and motor controllers from the traction power bus before technicians work on the system. Inside each battery box, the AC/DC converter, turbogenerator, and fuse box include dead facing contactors which remotely isolate power from the all feed-throughs to avoid inadvertent contact between personnel and live circuits. Redundant contactors were chosen for the power system, in essence it would require five separate contactors to fail in series to allow a power source to connect to any motor. The battery boxes have their own safety considerations which include disconnect switches between sections, fusing, and cell segregation as well as cell voltage and temperature monitoring in the battery management system (BMS).

In addition to addressing hazards present during expected use cases, designing for safety also entails preventing hazards caused by failure modes. Effects stemming from failure modes should be examined to identify conditions which are hazardous to personnel or equipment. Safe recovery states should be identifiable for each hazardous condition. The system should then be configured to default to these safe states in the event of a failure, and preferably be implemented through hardware means. It is entirely possible for there to not be any overall system configuration that addresses all possible hazardous failure modes and effects. In such an event, the configuration which addresses as many personnel hazards as possible should be selected, with the remaining hazardous effects addressed through separate mitigations.

Several of HEIST testbed hazards are introduced as a side-effect of being a remotely-controlled system. The root source of those hazards stem from the potential failure of the additional command, control, and communication nodes required, as well as the connecting communication links. Since these hazards stem from anomalous conditions, failure mode analysis is invaluable.

Some of the results and mitigations from failure mode and analysis (FMEA) of the HEIST testbed control system are of trivial ease, albeit significant impact. For example, see the diagram of the HEIST reflective memory network topology in Fig. 4. The local network of the HEIST testbed consists of two groups of two nodes in close proximity each, with the groups separated by a large distance. Failures in the HEIST communication network could result in a loss of high-rate telemetry, or a loss of control of relays, the turbo-electric power system, and the dynamometers. These failures could hinder the ability to detect and respond to conditions hazardous to system health. The most relevant failure mechanisms of small networks with a low bandwidth utilization are either failure of relaying network nodes, whether that be by being merely unresponsive or actually dropping off the network because of power loss or hardware failure, or failure of the transmission line itself. Analysis was conducted to identify if any components could become isolated due to a single failure of one or more additional nodes from the network, and thus result in loss of

control and/or telemetry for all other nodes. The redundant ring topology was the best choice for the HEIST communication network, reducing network drop-out due to isolated nodes, but the transmission cable remains a single-point failure risk. Therefore, it highlights the need for additional mitigations, such as armored cables.

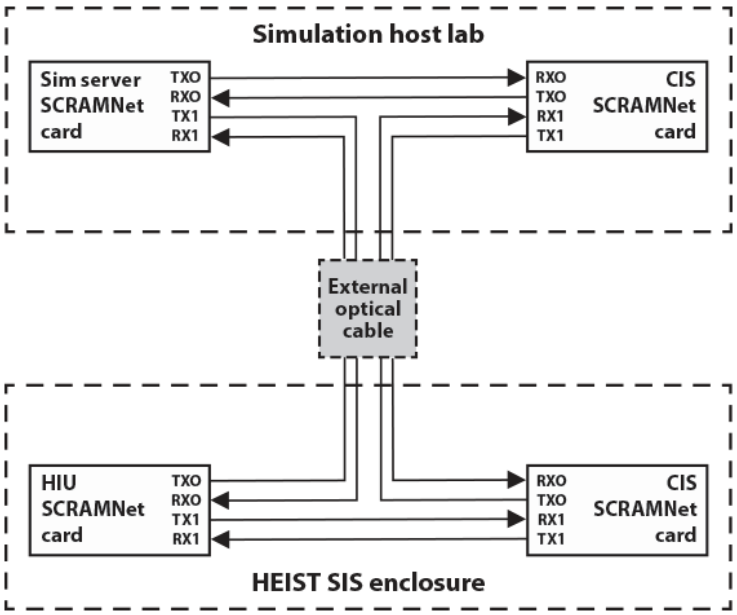


Figure 4. Redundant-ring network topology.

A FMEA should be conducted for both nominal and off-nominal operations, as well as system startup and shutdown. The behavior of some contactor relays, pre-charge circuitry, and other high-power hardware may be different for a hard shutdown versus a systematic, nominal shutdown. The failure modes analysis should also focus on how the system, including the high-power hardware, respond to a hard restart, ensuring that no additional hazards, specifically human hazards, are created for these off-nominal events. An example being the determination of the default states of the relays controlling the motor controller logic supply power. The design choice accounted for two types of failure cases: the first case where the hardware interface unit (HIU, the embedded system controlling relays) resets unexpectedly or fails completely during any operational state, and the second case where the E-stop is activated during any operational state. What happens after failure? What happens after normal operation is restored? Analysis of these cases can be reduced to just considering what the effects are of introducing or removing interruptions in logic power on the two power input interfaces (i.e. logic power in, traction power in) to the motor controller, during each operational state (uncharged, ready, and running loaded). Analysis of the particular motor controllers used by HEIST suggests that suddenly removing traction power when running at full load, in the absence of commands to throttle down, may result in equipment damage, because the controllers attempt to maintain the previous revolutions per minute (RPM). Having the logic power relays fail open will power down the controller along with the traction power contactors in the event of an HIU failure, albeit at the cost of losing command and telemetry of all motor controllers via the controller area network bus (CANBus). This failure is deemed an acceptable risk, since failure of the HIU automatically ends the test and motors spinning down to a stop by free-running is a safe condition as long as the propeller keep-out zone has been utilized.

IV. Designing for Safety of Remotely-Commanded, High Power Electric Propulsion Testbeds

This section will identify and provide operational considerations for high-voltage electric distributed propulsion testbeds. As shown in Table 3, there are numerous hazards associated with these systems. This section will provide some examples of sound practices in programming remotely commanded systems.

The first principle one should follow when designing remotely-operated systems for safety is to check inputs, such as commands and initial configurations, for correctness and reject incorrect inputs. A high-speed data recorder (HSDR) was used to capture sensor data at much higher frequencies (greater than 4 kHz) than the deterministic simulator computer system runs on (200 Hz). High speed data are sampled at 200 Hz and fed back into the simulator computer

by the HIU. The HSDR and HIU both check command inputs to verify legal values; commands with illegal values or commands not applicable to the current operating mode are ignored. Another example of this principle in the HEIST testbed design occurred during the initial configuration of these systems. Before applying a configuration loaded from disk during initialization, the loaded configuration should be checked for proper formatting and valid values. This implementation is a means of preventing un-commanded system operation or operation outside of prescribed limits.

Utilizing the design approach for desired end-state command as opposed to toggle command is another safety design consideration. An example is the contactor relay Boolean command. A toggle command would be interpreted by the relay to switch positions (go from closed to open or open to closed). This methodology can provide issues and potentially unsafe conditions if the command frequency and the switching frequency are staggered or out of phase. A toggle command may be interpreted a time-step after it was intended, with a command for the reverse toggle still waiting. In order to maintain situational awareness, a return sensor would be needed to identify the position of the relay. Instead, commanding from desired end-state eliminates any issue with system frequency mismatches. If the end-state is desired to be open, the system will open (whether it is already or not). This implementation is a means of preventing un-commanded system operation.

Another good practice in designing remotely-controlled targets is to have both received and implemented commands returned to the master as feedback. Both the HIU and the HSDR repeat back the commands they receive for a given iteration, in conjunction with reporting back the commands they will actually be implementing. There are several reasons for this implementation:

1) It provides acknowledgement that commands were received and confirms the data integrity of the commands so errors in the received message will be immediately identifiable.
2) It validates the command against any differences in command returns.

Another safety design approach is to actively search for both hardware and software faults, and have a means of correcting at least the minor ones short of halting operations or performing a full system reset. Utilizing heartbeat counters to reflective memory allows for all nodes in the memory ring to monitor the status of each other node.

It is vital that all software and hardware be initialized to a safe, known state. Both the HIU and the HSDR start their hardware and software in a known inactive safe state following initialization, and remain waiting in these passive states until actively ordered to do otherwise via a valid, correctly formatted command. These considerations ensure that HIU and HSDR are in a state which ensures health, without human intervention, even if faults have occurred. Furthermore, these systems have safe states which they can default to during normal operations in the case of faults, providing a method of fault recovery short of full system reset. These implementations increase system robustness and operational flexibility. This implementation is a means of preventing un-commanded system operation.

V. Conclusion

Personnel safety is the primary consideration in safety system design. Safety system design must be introduced at the beginning of the project and mature throughout the design, fabrication, testing, and operations. The National Aeronautics and Space Administration Armstrong Flight Research Center utilizes a safety process illustrated in Section II that addresses the project hazards, their specific causes, effects, severity and probability for human and asset damage, and mitigations. The traction bus failure hazard was specifically identified as a common hazard amongst the various electric / hybrid-electric projects. This paper addressed several safety design considerations, including the E-stop system which is a mitigation for almost all hazards, not by eliminating the causes of the hazards, but by reducing the severity of the effects. If it is not possible or feasible to completely eliminate a hazard in the design process, it is important to understand how to reduce the frequency of exposure to the hazard by personnel and/or reduce the magnitude/severity of the hazard exposure. Safety design, procedural steps, safety equipment, and vigilance in operations play a significant part in hazard mitigation. Taking this proactive approach allows designers to manage hazards throughout the project life cycle by improving their ability to make risk-informed decisions.

References

[1]National Aeronautics and Space Administration, *NASA Aeronautics Strategic Implementation Plan*, NP-2015-03-1479-HQ, National Aeronautics and Space Administration, Washington, DC, 2015.

[2]Clarke, S., Redifer, M., Papathakis, K., Samuel, A., and Foster F., "X-57 Power and Command System Design," ITEC2017.1090, 2017.

[3]Papathakis, K., Kloesel, K., Lin, Y., Clarke, S., Ediger, J., and Ginn, S., "Design and Development of a 200-kW Turbo-electric Distributed Propulsion Testbed," AIAA-2016-4611, 2016.

[4]National Aeronautics and Space Administration, *Hazard Management Procedure*, DCP-S-002, Rev. E-2, National Aeronautics and Space Administration Armstrong Flight Research Center, Edwards, California, Expires March 21, 2021.

[5]National Aeronautics and Space Administration, *General Safety Program Requirements*, NPR 8715.3C, National Aeronautics and Space Administration, Washington, DC, 2008.

[6]Federal Aviation Administration, *Title 14 of the Code of Federal Regulations, Chapter 1, Subchapter C, Part 25: Airworthiness Standards: Transport Category Airplanes*, URL: http://www.faa.gov [cited 12 May 2017].

[7]Moore, M., Clarke, S., Stoll, A., Clark A., MacAfee S., and Foster, T., "Affordable Flight Testing of LEAPTech Distributed Electric Propulsion," *Proceedings of the NASA Aeronautics Research Institute, NASA Aeronautics Research Mission Directorate (ARMD) 2015 LEARN/Seedling Technical Seminar*, Washington DC, January 13-15, 2015.