



National Aeronautics and
Space Administration

NASA Ames Research Center

Advanced Diagnostics and Prognostics Testbed (ADAPT)

System Description, Operations, and Safety Manual

Signature Page

Norm Picker, System Safety Representative
Occupational Safety, Health & Medical Services Division

Date

Shawn Puma, System Safety Representative
Occupational Safety, Health & Medical Services Division

Date

Scott Poll, ADAPT manager
Intelligent Systems Division

Date

Ann Patterson-Hine, Health Management Systems Lead
Intelligent Systems Division

Date

Joe Camisa, Primary ADAPT electrician
Project Development Division

Date

Revision History

Date	Revision	Description	Author

TABLE OF CONTENTS:

1. Introduction.....	1
2. Overview.....	1
2.1 Goals.....	1
2.2 Concept of Operations.....	2
2.3 Lab Layout.....	2
3. Systems Description.....	3
3.1 Power Generation.....	4
3.2 Power Storage.....	5
3.3 Power Distribution.....	6
3.4 Power Monitoring.....	8
3.5 Data Acquisition and Control.....	9
3.6 Computer Configuration.....	9
3.7 Computer Software.....	10
3.7.1 Operating System.....	10
3.7.2 Software.....	11
3.7.3 Configuration File.....	11
3.7.4 Data and Command Transmission.....	11
3.8 Software Architecture.....	11
3.9 Health Management Application.....	14
3.10 Fault Injection List.....	14
4. Systems Operations.....	15
4.1 Operational Modes.....	15
4.2 Operational Procedures.....	16
4.2.1 Computer Startup and Shutdown.....	16
4.2.2 HyDE Startup.....	16
4.2.3 Operator Stations.....	16
4.2.4 Emergency Stop.....	16
4.2.5 Manual Fault Injection.....	16
5. ADAPT Safety Considerations.....	16
5.1 Required Electrical Safety Training.....	16
5.2 De-energized Electrical Work and Lockout/Tagout.....	17
5.3 Energized Electrical Work / Manual Fault Injection.....	17
5.3.1 Personal Protective Equipment.....	17
5.3.2 Equipment Design, Labeling, Lab Setup, Tools, and Procedures.....	18
6. ADAPT Electrical Diagrams, Equipment Specifications, I/O List.....	19
Appendix A Acronyms.....	23
Appendix B Software Configuration File.....	24
Appendix C DataSockets Protocol.....	27
Appendix D Fault Injection List.....	30
1. Faults currently implemented.....	31
1.1 Circuit Breaker Tripped.....	31
1.2 Relay Failed Open.....	32
1.3 Relay Failed Closed.....	33

1.4	Relay Overheating	33
1.5	Sensor Shorted	34
1.6	Sensor Open Circuit.....	35
1.7	Sensor Stuck.....	36
1.8	AC Inverter Failed	36
1.9	Solar Array blocked	37
2.	Faults Under Consideration	37
2.1	Destructive testing	37
2.2	Sensor Out of Calibration	38
2.3	Battery Charger Failed.....	38
2.4	Photovoltaic Charger Failed	39
2.5	Battery Overheating.....	39
2.6	Battery Overcharged.....	39
2.7	Excessive Sensor Noise	40
2.8	Broken Wire.....	40
2.9	Faults in Loads.....	41
Appendix E	Computer Startup and Shutdown Procedures	42
Appendix F	HyDE Startup Procedure.....	44
Appendix G	Operator Station Procedures	45
Appendix H	Emergency Stop Procedures	49
Appendix I	Training Record	50
Appendix J	Lockout/Tagout Procedure.....	51
Appendix K	Personal Protective Equipment Requirements.....	53
Appendix L	Material Safety Data Sheet for Batteries	54
Appendix M	Manual Fault Injection General Safety Procedures	55
I)	Antagonist Safety Procedures for Manual Fault Injection.....	55
II)	User Safety Procedures for Hard Fault Recovery.....	56
III)	Observer Safety Procedures.....	56
Appendix N	Releasing a Victim of Electrical Shock	58
Appendix O	ADAPT Electrical Drawings, Equipment Specifications, I/O List.....	61

LIST OF FIGURES:

Figure 1. ADAPT Lab Layout.	3
Figure 2. ADAPT EPS equipment racks 1, 2, and 3.	4
Figure 3. Solar panel assembly.	5
Figure 4. Battery chargers 1 and 2.	5
Figure 5. Battery cabinet.	6
Figure 6. Electro-mechanical relays for switching loads.	7
Figure 7. Inverter panel.	7
Figure 8. Load banks 1 and 2 receptacle panel.	8
Figure 9. Current transducers for loads.	8
Figure 10. National Instruments Compact FieldPoint backplane.	9
Figure 11. National Instruments Compact FieldPoint (cFP) modules.	9
Figure 12. Computer configuration.	10
Figure 13. Build 1 software architecture.	11
Figure 14. Data acquisition functions and interfaces.	12
Figure 15. Antagonist functions and interfaces.	12
Figure 16. Avionics functions and interfaces.	13
Figure 17. User functions and interfaces.	13
Figure 18. Observer functions and interfaces.	14

1. Introduction

This document describes how to safely operate the Advanced Diagnostics and Prognostics Testbed (ADAPT). Required safety equipment, procedures, and training are listed. Also included are hardware and software procedures for facility startup, shutdown, nominal operations, and error recovery. The goals, unique concept of operations of ADAPT, lab layout, and descriptions of the hardware and software systems are given. Electrical drawings and equipment specifications are included as appendices. This document shall be located in the ADAPT lab for reference and shall be updated as changes are made to the testbed or as it is determined that procedures or other documentation should be modified. In addition, important safety information shall be posted prominently in the lab to notify personnel of potential dangers and to instruct on what to do in an emergency situation.

2. Overview

The following sections discuss the goals of the testbed, the unique concept of operations, and the lab layout.

2.1 Goals

Health management concepts and technologies are playing a critical role in the new vision for space exploration. While much of the current troubleshooting for crewed systems is done on the ground with a standing army of experts, as humans venture farther out of low earth orbit it becomes important to migrate that health management functionality to the crewed system itself so that the safety of the crew and the likelihood of mission success are not adversely impacted by the increasing delays of communications with earth. This will also lead to more sustainable and cost effective operations. In order to achieve this migration of functionality it is necessary to understand and mature the health management technologies that will be employed for exploration vehicles and habitats – this is the intended role of the testbed. It is important to note that the applicability of health management technologies is not limited to crewed systems, any complex engineering system is likely to show improvements in affordability, reliability, and effectiveness by the incorporation of health management concepts and technologies.

The purposes of the testbed are to test, measure, and evaluate diagnostic and health management technologies. More explicitly, the goals are to entail:

- Performance assessment of diagnostic tools and algorithms against a standardized testbed and repeatable failure scenarios.
- Development of prognostic models (performance degradation, remaining life estimation) for spacecraft Electrical Power System (EPS) and Guidance Navigation and Control (GNC) components.
- Development platform for Advanced Caution and Warning (ACW) methods.

The testbed provides a controlled environment to inject failures, either through software or hardware, in a repeatable manner. This will facilitate assessing the effectiveness of the technologies in terms of Figures of Merit (FOM) and Technical Performance Metrics (TPM). The intent is to characterize which technologies are most appropriate for various types of faults and situational contexts. The testbed will also investigate how health management concepts work

in emulated operational scenarios to discover any obstacles to implementation and to demonstrate effective human-machine interactions.

2.2 Concept of Operations

Unlike many testbeds, the primary articles under test are the health management applications, not the physical devices for which they are implemented. In order to operate the testbed in a way that facilitates characterizing the health management technology, three operator roles are defined:

- **User** – who simulates the role of a crew member operating and maintaining the testbed subsystems.
- **Antagonist** – who injects faults into the subsystem either manually, remotely through the Antagonist console, or automatically through software scripts.
- **Observer** – who records the initiation of the faults and resulting detection and remediation or lack thereof. The Observer also serves as the safety officer during all tests.

In addition to the roles above, during some tests there may be persons watching and participating in the demo, e.g., visiting dignitaries, engineering, crew or industry representatives, or technology developers. These persons shall be referred to as the **Audience**. Audience members may participate in the demos only under the direct supervision of a trained operator, as described in section 5.1 and as indicated in Appendix I. Under no circumstances, is an Audience member allowed to perform manual fault injection.

The ADAPT facility may be one piece of a larger simulation infrastructure. For example, other testbeds may be connected through the internet to provide a more complete vehicle simulation or to enable a more thorough analysis of human-machine interaction. It is also possible to expand the scope of ADAPT in the future to include more than the EPS that is currently implemented.

2.3 Lab Layout

A schematic of the lab is shown in Figure 1. The locations of the operators' consoles are indicated. Note that the observer console is located in a position to view both the antagonist and user console positions. A description of the testbed hardware, software, and safety equipment is given in subsequent sections.

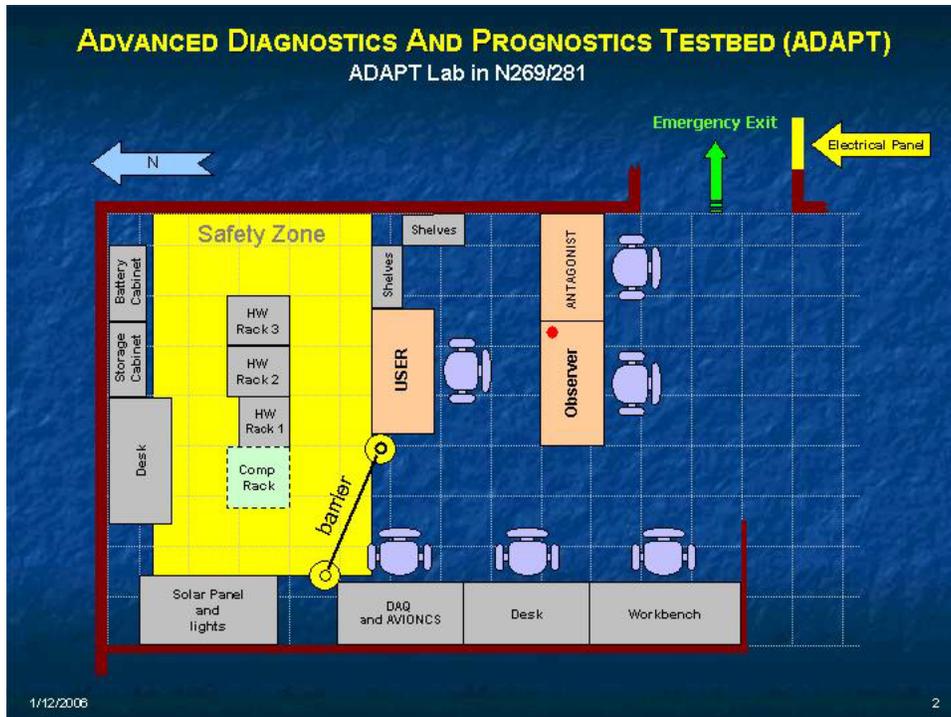


Figure 1. ADAPT Lab Layout.

3. Systems Description

The initial build of the testbed consists of an electrical power system that is functionally representative of an EPS in a space exploration vehicle. It was designed and built by the Electronics and Controls Branch (Code PMC) at NASA Ames Research Center. The EPS consists of three physical units: controller, battery cabinet, and solar panel unit. The controller is composed of three racks of equipment: power generation unit, power storage unit and power distribution unit. The racks are shown in Figure 2. Overall system diagrams are Power Subsystem One Line: A269-0500-E1, Process and Instrumentation Diagram: A269-0500-M1, and Elementary Diagram: A269-0599-E2; details of the racks with a panel-by-panel description are given in Appendix O.

The functions provided by the EPS include power generation, storage, distribution, and monitoring. The EPS provides 24 VDC and inverters for 120 VAC to power two load banks, which may represent subsystems such as propulsion, life support, thermal management systems, avionics, etc. Additionally, the EPS provides the capability to switch charging, power sources, and loads. A data acquisition system allows an operator to monitor and control the testbed. An emergency stop may be performed with either a manual or a software ESTOP button. The testbed operator stations are integrated into a software architecture that allows for nominal and failure operations of the EPS, including logging of all relevant data in order to assess the performance of the health management applications. In the initial build, the model-based reasoner HyDE (Hybrid Diagnostic Engine) serves as the health management application.

The following sections describe the EPS functions, the operator station computers and software architecture, the health management application, and the faults that may be injected into the testbed.

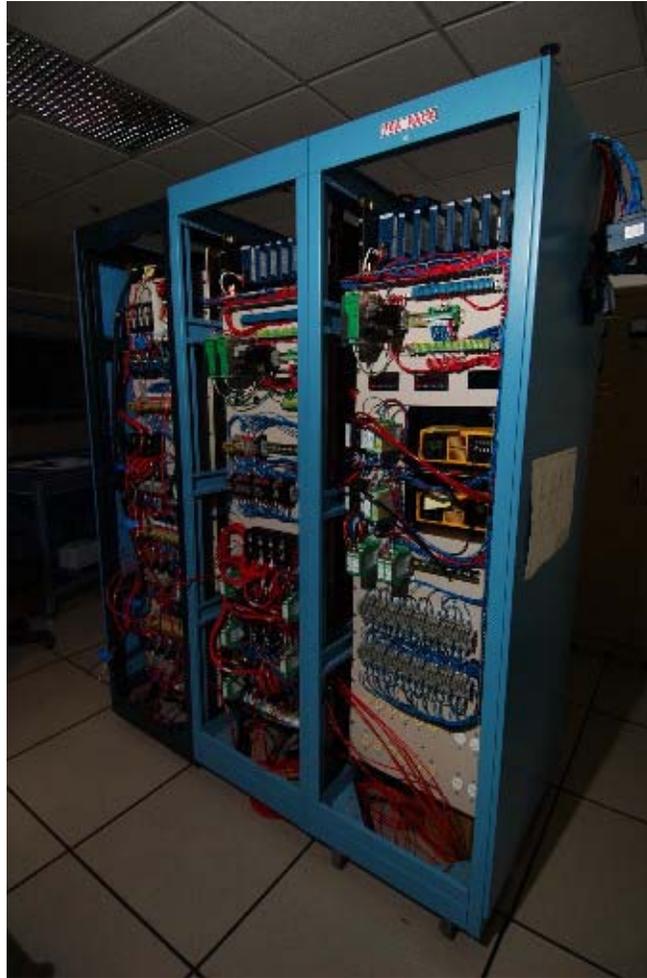


Figure 2. ADAPT EPS equipment racks 1, 2, and 3.

3.1 Power Generation

The power generation equipment of the testbed provides charging to the three sets of 24 VDC batteries. There are three sources for charging the batteries: the solar panels in conjunction with a charge controller, and two 24VDC, 20 amp battery charges that are powered by utility power. The solar panel assembly is shown in Figure 3, and the battery charges in Figure 4. Since there is no sunlight in the lab, the sources of energy for the solar panels are two controlled metal halide lamps. When the solar panels are used to charge the batteries, a charge controller monitors and regulates the amount of current that is delivered to the batteries. When the batteries are fully charged, the regulator shuts off the current. When utility power is used to charge the batteries, battery chargers are used to control the current. The data acquisition and control (DAC) unit provides the commands to switch any one of the three charging sources to charge any one of the three 24 VDC batteries. There is relay protective logic to prevent two charging sources from charging a single battery and also to prevent one charger's charging circuit from being connected

to another charger's charging circuit. Nominally, the equipment in rack 1 corresponds to the power generation function.



Figure 3. Solar panel assembly.



Figure 4. Battery chargers 1 and 2.

3.2 Power Storage

Three sets of 24VDC 100 Amp-Hr sealed lead acid batteries (two 12 volt batteries connected in series) are used to store energy. The battery specifications are given in Appendix O. They require no maintenance, very little ventilation, and can be positioned in any fashion. Figure 5 shows the batteries mounted in a cabinet in the northeast corner of the lab. Nominally, the equipment in rack 2 together with the battery cabinet corresponds to the power storage function.



Figure 5. Battery cabinet.

3.3 Power Distribution

The power distribution to AC and DC loads is accomplished with solid state and electro-mechanical relays. Electro-mechanical relays for load banks 1 and 2 are shown in Figure 6. The solid state and electro-mechanical relays are all normally open (N.O.). All relay control power is from a separate DC power supply energized by utility power. During nominal operations, the User controls the relays. During failure operations, the Antagonist controls the relays. Each load bank has an inverter panel, shown in Figure 7, to convert 24 VDC to 120 VAC. Currently, there is provision for 2 DC loads and 6 AC loads for each load bank, as shown in Figure 8. Nominally, the equipment in rack 3 corresponds to the power distribution function.

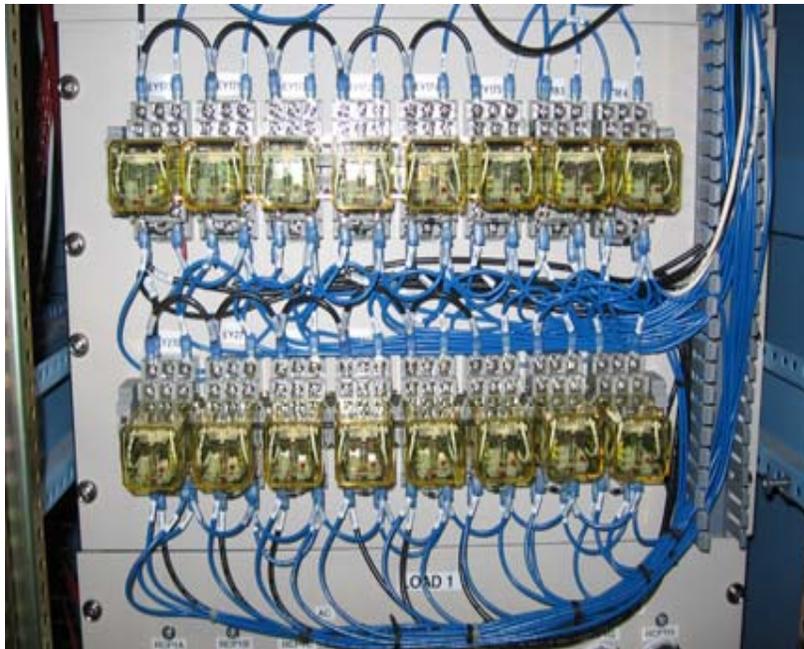


Figure 6. Electro-mechanical relays for switching loads.



Figure 7. Inverter panel.



Figure 8. Load banks 1 and 2 receptacle panel.

3.4 Power Monitoring

The testbed is outfitted with numerous voltage, current, and temperature sensors to monitor the health of the EPS. The voltage sensors are measuring the voltages upstream of the main battery relays, downstream of each battery circuit breaker, and in both load banks. Additionally, the solar panel voltage and charge controller input and output voltages are measured. The current sensors use non-intrusive magnetic pick up Hall Effect sensors for isolation from the circuit components, thereby reducing the chance for sensors to cause errors or induce failures. The current sensors are monitoring charging current to the batteries and the discharge currents from them. Figure 9 shows the current sensors for the AC and DC circuits of the two load banks. Thermal sensors are attached to the solar cell, the batteries, and the solid state relays. The solar photovoltaic cells have light measuring sensors as well. Circuit breakers are in series with the voltage supply and the loads to open the circuit and protect over-currents due to shorted conditions.

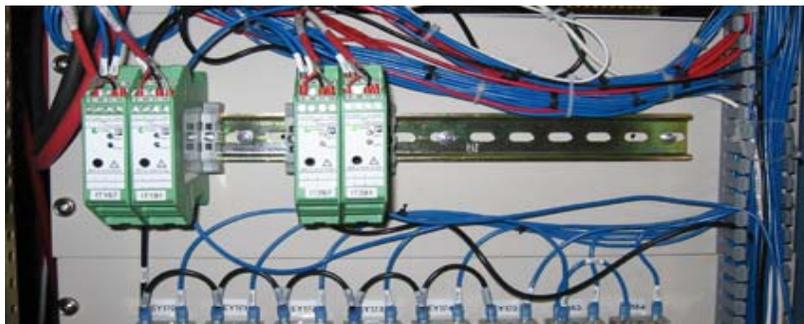


Figure 9. Current transducers for loads.

3.5 Data Acquisition and Control

National Instrument's LabVIEW software and Compact FieldPoint hardware are used for controlling the testbed and acquiring testbed data. Figure 10 shows one of the two Compact FieldPoint backplanes. Figure 11 depicts the module designations in the Compact FieldPoint and Appendix O lists the I/O channels. Each backplane has 8 I/O modules, 8 connector blocks (1 per I/O module) and one real-time controller.



Figure 10. National Instruments Compact FieldPoint backplane.

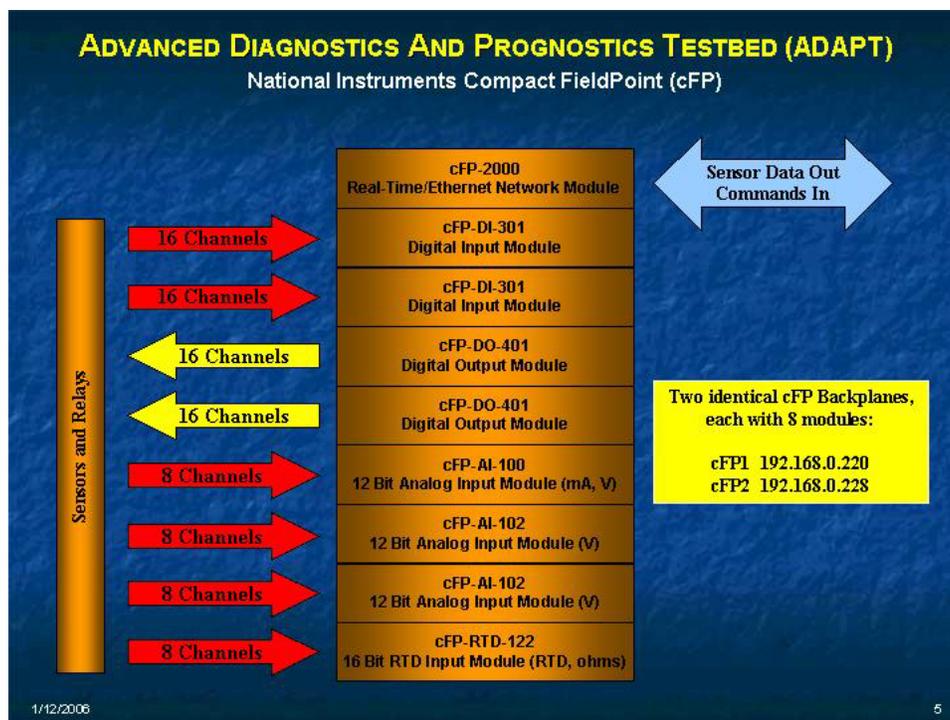


Figure 11. National Instruments Compact FieldPoint (cFP) modules.

3.6 Computer Configuration

There are five computers networked together via an Ethernet switch, as shown in Figure 12. These are:

- Data Acquisition (DAQ) – interface to the sixteen Compact FieldPoint (cFP) modules. Retrieves sensor measurements and packages the data into a double precision array for transmission. Receives relay/switch commands and sends them to the appropriate cFP module.
- Antagonist (ANT) – allows software injection of faults via data “spoofing” (substituting values) or command interception.
- Avionics (AVI) – residence of the “Test Article” or health management application.
- User (USR) – main testbed control. The User station has full control of the relays and switches that control the testbed.
- Observer/Logger (LOG) – monitors all DataSocket points, and logs data and commands to files when an experiment is run. Has no ability to affect testbed operations directly.

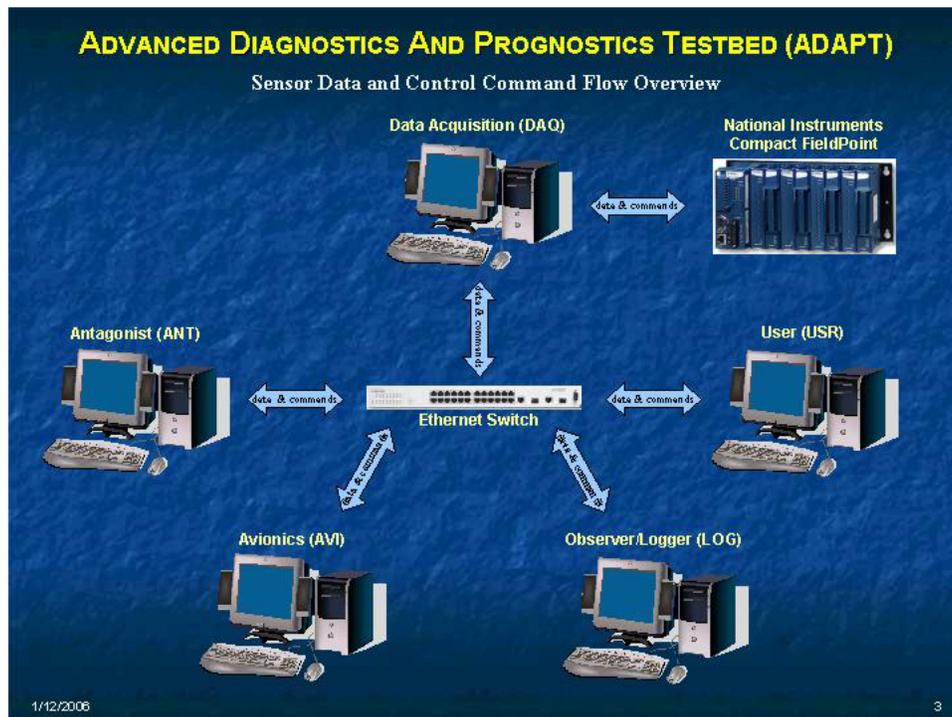


Figure 12. Computer configuration.

3.7 Computer Software

3.7.1 Operating System

DAQ and AVI run under Windows 2000; the others run under Windows XP Professional.

3.7.2 Software

All of the software except for the test article interface were developed under the National Instruments LabVIEW Professional Development System, version 7.1. The test article interface was developed under Microsoft C/C++.

3.7.3 Configuration File

The configuration file **C:\ADAPT\Config\config.txt** is used by all of the ADAPT computers. The configuration file contains information that enables the computer nodes to communicate with each other, and should only be modified by authorized software personnel. The configuration file is listed in Appendix B.

3.7.4 Data and Command Transmission

Sensor data, control commands, diagnostic messages, and general messages are passed between computers using National Instrument's DataSocket. DataSocket communications, based on TCP/IP, allows simple data connections between computers. A DataSocket server runs on each machine, with publisher or reader clients. The format of the protocol is given in Appendix C.

3.8 Software Architecture

The Build 1 software architecture is depicted in Figure 13. As previously mentioned, a separate computer is used for each of the functions encapsulated by the larger rectangles (DAQ, ANT, AVI, USR, LOG). The functions and interfaces of each of the computers are shown in subsequent figures.

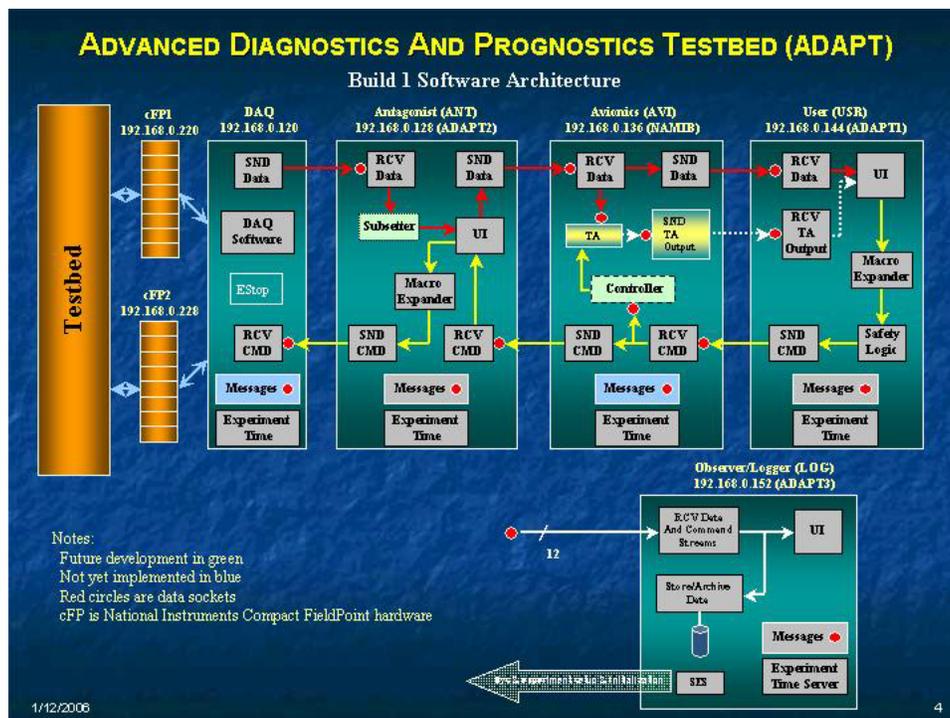


Figure 13. Build 1 software architecture.

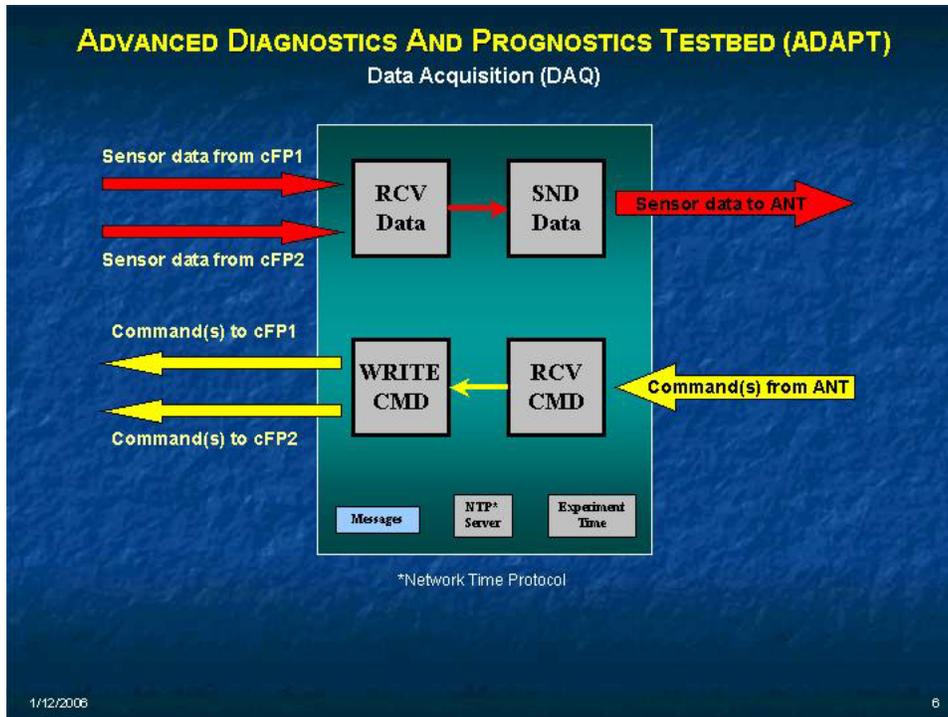


Figure 14. Data acquisition functions and interfaces.

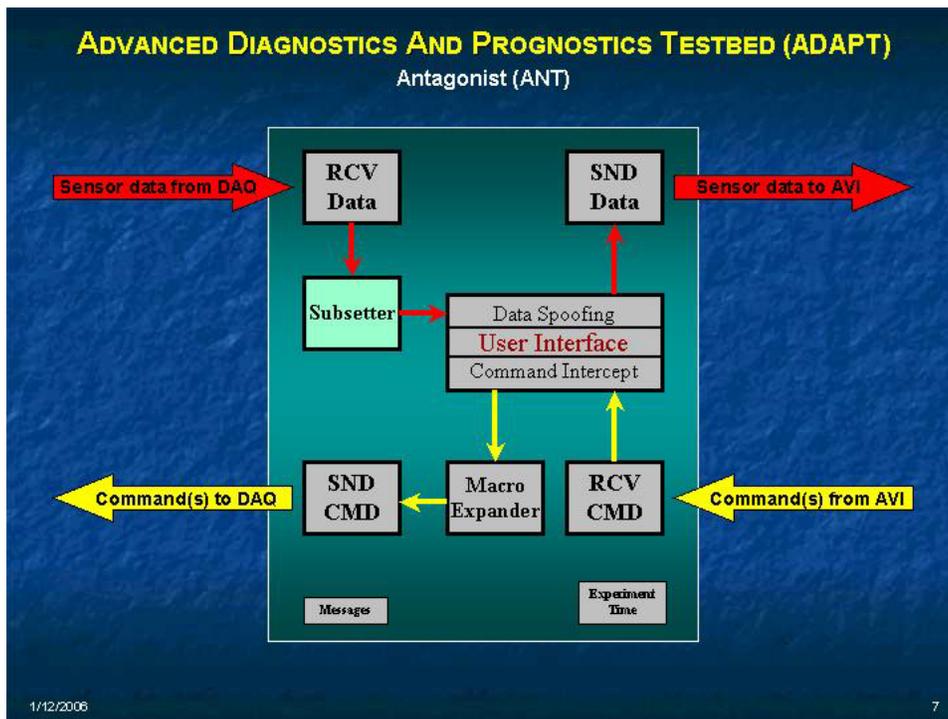


Figure 15. Antagonist functions and interfaces.

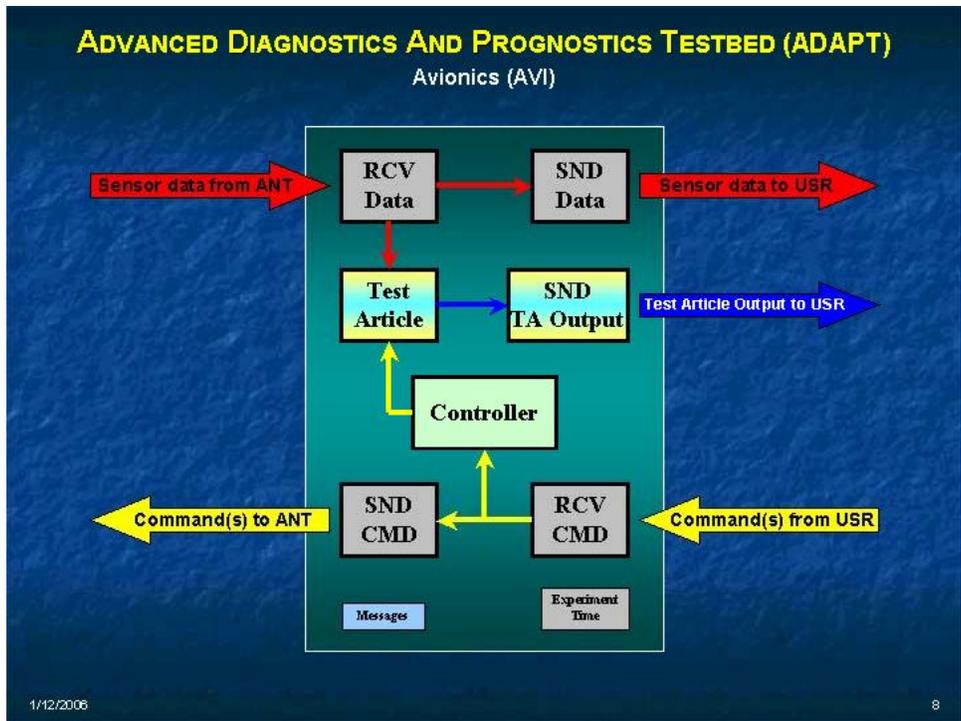


Figure 16. Avionics functions and interfaces.

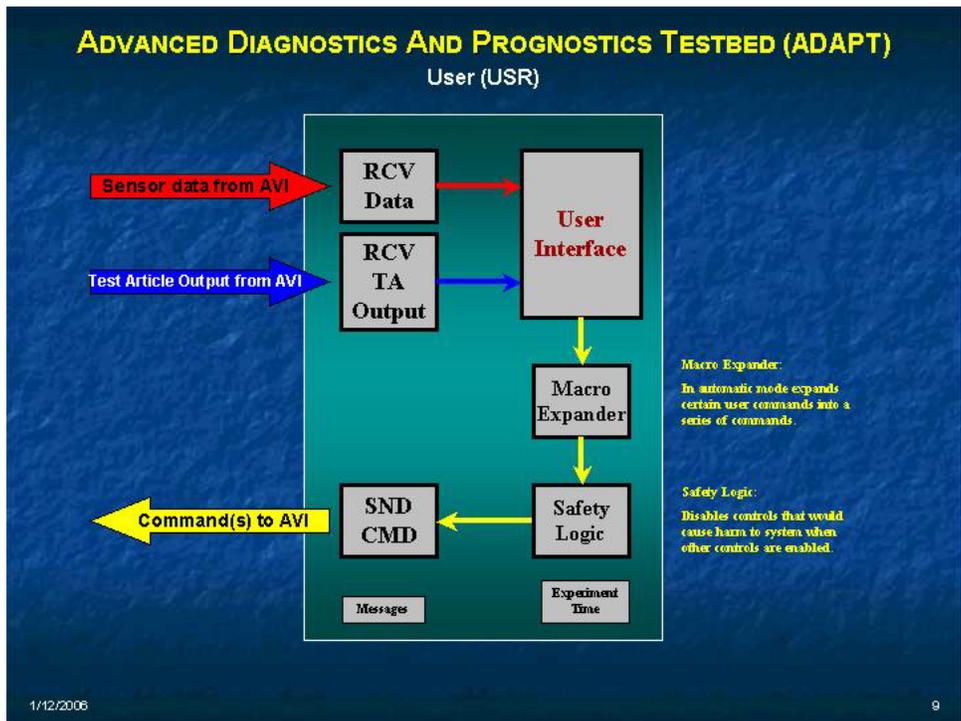


Figure 17. User functions and interfaces.

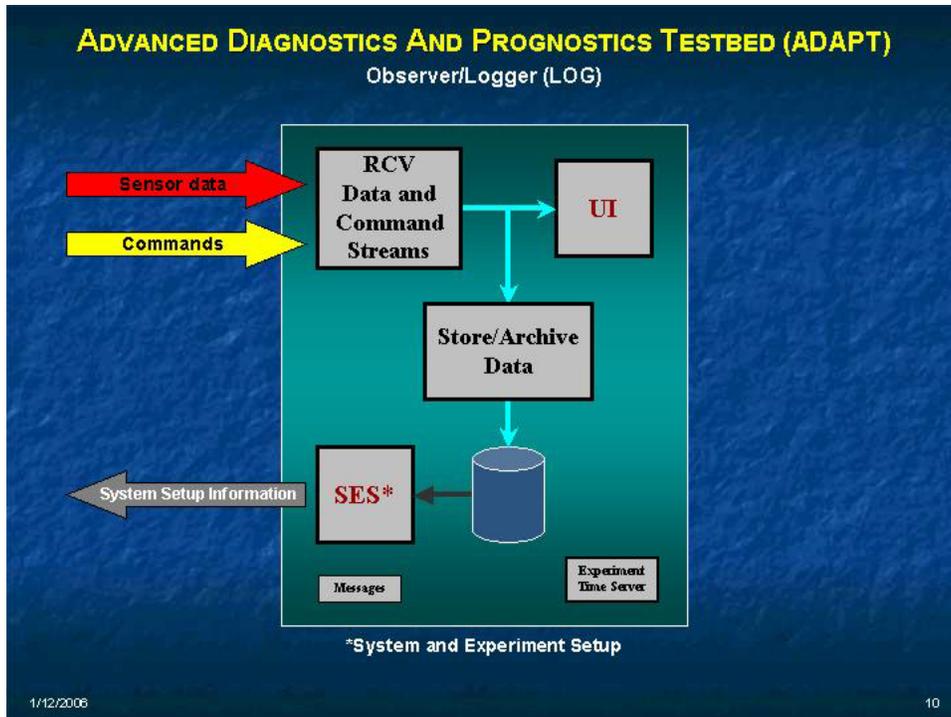


Figure 18. Observer functions and interfaces.

3.9 Health Management Application

The health management application deployed in Build 1 is the Hybrid Diagnostic Engine (HyDE), developed at NASA Ames Research Center. HyDE is a model-based software tool for diagnosing systems. It provides online system mode tracking, fault detection and fault isolation to the component level. HyDE itself is a general inference engine: it is adapted to specific systems by loading a model of the system. It is similar in that respect to its predecessor, Livingstone 2, and incorporates some of the same search algorithms. However, Livingstone can only accept discrete system models, and HyDE has the additional capability to accept real-valued and interval-valued system models. Other capabilities include modeling differential equations, differential inclusions, and tracking with kalman filters and particle filters.

In future efforts health management applications from industry, academia, and government employing different techniques will be integrated and tested. It is anticipated that these technologies will exhibit different strengths and weaknesses that will need to be considered when constructing a health management solution for a particular system.

3.10 Fault Injection List

Faults may be injected into the testbed in a repeatable manner via software or hardware in order to assess the performance of the health management applications. The faults may be of the continuous and/or discrete type with different timescales. A description of the faults currently implemented and faults under consideration are given in Appendix D.

4. Systems Operations

4.1 Operational Modes

The operational modes of the EPS are determined by how the power subsystem is being used. There are fundamentally two types of operating modes, baseline normal operational modes that render nominal data, and failure operational modes that render data different from nominal. It is conceivable that the number of operational failure modes can be based on the number of failures that have occurred at a given time, as well as the types of failures that are occurring, thereby generating a very large number of failure operational modes. This is good for demonstrating failure ambiguity, fault group size detection and isolation capability. External breakage (real hardware failures) or failures generated by a person (manual failures) on the EPS can be used for demonstration. They are naturally unpredictable types of failures. However, these failures should be repairable and realistically represent failures that do occur or can occur on a crewed exploration vehicle.

There are five main baseline (no failures) EPS operational modes. The states of the solid state and electromechanical relays will dictate the EPS state/operational mode. The ADAPT EPS system modes include the following:

- 1) Offline:
 - The Observer, Antagonist, User, DAQ, and Avionics computers are getting power but may not be turned on.
 - Battery cabinet circuit breakers are open (tripped).
- 2) Standby:
 - The computer startup procedures in Appendix E have been completed.
 - Battery cabinet circuit breakers are closed (not tripped).
 - Emergency stop is armed.
- 3) Battery Charging:
 - Solar array lamps on and relays configured to charge any one of battery 1, 2, or 3 from solar array/charge control regulator.
 - or
 - Relays configured for either battery charger 1 or battery charger 2 to charge any one of batteries 1, 2, or 3.
 - or
 - Relays configured for both battery charger 1 and battery charger 2 to charge any two of batteries 1, 2, and 3, with each charger charging a different battery.
- 4) Battery Discharging
 - Relays configured for any one of batteries 1, 2, or 3 providing power to either load bank 1 or 2.
 - or
 - Relays configured for any two of batteries 1, 2, and 3 providing power to both load banks 1 and 2, with each load bank powered by a different battery (equivalently, each battery may drive only one load bank).

5) Battery Charging and Discharging

- Relays configured for charging one or more batteries (from solar array and/or battery chargers) and one or two batteries driving one or both load banks. Each load bank is powered by a different battery (equivalently, each battery may drive only one load bank). Any battery being charged must be unloaded.

For some investigations, when a failure causes the disruption of the intending operating mode, automated software, the User, or a combination of the two will identify the problem, devise a remediation plan, and execute the recovery actions.

4.2 Operational Procedures

Procedures have been written to ensure the safe operation of the testbed. The following sections provide references to Appendices that have more detailed information.

4.2.1 Computer Startup and Shutdown

The procedures to bring the five computers to an experiment-ready condition are given in Appendix E.

4.2.2 HyDE Startup

The procedure to start up HyDE is given in Appendix F.

4.2.3 Operator Stations

The procedures for the User, Antagonist, and Observer operator stations are given in Appendix G.

4.2.4 Emergency Stop

In the event of an unsafe operation condition, an emergency stop should be initiated. See Appendix H.

4.2.5 Manual Fault Injection

Special care must be taken when performing manual fault injection. Refer to section 5.3. The general safety procedures for each operator during manual fault injection are detailed in Appendix M.

5. ADAPT Safety Considerations

Because the ADAPT facility uses energized equipment, specific training, equipment, and procedures are required to insure the safety of those persons working in or near the lab. The following sections discuss the required training, personal protective equipment, tools, equipment design and labeling, lab setup, and procedures to maintain a safe working environment.

5.1 Required Electrical Safety Training

Only qualified electrical workers can work on or near energized components. To be qualified, employees shall be trained in the following:

1. The hazards of electrical energy.
2. Avoiding the electrical hazards of working on or near exposed energized parts.
3. Distinguishing between live parts and other parts of electrical equipment.
4. Skills and techniques to determine nominal voltage and exposure clearance distances.
5. Equipment specific lockout/tagout procedures.
6. Construction, operation and hazards associated with the specific equipment typically worked on.
7. Use of precautionary techniques, PPE, insulating and shielding materials, and insulated tools and test equipment.
8. Pre-task planning: determination of degree and extent of hazards and the steps needed to perform task safely.
9. Methods to release victims from contact with live parts.
10. First aid/CPR.

This training can be done in a classroom or on the job. Training must be fully documented (name of student, date of class or on the job training, list of topics covered, name of instructor). A record of the training for the ADAPT facility is given in Appendix I. Also included in this Appendix is training course material.

The training provided for ADAPT staff does not qualify personnel to work on or near other electrical systems. The training is for injecting and repairing ADAPT faults only. Furthermore, any faults associated with the large wires carrying the full DC current (70 amps) shall be repaired by the responsible electrical engineer or an electrician.

5.2 De-energized Electrical Work and Lockout/Tagout

Other than manual fault injection and troubleshooting, work on the simulator racks shall be done in an electrically safe condition. An electrically safe condition is achieved by properly locking out the power. This includes de-energizing, locking/tagging, relieving any stored energy, testing and attempting to start.

The lockout/tagout procedure for performing maintenance or repair work of the facility equipment racks is given in Appendix J.

5.3 Energized Electrical Work / Manual Fault Injection

Energized Electrical Work, including troubleshooting and manual fault injection, requires Personal Protective Equipment (PPE), tools, barriers, signs/labels, and specific procedures.

5.3.1 Personal Protective Equipment

The PPE for energized electrical work is given in Appendix K and repeated here for convenience.

- Natural fiber pants (e.g., denim)
- Long sleeve cotton shirt
- Safety glasses

- Insulated rubber gloves rated for the voltage and amperage
- Insulated tools rated for the voltage and amperage
- Conductive apparel shall not be worn (such as jewelry, rings, watchbands, belts, key chains, metal frame eyeglasses)

The first three are sufficient for working on the equipment racks after it has been confirmed that there is a zero energy state.

5.3.2 Equipment Design, Labeling, Lab Setup, Tools, and Procedures

An emergency stop button is included both in hardware and software. A hardware emergency stop button is located at the Observer station (see Figure 1). Each operator station also has an emergency button implemented in LabVIEW as a software emergency stop. A hardware emergency stop should be initiated in the event of an electrical shock. More information on the emergency stop can be found in Appendix H and Appendix O. The procedure to release a victim from contact with live parts is given in Appendix N.

Each equipment rack door is labeled as follows:

Label 1: Danger: Hazardous Voltage. Energized testing to be performed by qualified/trained personnel only. Wear proper PPE and use proper tools.

Label 2: Danger: Hazardous Voltage, 2 sources. Turn off and lockout AC and battery power before servicing.

The equipment rack doors and the battery cabinet doors are to be normally locked. The keys will be kept in the lockout/tagout box. The doors will be opened only for repair and maintenance and for manual fault injection. The equipment racks are bolted together and the middle rack is seismically braced to the north wall. The battery cabinet is also seismically braced to the north wall.

As shown in Figure 1 there are safety zones around the equipment racks and battery cabinet. The clearance in front of the racks must be: 36” deep, 78” tall, and as wide as the racks. The front of the battery rack must be 36” away from the equipment racks. A barrier will be positioned 3’6” away from the front of the racks to prevent access to energized equipment during testing. A sign is placed on the barrier stating: “Danger: Electrical Equipment. Authorized Personnel Only. Do not cross barrier when racks are energized and covers are open without proper training, tools, and protective equipment.”

Only personnel certified for manual fault injection, as indicated in Appendix I, may cross the barrier with the proper PPE (see Appendix K) and inject faults at the equipment racks. Care must be taken to following the procedures in Appendix M to avoid the possibility of injury.

6. ADAPT Electrical Diagrams, Equipment Specifications, I/O List

A functional, panel-by-panel description of the testbed, electrical drawings, I/O list, and equipment cut sheets are included in Appendix O (a separate binder). A list of the drawings included is given below.

Table 1. ADAPT electrical drawing list.

Item	Drawing Number	Re- vision	Sheet No.	Title	File Name
1	A269-0500-E1	-	1	ISHM ADAPT Power Subsystem One Line	269-0500-E2_1_-.DWG
2	A269-0500-E2	-	1	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_1_-.DWG
3	A269-0500-E2	-	2	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_2_-.DWG
4	A269-0500-E2	-	3	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_3_-.DWG
5	A269-0500-E2	-	4	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_4_-.DWG
6	A269-0500-E2	-	5	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_5_-.DWG
7	A269-0500-E2	-	6	ISHM ADAPT Power Subsystem Elementary Diagram	269-0500-E2_6_-.DWG
8	A269-0500-E5	-	1	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_1_-.DWG
9	A269-0500-E5	-	2	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_2_-.DWG
10	A269-0500-E5	-	3	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_3_-.DWG
11	A269-0500-E5	-	4	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_4_-.DWG
12	A269-0500-E5	-	5	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_5_-.DWG
13	A269-0500-E5	-	6	ISHM ADAPT Power Subsystem	269-0500-E5_6_-.DWG

				Cabinet 1 Wiring Diagram	
14	A269-0500-E5	-	7	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_7_-.DWG
15	A269-0500-E5	-	8	ISHM ADAPT Power Subsystem Cabinet 1 Wiring Diagram	269-0500-E5_8_-.DWG
16	A269-0500-E6	-	1	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_1_-.DWG
17	A269-0500-E6	-	2	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_2_-.DWG
18	A269-0500-E6	-	3	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_3_-.DWG
19	A269-0500-E6	-	4	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_4_-.DWG
20	A269-0500-E6	-	5	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_5_-.DWG
21	A269-0500-E6	-	6	ISHM ADAPT Power Subsystem Cabinet 2 Wiring Diagram	269-0500-E6_6_-.DWG
22	A269-0500-E7	-	1	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_1_-.DWG
23	A269-0500-E7	-	2	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_2_-.DWG
24	A269-0500-E7	-	3	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_3_-.DWG
25	A269-0500-E7	-	4	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_4_-.DWG
26	A269-0500-E7	-	5	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_5_-.DWG

27	A269-0500-E7	-	6	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_6_-.DWG
28	A269-0500-E7	-	7	ISHM ADAPT Power Subsystem Cabinet 3 Wiring Diagram	269-0500-E7_7_-.DWG
29	A269-0500-E13	-	1	ISHM ADAPT Power Subsystem Backplane 1 Wiring Diagram	269-0500-E13_1_-.DWG
30	A269-0500-E14	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 1 Wiring Diagram	269-0500-E14_1_-.DWG
31	A269-0500-E15	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 2 Wiring Diagram	269-0500-E15_1_-.DWG
32	A269-0500-E16	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 3 Wiring Diagram	269-0500-E16_1_-.DWG
33	A269-0500-E17	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 4 Wiring Diagram	269-0500-E17_1_-.DWG
34	A269-0500-E18	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 5 Wiring Diagram	269-0500-E18_1_-.DWG
35	A269-0500-E19	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 6 Wiring Diagram	269-0500-E19_1_-.DWG
36	A269-0500-E20	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 7 Wiring Diagram	269-0500-E20_1_-.DWG
37	A269-0500-E21	-	1	ISHM ADAPT Power Subsystem Backplane 1, Module 8 Wiring Diagram	269-0500-E21_1_-.DWG
38	A269-0500-E22	-	1	ISHM ADAPT Power Subsystem Backplane 2 Wiring Diagram	269-0500-E22_1_-.DWG
39	A269-0500-E23	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 1 Wiring Diagram	269-0500-E23_1_-.DWG
40	A269-0500-E24	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 2	269-0500-E24_1_-.DWG

				Wiring Diagram	
41	A269-0500-E25	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 3 Wiring Diagram	269-0500-E25_1_-.DWG
42	A269-0500-E26	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 4 Wiring Diagram	269-0500-E26_1_-.DWG
43	A269-0500-E27	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 5 Wiring Diagram	269-0500-E27_1_-.DWG
44	A269-0500-E28	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 6 Wiring Diagram	269-0500-E28_1_-.DWG
45	A269-0500-E29	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 7 Wiring Diagram	269-0500-E29_1_-.DWG
46	A269-0500-E30	-	1	ISHM ADAPT Power Subsystem Backplane 2, Module 8 Wiring Diagram	269-0500-E30_1_-.DWG
47	A269-0500-E41	-	1	ISHM ADAPT Power Subsystem Battery Enclosure Arrangement	269-0500-E41_1_-.DWG
48	A269-0500-E42	-	1	ISHM ADAPT Power Subsystem Cabinet Panel Arrangement	269-0500-E42_1_-.DWG
49	A269-0500-E42	-	2	ISHM ADAPT Power Subsystem Cabinet Panel Arrangement	269-0500-E42_2_-.DWG
50	A269-0500-E42	-	3	ISHM ADAPT Power Subsystem Cabinet Panel Arrangement	269-0500-E42_3_-.DWG
51	A269-0500-E42	-	4	ISHM ADAPT Power Subsystem Cabinet Panel Arrangement	269-0500-E42_4_-.DWG
52	A269-0500-M1	-	1	ISHM ADAPT Power Subsystem Process & Instrumentation Diagram	269-0500-M1_1_-.DWG

Appendix A Acronyms

AC	Alternating Current
ACW	Advanced Caution and Warning
ADAPT	Advanced Diagnostics And Prognostics Testbed
ANT	Antagonist computer
AVI	Avionics computer
cFP	Compact Field Point
DAC	Data Acquisition and Control
DAQ	Data Acquisition
DC	Direct Current
EPS	Electrical Power System
FOM	Figures of Merit
HyDE	Hybrid Diagnosis Engine
I/O	Input/Output
LED	Light Emitting Diode
LOG	Observer/Logger computer
NC	Normally Closed
NO	Normally Open
PPE	Personal Protective Equipment
TPM	Technical Performance Measures
USR	User computer
VAC	Voltage Alternating Current
VDC	Voltage Direct Current

Appendix B Software Configuration File

```
[SETUP]
date=09/13/05
version=0.0
rootdir=
experimentPI=
experimentID=

[ADAPT]
192.168.0.120=DAQ
192.168.0.128=ANTAGONIST
192.168.0.136=AVIONICS
192.168.0.144=USER
192.168.0.152=LOGGER
iolist="daq\adaptIOList.txt"
BufferMaxBytes=8192
BufferMaxPackets=256
wirediagram="WireDiagram\WireDiagram.vi"

[USER_VIS]
DataSocket\Diagnosis\readDiagnosis.vi=
DataSocket\Command\sendCommands.vi=
DataSocket\Sensor\readWriteSensorData.vi=
DataSocket\Message\sendMessages.vi=
DataSocket\Message\receiveMessages.vi=
WireDiagram\WireDiagram.vi=

[ANTAGONIST_VIS]
DataSocket\Diagnosis\readDiagnosis.vi=
DataSocket\Command\sendCommands.vi=
DataSocket\Command\receiveCommands.vi=
DataSocket\Sensor\readWriteSensorData.vi=
DataSocket\Message\sendMessages.vi=
DataSocket\Message\receiveMessages.vi=
WireDiagram\WireDiagram.vi=

[LOGGER_VIS]
DataSocket\Logging\Log.vi=
DataSocket\Diagnosis\readDiagnosis.vi=
DataSocket\Sensor\readWriteSensorData.vi=
DataSocket\Message\sendMessages.vi=
DataSocket\Message\receiveMessages.vi=
WireDiagram\WireDiagram.vi=

[USER_DS]
sensorRead0=dstp://localhost/aviDATA
sensorWrite=""
commandRead0=""
commandWrite=dstp://192.168.0.136/usrCMD
TADiagnosisRead0=dstp://localhost/aviDIAG
TADiagnosisWrite=""
messageRead0=dstp://localhost/usrMSG
```

```
messageRead1=dstp://localhost/logMSG
messageWrite0=dstp://localhost/usrMSG
expStatURL=dstp://192.168.0.152/expSTAT
```

```
[ANTAGONIST_DS]
```

```
sensorRead0=dstp://localhost/daqDATA
sensorWrite=dstp://192.168.0.136/antDATA
commandRead0=dstp://localhost/aviCMD
commandWrite=dstp://192.168.0.120/antCMD
TADiagnosisRead0=""
TADiagnosisWrite=""
messageRead0=dstp://localhost/antMSG
messageRead1=dstp://localhost/logMSG
messageWrite0=dstp://localhost/antMSG
expStatURL=dstp://192.168.0.152/expSTAT
```

```
[AVIONICS_DS]
```

```
sensorRead0=dstp://localhost/antDATA
sensorWrite=dstp://192.168.0.144/aviDATA
sensorWriteTA=dstp://localhost/taDATA
commandRead0=dstp://localhost/usrCMD
commandWrite=dstp://192.168.0.128/aviCMD
commandWriteTA=dstp://localhost/taCMD
TADiagnosisRead0=dstp://localhost/taDIAG
TADiagnosisWrite=dstp://192.168.0.144/aviDIAG
messageRead1=dstp://localhost/daqMSG
messageRead0=dstp://localhost/logMSG
messageWrite0=dstp://localhost/aviMSG
expStatURL=dstp://192.168.0.152/expSTAT
```

```
[DAQ_DS]
```

```
sensorRead0=""
sensorWrite=dstp://192.168.0.128/daqDATA
commandRead0=dstp://localhost/antCMD
commandWrite=""
TADiagnosisRead0=""
TADiagnosisWrite=""
messageRead0=dstp://localhost/daqMSG
messageRead1=dstp://localhost/logMSG
messageWrite0=dstp://localhost/daqMSG
expStatURL=dstp://192.168.0.152/expSTAT
```

```
[LOGGER_DS]
```

```
sensorRead0=dstp://192.168.0.128/daqDATA
sensorRead1=dstp://192.168.0.136/antDATA
sensorRead2=dstp://192.168.0.144/aviDATA
sensorWrite=""
commandRead0=dstp://192.168.0.136/usrCMD
commandRead1=dstp://192.168.0.128/aviCMD
commandRead2=dstp://192.168.0.120/antCMD
commandWrite=""
TADiagnosisRead0=dstp://192.168.0.144/aviDIAG
TADiagnosisWrite=""
messageRead0=dstp://localhost/logMSG
messageRead1=dstp://192.168.0.144/usrMSG
messageRead2=dstp://192.168.0.128/antMSG
messageRead3=dstp://192.168.0.136/aviMSG
```

messageRead4=dstp://192.168.0.120/daqMSG
messageWrite0=dstp://localhost/logMSG
messageWrite1=dstp://192.168.0.144/logMSG
messageWrite2=dstp://192.168.0.136/logMSG
messageWrite3=dstp://192.168.0.128/logMSG
messageWrite4=dstp://192.168.0.120/logMSG
expStatURL=dstp://localhost/expSTAT

[USER_CTRL]

Manual_visible=TRUE
Blinking Controls Tree_visible=TRUE
Spoofed Data List_visible=FALSE
Spoof Data_visible=FALSE
Intercept List_visible=FALSE
Intercept Commands_visible=FALSE
Messages_posLeft=1061
Messages_posTop=-375
Experiment Start_visible=FALSE
Exp Time_DS=Subscribe
Message_visible=FALSE
Send Message_visible=FALSE

[ANTAGONIST_CTRL]

Manual_visible=FALSE
Blinking Controls Tree_visible=FALSE
Spoofed Data List_visible=TRUE
Spoof Data_visible=TRUE
Intercept List_visible=TRUE
Intercept Commands_visible=TRUE
Messages_posLeft=1061
Messages_posTop=-600
Experiment Start_visible=FALSE
Exp Time_DS=Subscribe
Message_visible=FALSE
Send Message_visible=FALSE

[LOGGER_CTRL]

Manual_visible=FALSE
Blinking Controls Tree_visible=FALSE
Spoofed Data List_visible=FALSE
Spoof Data_visible=FALSE
Intercept List_visible=FALSE
Intercept Commands_visible=FALSE
Messages_posLeft=789
Messages_posTop=-397
Experiment Start_visible=TRUE
Exp Time_DS=Publish
Message_visible=TRUE
Send Message_visible=TRUE

Appendix C DataSockets Protocol

General Datasockets info

The ADAPT testbed is currently using the National Instruments datasockets protocol for sending messages between the software components. This protocol has a particular format of particular datatypes. The basic datatypes available to C++ applications in the Measurement Studio product are:

bool
char
int
short
long
float
double
CString: Microsoft MFC String class
COleVariant: Microsoft MFC wrapper class for binary data
CNiComplex: National Instruments complex number class
CNiVector: National Instruments vector class, can be a vector of several NI-defined numeric datatypes, e.g. CNiReal32Vector
CNiMatrix: National Instruments matrix class, can be a matrix of several NI-defined numeric datatypes, e.g. CNiReal32Matrix

The Labview datatypes are analogous to these. These datatypes can be assembled into a datasocket message. It looks like this can be of the following form, where <any> can take on any of the datatypes listed above:

```
CNiDataSocketData
|- <any> Value
|- Attributes (0...n)
   |- CString name
   |- <any> Value
```

The "Value" field is any data value to be sent. There can be an unlimited number of attributes sent with the message, which contain a name (string type) and a Value, which can be any type. ADAPT makes extensive use of the attributes in its software messages.

ADAPT Datasocket URLs

The messages are currently sent point-to-point.

A software component connects to a datasocket channel specified with a URL. On the avionics PC, the datasocket URLs are

1. dstp://localhost/taDATA - avionics writes sensor data to be read by the test article
2. dstp://localhost/taCMD - avionics writes system commands from the user to be read by the test article
3. dstp://localhost/taDIAG - test article writes a diagnosis to be read by the avionics

ADAPT Datasocket messages

SensorValuesMessage

```
|- CString Value = "sensors"
|- Attribute
  |- CString name = "idTag"
  |- int (i32) Value
|- Attribute
  |- CString name = "timeStamp"
  |- double Value
|- Attributes (n = #sensors = ~110)
  |- CString name = "sensorId"
  |- double Value
```

CommandMessage

```
|- CString Value = "command"
|- Attribute
  |- CString name = "idTag"
  |- int (i32) Value
|- Attribute
  |- CString name = "timeStamp"
  |- double Value
|- Attribute (n = 1)
  |- CString name = "controlId"
  |- CString Value <-- name of relay/switch
|- Attribute (n = 1)
  |- CString name = "commandId"
  |- bool Value
```

DiagnosisCandidate message

```
|- CString Value = "diagnosis"
|- Attribute
  |- CString name = "idTag" <- increments by 1 for each message
  |- int (i32) Value
|- Attribute
  |- CString name = "diagnosisId" <- All candidates from the same
  |- int (i32) Value diagnosis will have the same value
|- Attribute
  |- CString name = "numberOfCandidates"
  |- int (i32) Value
|- Attribute
  |- CString name = "candidateTimeStamp" <- May not be needed anymore,
  |- double Value if timeStamps are given to faults
|- Attribute
  |- CString name = "candidateNumber"
```

```

    |- int (i32) Value
|- Attribute
  |- CString name = "probability"
  |- double Value
|- Attribute
  |- CString name = "numberOfFaults"
  |- int (i32) Value
|- Attribute
  |- CString name = "faultX"           \
  |- CString Value                     \
|- Attribute                           / These 2 repeat for # of faults
  |- CString name = "timeOfFaultX"    /
  |- double Value                     /

```

LogMessage

```

|- CString Value = "logMessage"
|- Attribute
  |- CString name = "idTag"
  |- int (i32) Value
|- Attribute
  |- CString name = "timeStamp"
  |- double Value
|- Attribute
  |- CString name = "sender"
  |- CString Value
|- Attribute
  |- CString name = "message"
  |- CString Value

```

Appendix D Fault Injection List

First created: Jan 13, 2006

Last modified: Jan 18, 2006

This document contains a brief outline of the faults which are considered by the ADAPT testbed. It begins with the faults currently implemented, and continues with faults which have been considered for implementation. Finally, this list is not exhaustive; any specific fault or test desired by a test article could potentially be tested on ADAPT, subject to safety and expense considerations.

Quick Summary:

- 1.0 Faults currently implemented
 - 1.1 Circuit Breaker Tripped
 - 1.2 Relay Failed Open
 - 1.3 Relay Failed Closed
 - 1.4 Relay Overheating
 - 1.5 Sensor Shorted
 - 1.6 Sensor Open Circuit
 - 1.7 Sensor Stuck
 - 1.8 AC Inverter Failed
 - 1.9 Solar Array blocked
- 2.0 Faults Under Consideration
 - 2.1 Destructive testing
 - 2.2 Sensor Out of Calibration
 - 2.3 Battery Charger Failed
 - 2.4 Photovoltaic Charger Failed
 - 2.5 Battery Overheating
 - 2.6 Battery Overcharged
 - 2.7 Excessive Sensor Noise
 - 2.8 Broken Wire
 - 2.9 Faults in Loads

Related documents: These documents contain information used for this fault list:

I/O Channel List:

[Code TI](#) » [DASH](#) » [ITeM](#) » [ADAPT](#) » [Documentation](#) » [Interface](#) » Data Acquisition I/O list.doc

<https://nx.arc.nasa.gov/nx/dsweb/View/Collection-9410>

Initial 10 ADAPT faults developed by the function-failure analysis:

1. Faults currently implemented

The faults currently implemented are mainly implemented via software. They are injected at the antagonist workstation in the ADAPT software architecture. There are 3 capabilities given by the antagonist workstation: first, the ability to send commands to the testbed which were not initiated by the user or seen by the ISHM test article, second, the ability to intercept commands sent by the user, preventing them from reaching the testbed, and third, the ability to set sensor data from the testbed to a given (constant) value, which the user and ISHM test article will see. These three capabilities are combined to produce the software faults in the list below (when software procedures are given).

Note that all fault injections, especially the hardware or manual fault injections, must be done in a safe manner and according to the ADAPT software procedures.

1.1 *Circuit Breaker Tripped*

Description:

A circuit breaker on the ADAPT power system trips, cutting off the current flow through itself.

Fault Type: Discrete event fault

Component List:

Commandable circuit breakers: EY136, EY236, EY336.

Non-commandable circuit breakers: ISH104, ISH204, ISH304, ISH110, ISH210, ISH310, ISH162, ISH262, ISH166, ISH180, ISH266, ISH280.

Injection Procedure:

Software: The commandable circuit breakers may be sent a software command to trip from the antagonist workstation. The antagonist will send a trip command to one of these commandable circuit breakers. The fault injection time will be considered to be the time when the trip command is sent.

Hardware: All circuit breakers are equipped with manual throw bars. The antagonist will physically throw the circuit breaker on the testbed. The fault injection time will be considered to be the timestamp of the first frame of telemetry which contains the changed sensor values as a

result of the fault injection. A screen will be set in place so the user cannot see the antagonist's actions.

Clearing Procedure:

There is no software command available to reset any of the circuit breakers. For both hardware and software fault injections, the antagonist must manually reset the circuit breaker to the closed position.

1.2 Relay Failed Open

Description: A relay on the ADAPT power distribution system fails in the open state, i.e. electrical current will no longer flow through it. All subsequent commands to the relay will have no effect.

Fault Type: Discrete event fault

Component List: The components that can exhibit this behavior are the following:

Electromechanical Relays: EY106, EY206, EY306, EY115, EY116, EY117, EY215, EY216, EY217, EY315, EY316, EY317, EY126, EY226, EY326, EY170-175, EY183-184, EY270-275, EY283-284

Solid-State Relays: EY141, EY144, EY241, EY244, EY341, EY344, EY160, EY260

Injection Procedure:

Software: First, the antagonist software station will block all future commands to the relay. Second, if the relay is closed, the antagonist will command the relay open. Neither of these actions is visible to the user or the test article. If the relay is closed, the fault injection time will be defined as the time at which the open command is sent by the antagonist. If the relay is open, the fault injection time will be defined as the next time at which the user attempts to close the relay (and it remains open).

Hardware: The antagonist goes to the panel and physically removes the relay from the circuit. A screen will be set in place so the user cannot see the antagonist's actions.

Clearing Procedure:

Software: The antagonist will remove the command block on the relay via the antagonist workstation software. Either the user or antagonist may then command the relay to the desired position.

Hardware: After the test run, the antagonist or other authorized personnel will power down the testbed and reinstall the relay.

1.3 Relay Failed Closed

Description: A relay on the ADAPT power distribution system fails in the closed state, i.e. electrical current is allowed to flow through it. All subsequent commands to the relay will have no effect.

Fault Type: Discrete event fault

Component List:

All of the electromechanical and solid-state relays listed in the "Relay Failed Open" fault can also exhibit this "Relay Failed Closed" fault.

Injection Procedure:

Software: First, the antagonist software station will block all future commands to the relay. Second, if the relay is open, the antagonist will command the relay closed. Neither of these actions is visible to the user or the test article. If the relay is open, the fault injection time will be defined as the time at which the close command is sent by the antagonist. If the relay is closed, the fault injection time will be defined as the next time at which the user attempts to open the relay (and it remains closed).

Hardware: The antagonist goes to the relay and sets a short-circuit across the relay terminals. A screen will be set in place so the user cannot see the antagonist's actions. **CAUTION:** remain calm, sparks may occur; attempt to set the short-circuit in a smooth and deliberate motion. If a hazardous situation results, hit the ESTOP button.

Clearing Procedure:

Software: The antagonist will remove the command block on the relay via the antagonist workstation software. Either the user or antagonist may then command the relay to the desired position.

Hardware: The antagonist returns to the relay and removes the short-circuit across the relay.

1.4 Relay Overheating

Description:

A relay on the ADAPT power system failed by overheating. This will result in current being allowed through the relay. All subsequent commands to the relay will have no effect.

Fault Type: Discrete event fault

Component List:

Only the solid-state relays defined in the fault, "Relay Failed Open" will exhibit this fault.

Injection Procedure:

Software: After determining the effects of this fault via hardware, a method to mimic it in software will be developed.

Hardware: The antagonist goes to the relay and heats it with a heat gun until a fault is induced.

Clearing Procedure:

Software: N/A

Hardware: Remove the heat gun from the relay and wait for the relay to return to room temperature.

1.5 Sensor Shorted

Description:

A sensor on the ADAPT testbed has shorted, or the wires leading to the sensor have shorted. This will correspond to the sensor reporting the value which corresponds to zero voltage. After the fault injection, the sensor will only report that value.

Fault Type: Discrete event fault

Component List:

Voltage Sensors: E105, E107, E109, E125, E135, E140, E142, E161, E165, E167, E181, E225, E235, E240, E242, E261, E265, E267, E281, E325, E335, E340.

Current Sensors: IT127, IT140, IT161, IT167, IT181, IT227, IT240, IT261, IT267, IT281, IT327, IT340.

Temperature Sensors: TE103, TE128, TE129, TE133, TE141, TE144, TE160, TE228, TE229, TE241, TE244, TE260, TE328, TE329, TE341, TE344.

AC Frequency Sensors: FT165, FT265.

Relay/CircuitBreaker Position Sensors: ESH101, ISH104, ESH106, ISH110, ESH115A, ESH116A, ESH117A, ESH126A, ISH136, ESH141A, ESH144A, ESH160A, ISH162, ISH166, ESH170, ESH171, ESH172, ESH173, ESH174, ESH175, ISH180, ESH183, ESH184, ISH204, ESH206, ISH210, ESH215A, ESH216A, ESH217A, ESH226A, ISH236, ESH241A, ESH244A, ESH260A, ISH262, ISH266, ESH270, ESH271, ESH272, ESH273, ESH274, ESH275, ISH280,

ESH283, ESH284, ISH304, ESH306, ISH310, ESH315A, ESH316A, ESH317A, ESH326A, ISH336, ESH341A, ESH344A.

Light Sensor: LT103

Injection Procedure:

Software: The antagonist will reset ("spoof") the value for the affected sensor to correspond with that sensor's zero-voltage reading.

Hardware: The antagonist will go to the sensor wiring on the panel and induce a short circuit past the sensor wires. A screen will be set in place so the user cannot see the antagonist's actions.

Clearing Procedure:

Software: The antagonist will remove the sensor value block, aka stop spoofing the sensor value.

Hardware: The antagonist will return to the sensor wiring and remove the short circuit across the sensor.

1.6 Sensor Open Circuit

Description:

A sensor on the ADAPT testbed has failed in an open circuit, or the wires leading to the sensor are broken. This will correspond to the sensor reporting the value which corresponds to full-scale voltage. After the fault injection, the sensor will only report that value.

Fault Type: Discrete event fault

Component List:

All sensors listed in the "Sensor shorted" fault can also fail in this manner.

Injection Procedure:

Software: The antagonist will reset ("spoof") the value for the affected sensor to correspond with that sensor's full-scale reading.

Hardware: The antagonist will remove a sensor wire from going to the data acquisition board. A screen will be set in place so the user cannot see the antagonist's actions.

Clearing Procedure:

Software: The antagonist will remove the sensor value block, aka stop spoofing the sensor value.

Hardware: The antagonist will return to the sensor and replace the sensor wire.

1.7 Sensor Stuck

Description:

A sensor on the ADAPT testbed has stuck on a value, and does not accurately report the quantity it is measuring. The sensor will be reporting the value between the zero-voltage value and the full-scale voltage value. After the fault injection, the sensor will only report that value.

Fault Type: Discrete event fault

Component List:

All sensors listed in the "Sensor shorted" fault, except for the relay and circuit breaker position sensors, can also fail in this manner. The relay and circuit breaker position sensors are digital sensors, and so this fault would be indistinguishable from the "sensor shorted" and "sensor open circuit" faults.

Injection Procedure:

Software: The antagonist will reset ("spooof") the value for the affected sensor to a randomly chosen value in between that sensor's zero-voltage reading and the full-scale reading.

Hardware: TBD

Clearing Procedure:

1.8 AC Inverter Failed

Description: One of the AC inverters fails, and no longer provides AC power to the loads.

Fault Type: Discrete event fault

Component List: INV1, INV2

Injection Procedure:

Software: N/A

Hardware: The antagonist goes to the panel with the AC Inverter, and switches off the inverter. A screen will be set in place so the user cannot see the antagonist's actions.

Clearing Procedure:

Software: N/A

Hardware: The antagonist returns to the panel with the AC Inverter and turns it on again.

1.9 Solar Array blocked

Description:

The solar arrays on the ADAPT testbed have failed, or they are partially blocked.

Fault Type: Discrete event fault

Component List:

PV, the photovoltaic panel

Injection Procedure:

Software: The antagonist will first spoof the value of ESH106 to correspond to a closed relay, and then will block user commands to EY106 and command EY106 open.

Hardware: The antagonist will cover part of, or all of, the solar array panels with cardboard, preventing the light from reaching the solar arrays. **CAUTION:** Fire Hazard. Do not place cardboard near the lamps.

Clearing Procedure:

Software: The antagonist removes the spoofed value of ESH106 and removes the block on EY106 commands from the user.

Hardware: The antagonist removes the cardboard that was blocking the solar panel.

2. Faults Under Consideration

The following is a list of faults currently under consideration for implementation. They have not been implemented for several reasons including development time and pending approval by the safety division.

2.1 Destructive testing

Description:

Fault Type: varies

Component List:

Requested by: ADAPT team

Entails:

Creating list of destructive tests to be done

Safety approval of list

Purchasing of replacement equipment

2.2 Sensor Out of Calibration

Description: One or more sensors on the testbed falls out of calibration, returning erroneous readings. Not covered by current spoofing capability, which only resets a sensor to a constant value.

Component List:

All sensors except for the relay and circuit breaker position sensors.

Fault Type: Discrete event fault

Requested by: ADAPT team

Entails:

Modifying antagonist SW to add another spoofing capability: insert a scaling factor and offset to apply to the original sensor value.

2.3 Battery Charger Failed

Description: One of the battery chargers fails in one of several TBD ways.

Fault Type: varies

Component List: BC1, BC2

Requested by: ADAPT team

Entails:

Investigate battery charger fault modes

Determine how to replicate fault modes on ADAPT
Safety approval of implementation of fault modes

2.4 Photovoltaic Charger Failed

Description: The photovoltaic charger fails in one of several TBD ways.

Fault Type: varies

Component List: CC

Requested by: ADAPT team

Entails:

Investigate photovoltaic charger fault modes
Determine how to replicate fault modes on ADAPT
Safety approval of implementation of fault modes

2.5 Battery Overheating

Description: One of the batteries on the testbed overheats.

Fault Type: varies

Component List: BATT1A, BATT1B, BATT2A, BATT2B, BATT3A, BATT3B

Requested by: ADAPT team

Entails:

Determining fault injection method
Safety approval of fault injection method
Development and implementation of detection methodology

2.6 Battery Overcharged

Description: One of the batteries on the testbed is overcharged.

Fault Type: varies

Component List: All batteries listed above

Requested by: ADAPT team

Entails:

Determining fault injection method
Safety approval of fault injection method
Development and implementation of detection methodology

2.7 Excessive Sensor Noise

Description: One or more sensors experiences excessive sensor noise. This fault could either be used as a prognostic indicator of sensor failure, or could be used to test the robustness of ISHM technologies.

Fault Type: discrete event (could be continuous, noise level gradually increased over time)

Component List: Any of the continuous-valued sensors

Requested by: ADAPT team

Entails:

Instead of spoofing to a specific value, the antagonist will add noise to a sensor value.
Could choose a distribution or assume a Gaussian distribution for the noise.
Diagnostic methods which will detect or otherwise be affected by sensor noise (data-driven methods).

2.8 Broken Wire

Description: A wire on the testbed breaks. This will have the same effect as several of the faults listed before, such as relay failed open or sensor open circuit.

Fault Type: Discrete event fault

Component List: Not relevant to any particular component

Requested by: ADAPT team

Entails:

Possibly cutting several wires on the testbed and adding connectors to the wires, allowing for easy disconnection and reconnection.

2.9 *Faults in Loads*

Description: TBD

Fault Type: varies

Component List:

Requested by: ADAPT team

Entails:

Choosing and adding particular loads to the ADAPT system

Choosing faults in which to inject

Development of methods to detect the injected faults.

Appendix E Computer Startup and Shutdown Procedures

Startup procedures

Note: The computers can be brought up in any order, but problems may occur if the LabVIEW software is started on one computer before the others are ready. It is best to have all computers running, be logged in, and the DataSocket Server running before bringing up the LabVIEW software.

- 1) Common procedures to all computers
 - a) If necessary, boot computers.
 - b) Log into the ADAPT account; see testbed manager for the password.
 - c) The DataSocket Server is automatically started on login. To verify that the server is running, check the system tray in the lower right corner, or use the Windows Task Manager (look under the Processes tab for cdwss.exe). If the DataSocket Server is not running, click on the Start button and select **DataSocket Server**. (The DataSocket Server is also started by the LabVIEW software described below, but its better to have the servers already running before starting the software.)
 - d) Open the folder **c:\ADAPT**.
- 2) Starting the Data Acquisition (DAQ)
 - a) Double click on the file **ADAPT DAQ.vi**. This loads the LabVIEW data acquisition software. Once the software has finished loading, click on the white arrow in the upper left corner of the displayed panel to start the software running; the arrow should turn black. Verify data is being acquired by examining the SensorData box.
- 3) Starting the Avionics (AVI)
 - a) Double click on the file **ADAPT Avionics.vi**. This loads the LabVIEW avionics software, but NOT the Test Article Software. See Appendix x for specific Test Article instructions. Once the software has finished loading, click on the white arrow in the upper left corner of the displayed panel to start the software running; the arrow should turn black.
- 4) Starting the User (USR), Antagonist (ANT), and Logger (LOG)
 - a) Double click on the file **ControlPanel.vi**. This loads the LabVIEW avionics software. Once the software has finished loading, click on the white arrow in the

upper left corner of the displayed panel to start the software running; the arrow should turn black. A second LabVIEW display (the wire diagram) will come up on the left hand screen; verify values are updating.

Shutdown procedures

- 1) All computers
 - a) Click on the **STOP** button located on each LabVIEW software panel. This should stop all LabVIEW software running on the computer. This may take several seconds due to the timing within each software module.
 - b) If you want to exit LabVIEW, drag down on the File menu list, and select Exit.

Appendix F HyDE Startup Procedure

- 1) Start up the ADAPT software as described in Appendix E.
- 2) On the avionics computer, check that the HyDE harness file corresponds to the current state of the testbed. The default state is all circuit breakers closed (check that battery circuit breakers are closed), all relays open.

Open the text file

```
C:\user\adam\ADAPT\TestArticle\  
ADAPT-HyDE\model\ADAPTDiscretePowerSubsystem.hah
```

This specifies the initial state of all the components in the HyDE model, including sensors. This must correspond to the mode of the testbed (which relays and circuit breakers are open or closed) when HyDE is started. The easiest way to search for particular components is with notepad's "find" function, and the possible startup values for the different types are

relays: open, closed

circuit breakers: closed, tripped

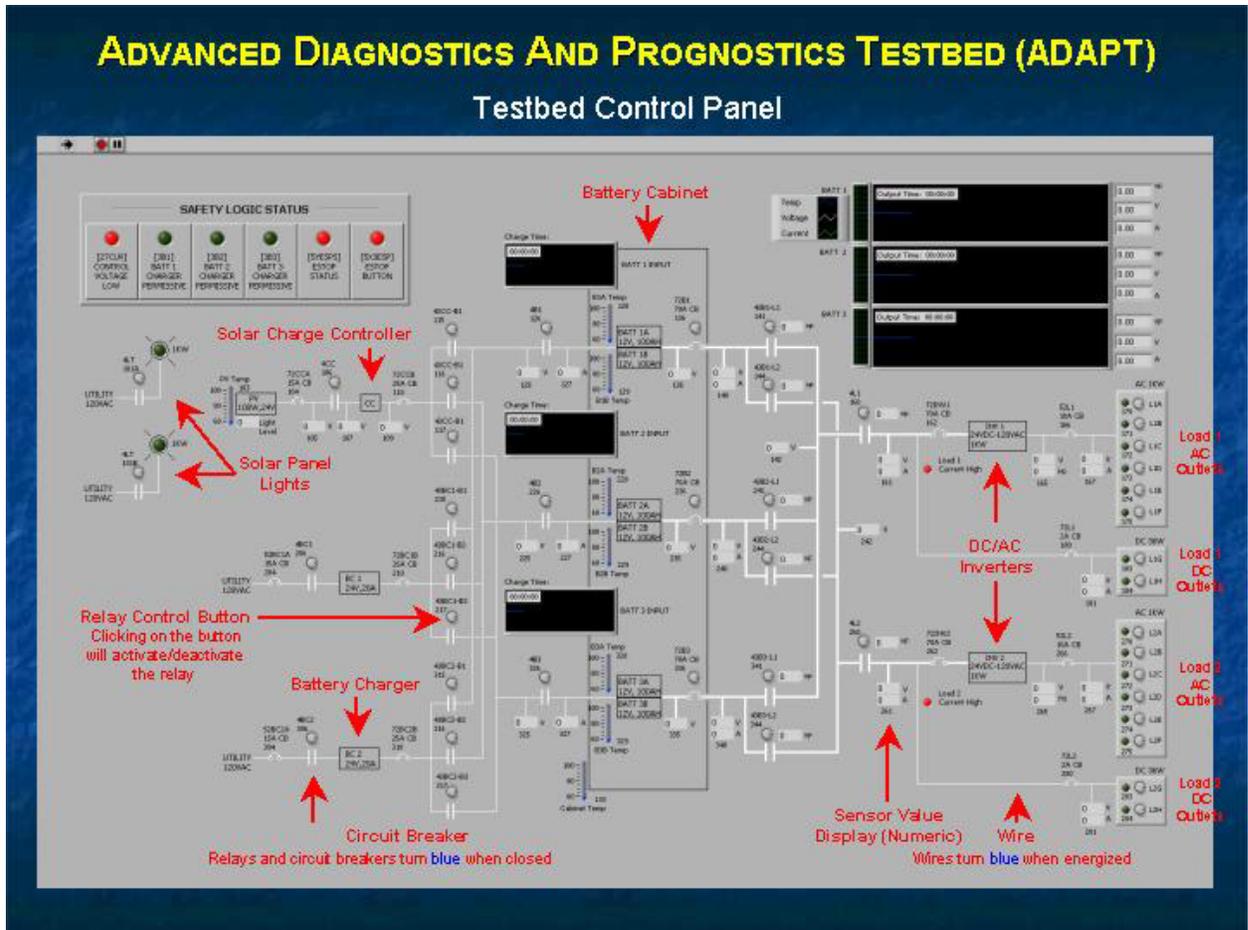
sensors: nominal, unknownFault

Save the changes to the harness file.

- 3) Launch the executable which uses HyDE:
C:\user\adam\ADAPT\TestArticle\ADAPT-HyDE\bin\ADAPT-HyDE.exe
- 4) HyDE will load the files, several confirmation lines will be printed to the console window, and then it will wait. The scenario/demo may be started anytime after this point. If HyDE is printing more than one "candidate" to the screen, or a fault diagnosis immediately appears on the user control screen, the most likely explanation is that the HyDE harness file did not correspond to the actual system state (step 2). The fault diagnosis indicates which component states are probably incorrect in the harness file.

Appendix G Operator Station Procedures

All operator stations have the schematic shown below. However, the information presented on each display is not necessarily the same. For example, the User display will not indicate where a fault is being injected, as the Antagonist display does. Each operator station also has individual control panels to perform the functions unique to each station.



Being an Antagonist

1) Data Spoofing

To spoof sensor data, do the following on the Antagonist's control panel:

- Click in the center of the **Spoofed Data List** box; The message "Please select a sensor from the Wire Diagram." should appear.
- Click on any sensor data numeric display (a temperature, voltage, or amperage). The control name should appear in the "Sensor" column of the Spoofed Data List.

- c) Type in a numeric data value into the “**Spoof**” column in the same row as the control name.
- d) Repeat for the number of sensors to be spoofed.
- e) When ready to spoof, click on the **SPOOF DATA** button. The button’s light should illuminate, and real data values should appear in “Real Value” column of the Spoofed Data List box.

To stop data spoofing, click on the SPOOF Data button again. The button’s light should go out, and the Spoofed Data List should clear.

2) Intercepting commands

To intercept USR commands, do the following on the Antagonist’s control panel:

- a) Click in the center of the Intercept List box; The message “Please select a control from the Wire Diagram.” should appear.
- b) Click on any control (relay or breaker). The control name should appear in the Intercept List in the Command column
- c) Repeat for the number of controls to be intercepted.
- d) When ready to spoof, click on the INTERCEPT COMMANDS button. The button’s light should illuminate, and the selected controls should blink yellow.

To stop intercepting commands, click on the Intercept Commands button again and the button’s light should go out. To clear the table, right click on the Intercept List box, and select “Empty Table”.

Logging an Experiment

On the Observer/Logger’s control panel, click the **Experiment Start** button. The button’s light should illuminate, and the **Experiment Time** numeric display should begin incrementing. Files will be opened and data/commands will be written to the files. These files are located in **C:\ADAPT\logfiles\yyyy-mm-dd\hh.mm.ss**, where yyyy-mm-dd is the current date and hh.mm.ss is the current time. Stop data and command writing to files by clicking on the **Experiment Start** button again. New folders and files are created each time an experiment is started.

Messages can be sent to all nodes and log file by typing the message in the **Message** box and clicking on the **Send Message** button.

Being a User

Automatic and Manual modes

There are two operational modes: Manual (Manual Mode: ON) and Automatic (Manual Mode: OFF). In manual mode, all controls are selectable; in automatic mode, some controls are commanded as part of a sequence of commands issued by

selecting other controls; they are “grayed out” and can not be selected. To select the mode, click on the **Manual Mode:** button. The default setting is Automatic mode.

General Operations

Clicking on a control brings up a dialog box indicating the state change and waits for a response from the User. Click on the OKAY button to accept the change, and CANCEL to cancel the change.

Each LOAD is enabled separately, and each outlet in each load leg (both AC and DC) can be enabled individually.

Note: Circuit Breaker controls 136, 236, and 336 cannot be used to reset the breakers physically, but can be used to trip the breakers.

Charging the batteries

Each of the three sets of batteries can be charged from the three power sources (solar, battery chargers 1 & 2). The following table shows which relay control charging:

Relay control:	115	Solar array panel charges Battery 1
	116	Battery charger 1 charges Battery 1
	117	Battery charger 2 charges Battery 1
	215	Solar array panel charges Battery 2
	216	Battery charger 1 charges Battery 2
	217	Battery charger 2 charges Battery 2
	315	Solar array panel charges Battery 3
	316	Battery charger 1 charges Battery 3
	317	Battery charger 2 charges Battery 3

Each charging source can charge only a single battery set at a time; safety logic built into the software will not permit multiple charging sources or destinations. Once a charging source has been selected to a battery, the other potential charging source control relays are “grayed out” and not selectable.

Selecting the battery charging source should normally be done in automatic mode (Manual Mode: OFF). Click on the appropriate relay control (see above), click on the OKAY button and the voltage path from the charging source to the battery should turn from white to blue.

Operating the solar panel

The solar panel should be in the horizontal position for full effect, and the black curtain should be arranged to block most of the light output by the two bulbs. The two

lights that power the solar array panel are controlled by relays 101A and 101B. Click on those buttons, click on the OKAY button, and the lights should power on. The “sun” symbol on the wire diagram panel should illuminate. The lights take several minutes to come to full illumination, and should not be looked at directly for long periods of time. Click on the buttons again to turn the lights off.

* Note: once a light has been powered down, do NOT attempt to power it on again until at least 5 minutes have passed; the light bulb and transformer need that time to cool down and reset.

Appendix H Emergency Stop Procedures

On each of the USR, AVI, and ANT control panels is a large red ESTOP button. Clicking on the button will activate a safety hardware trip mechanism that partially shuts down testbed power. There is also a mechanical ESTOP button that is located by the LOG computer. Pressing any one of these software or mechanical buttons will activate an ESTOP.

Activating the ESTOP removes from the circuit the following sources of power:

1. AC power to the photovoltaic cell's 2 lamps.
2. Photovoltaic cells and AC power to two battery chargers.
3. Three batteries, except for inside battery cabinet.

The 24 VDC, 5 amp control power supplies and the batteries within the battery cabinet remained energized. Use caution when working in the vicinity of these energized elements.

If the ESTOP has been activated, and once the error condition that caused the ESTOP has been resolved, the ESTOP mechanism needs to be reset. For an ESTOP initiated from a software button, on the ControlPanel, click on the **RESET ESTOP**, then push the black mechanical button on the ESTOP box. For an ESTOP initiated from the hardware button, pull up the ESTOP button, then depress the black mechanical button on the ESTOP box.

If the cabinet circuit breakers cannot be reset after an ESTOP, verify that CB136, CB236, and CB336 on the wire diagram GUI are enabled (the LED on the control button is lit).

In the event that someone is in contact with live power even after hitting the ESTOP, turn off circuit breakers 9, 11, 18, and 19 (labeled ADAPT facility) in panel LLQ. Also see Appendix N.

Appendix I Training Record

The following inserted pages include the names of personnel who have attended an ADAPT safety training class and the materials that were presented in the class. The training provided for ADAPT staff does not qualify personnel to work on or near other electrical systems. The training is for injecting and repairing ADAPT faults only. Furthermore, any faults associated with the large wires carrying the full DC current (70 amps) shall be repaired by the responsible electrical engineer or an electrician.

Appendix J Lockout/Tagout Procedure

The ADAPT lockout/tagout (LOTO) procedure is to be completed when performing maintenance or repair of the facility equipment racks. Lockout/tagout must be applied to each of the following locations (see lab schematic in Figure 1):

LOTO locations:

1. LLQ circuit breaker panel on south wall of lab near east entrance/exit.
2. Rear of equipment rack 2.
3. Battery cabinet circuit breakers.

Preparation:

1. Make entry in LOTO log book.
2. Retrieve tags (ARC 316) and locks to be used from LOTO box located in the lab.
3. Notify affected employees of work to be done.

Shutdown:

1. Open LLQ circuit breaker panel
2. Turn off circuit breakers 9, 11, and 19. Each of these are labeled, "ADAPT circuit". Do NOT turn off circuit breaker 18.
3. Attach circuit breaker lockout devices, locks, and tags to circuit breakers 9, 11, and 19. Note that one lock/tag may be used for 9 and 11. Ensure that tags are clearly labeled with employee's name and phone/pager number.
4. Attempt to turn on locked-out circuit breakers.
5. Go to equipment rack 2 and open front panel.
6. Turn off "SW1 PWR Supplies AC IN" knob next to large orange indicator light.
7. Close front panel and open back panel of rack 2.
8. Remove plug from power strip and attach the power cord safety lock and tag to the plug. Ensure that tag is clearly labeled with employee's name and phone/pager number.
9. Go to battery cabinet. Turn off battery circuit breakers.
10. Attach circuit breaker lockout devices, locks, and tags to each of the three circuit breakers. Ensure that tag is clearly labeled with employee's name and phone/pager number.
11. Attempt to turn on locked-out circuit breakers.
12. Don appropriate Personal Protective Equipment for Hazard Category 0 (see Appendix K).
13. Using digital voltmeter, test for electrical energy at the rack locations requiring work.
14. Perform work. Note: PPE can be reduced after confirming zero energy state (see Appendix K).

Release from LOTO (do we need to sign the log book anywhere during this?):

1. Verify that work has been completed and that it is safe to re-energize.
2. Notify affected personnel.
3. Clear all tools and personnel from equipment.

4. Remove locks and tags from battery circuit breakers. Note: only the person who applied the locks is authorized to remove them.
5. Remove lock and tag from plug at equipment rack 2 and plug into power strip. Note: only the person who applied the locks is authorized to remove them.
6. Remove locks and tags from LLQ circuit breaker panel and turn on circuit breakers 9, 11, 19. Note: only the person who applied the locks is authorized to remove them.
7. Follow ADAPT startup procedures (see Appendix E).

Appendix K Personal Protective Equipment Requirements

Type of Work	PPE Requirements	Notes
De-energized circuits	<ul style="list-style-type: none"> • No conductive apparel • Natural fiber pants (e.g., denim) • Long sleeve cotton shirt • Safety glasses 	For work on electrical panels, this level of PPE is only acceptable after confirming zero energy state through testing with voltmeter
Energized electrical work (\leq 120V) at equipment racks corresponding to antagonist fault injection	<ul style="list-style-type: none"> • No conductive apparel • Natural fiber pants (e.g., denim) • Long sleeve cotton shirt • Safety glasses • Insulated rubber gloves rated for the voltage and amperage* • Insulated tools rated for the voltage 	Hazard Category 0 [NFPA 70e, Table 130.7(C)(9)(a)].

*Gloves may be removed if their use for the task is impractical and actually increases the hazard, provided an insulated tool is being used.

Appendix L Material Safety Data Sheet for Batteries

Hardcopies inserted on following pages.

Appendix M Manual Fault Injection General Safety Procedures

Only qualified personnel can manually inject faults while the system is powered. User, Antagonist, and Observer operators should be qualified personnel during manual fault injection.

Personnel are qualified by training in CPR, electrical hazards, first aid for electrical injury and the following safety procedures. See section 5 and Appendix I for more information.

l) Antagonist Safety Procedures for Manual Fault Injection

- **Only the Antagonist shall work on live power components during a test.**
- Identify fault to be injected and plan process, first.
- Inform Observer of the fault and the process for injection, before implementing to give info and to start clock. (This should be at least verbally and can include written descriptions. The Antagonist should confirm that the Observer understands the process and is ready to start the test.)
- Collect tools needed and list these tools on a test description or traveler (for confirmation later that all the tools have been removed from the test area). Put on protective clothing (natural fiber pants and natural fiber long-sleeved shirt, safety glasses, gloves; see Appendix K) and remove all metallic or conducting apparel such as jewelry and metal frame glasses.
- Pass barrier and close behind you after confirming that you are the only person between barrier and power cabinets and racks.
- Confirm power on or off. If not in the desired state, change it before continuing.
- Unlock and open cabinet or rack door to specific locale of fault.
- If necessary, light the interior of the rack or cabinet with the magnetically mounted flashlights provided. (One such flashlight shall be located on the back of the racks and one on the front of the racks.)
- Signal (verbally) the Observer that you are about to initiate fault.
- Observer shall watch any- and everyone within the test area while the system is active or powered. His roles are timer, recorder **and** safety officer. (*We may need a fish-eye mirror mounted to let the Observer see behind the racks during these operations.*)
- Using insulated tools and/or touching only the insulated parts of any wires, disconnect or loosen wire(s), card(s) or equipment involved in the fault or open or close switch, fuse or circuit breaker according to the plan established with Observer. Do not remove wires from solid-state relays or from the ESTOP circuitry. Indicate verbally to Observer that fault is initiated as it happens. The Antagonist should not turn and look away from the power subsystem to communicate with the Observer during fault injection; he should keep his eyes on the components to be changed.

- Disconnected wire ends shall be covered with insulating caps or protectors.
- Fuses shall only be removed with appropriate tool.
- Collect and remove all tools.
- Remain in the Test Area until the User has remediated the fault or the Observer has declared the fault to be “Missed”.
- Rack or cabinet door shall be closed and locked before departing the test area.
- Leave the test area by passing the barrier and closing behind you.

II) User Safety Procedures for Hard Fault Recovery

- User must be wearing natural fiber pants and shirt (long-sleeved), and no metallic or conductive apparel.
- Identify and isolate fault to least number of possibilities.
- Isolate/remove power to affected areas of the power subsystem from console if possible.
- Put on safety glasses and collect tools needed before entering test area. (Tool kit shall have an inventory list that shall be confirmed before leaving the test area.)
- Enter test area by passing through barrier and closing behind you.
- Confirm that you and possibly the Antagonist are the only people in the test area before closing barrier.
- Remove power to fault locale by manual throwing switches if not already done so from console, if required to safely remedy the fault. Perform lockout/tagout of equipment racks.
- Unlock and open cabinet or rack door in the specific fault locale(s).
- Confirm state of power in each area of the subsystem, via lights or test equipment.
- Repair fault. Remove lockout/tagout. Test repair. Report completed repair to Observer.
- Collect all tools and return them to the tool kit. Close and lock all doors to cabinets or racks.
- Leave test area through the barrier and close barrier behind you.
- Confirm full system operation at the console.

III) Observer Safety Procedures

- Record the fault description and injection plan as described by the Antagonist prior to Antagonist entry to the test area.
- Monitor the Antagonist and User whenever they enter the test area beyond the barrier.
- Record the time of the initiation of the fault and the time of the completion of the remediation. The time of the detection and isolation of the fault should be automatically recorded.
- Should any mishap occur, immediately activate the E-Stop button on the Observer console.
- If any injury or electrical shock should occur, immediately shut-off all power to the testbed via the circuit breakers near the main lab door. Attend to the victim and ascertain

the extent of the injury. If necessary, call 911 for emergency medical assistance. Document everything that occurred during the mishap.

Appendix N Releasing a Victim of Electrical Shock

Whenever an electrical shock occurs, activate the ESTOP immediately. If the victim is still in contact with live electrical power after depressing the ESTOP, turn off breakers #9, #11, #18, and #19 in circuit breaker panel LLQ. If the shock has caused a medical emergency, call 911 immediately on a NASA phone or 650-604-5555 on a cell phone. If the shock was significant but not the cause of a medical emergency, report to the Ames Health Unit for evaluation.

After electrical shock has occurred, the current must be turned off. After the power is clearly off, the injured person can be assisted. If there is any indication of continued shock or electrical energy, do not approach the victim. The rescuer should use extreme care to avoid becoming another victim.

If you are trained in CPR/AED, proceed with the following (an adult CPR/AED skills card with the following information will be kept in the lab...):

Checking an Unconscious Victim:

1. Check the scene for safety (as stated above, do not approach the victim if there appears to be continued shock or electrical energy), then check the victim.
2. Tap the victim's shoulder and shout to see if the victim responds.
3. If the victim does not respond... Call, or have someone else call 911 from a NASA phone or 650-604-5555 from a cell phone.
4. Without moving the victim, look, listen, and feel for breathing for about 5 seconds.
5. If the victim is unconscious, but is breathing and shows signs of circulation... Place him or her in the recovery position. Turn the victim to the opposite side if signs of circulation to the lower arm are lost.
6. If the victim is not breathing or you cannot tell... Roll the victim onto the back, while supporting the head and neck.
7. Tilt the head back and lift the chin to open the airway. Look, listen, and feel for breathing for about 5 seconds.
8. If the victim is not breathing, give 2 rescue breaths: tilt the head back and lift the chin to open the airway. Pinch the nose shut. Take a breath and breathe slowly into the victim. If the breaths do not go in, go to Unconscious Choking, Step 1.
9. If the breaths go in, check for signs of circulation. Find the Adam's apple and slide your fingers toward you and down into the groove at the side of the neck. Check for signs of circulation for no more than 10 seconds. Go to next care steps...

Next Care Steps:

If there are signs of circulation and breathing...

Monitor victim's circulation and breathing and place victim in recovery position.

If there is no pulse...

Retrieve the AED from the west 2nd floor stairwell of Bldg. 269. Perform CPR in Progress/Using and AED.

If there are signs of circulation and no breathing...

Perform Rescue Breathing.

CPR in Progress/Using an AED:

1. Do CPR until AED is ready to use.

CPR:

1. Find hand position on breastbone. Find notch at lower end of the breastbone and place the heel of one hand next to and above this notch. Place your other hand on top.
 2. Give 15 compressions. Position the shoulders over the hands. Compress the chest about 2 inches deep.
 3. Give 2 rescue breaths. Tilt the head back and lift the chin to open the airway. Pinch the nose shut. Take a breath and breathe slowly into the victim.
 4. Do about 3 more cycles of 15 compressions and 2 rescue breaths.
 5. Recheck for signs of circulation. Find the Adam's apple and slide your fingers towards you and down into the groove at the side of the neck. Check for signs of circulation for no more than 10 seconds.
 6. If there are signs of circulation but no breathing, go to Rescue Breathing.
2. When the AED is ready to use... Recheck the pulse. Find the Adam's apple and slide your fingers towards you and down into the groove at the side of the neck. Check for signs of circulation for no more than 10 seconds.
 3. If the victim shows no circulation (pulse), turn on the AED.
 4. Prepare to use the AED. Wipe the victim's chest dry. Attach the pads to the victim. Place one pad on the victim's upper right chest, and the other pad on the victim's lower left side. Plug the electrode cable into the AED.
 5. Let the AED analyze the victim's heart rhythm (or push the "analyze" button). Make sure no one is touching the victim. Say, "Everyone stand clear."
 6. Deliver a shock if prompted.

If the AED advises a shock is needed: make sure no one is touching the victim; say, "Everyone stand clear"; deliver a shock when prompted by pushing the "shock" button; repeat step 5.

If the AED advises no shock is needed... Check the pulse. Find the Adam's apple and slide your fingers towards you and down into the groove at the side of the neck. Check for signs of circulation for no more than 10 seconds.

7. If there is a pulse...Go to Next Care Steps. If there is no pulse...Do CPR until the AED reanalyzes.

Rescue Breathing:

1. If the victim shows signs of circulation but is not breathing...Give 1 rescue breath. Tilt the head back and lift the chin to open the airway. Pinch the nose shut. Take a breath and breathe slowly into the victim until the chest clearly rises.
2. Continue to give 1 rescue breath about every 5 seconds. Do this for about 1 minute (12 breaths).
3. Recheck for signs of circulation. Find the Adam's apple and slide your fingers towards you and down into the groove at the side of the neck. Check for signs of circulation for no more than 10 seconds.
4. If there are signs of circulation but no breathing...Continue Rescue Breathing. If there are no signs of circulation...Go to CPR and Using and AED.

Appendix O ADAPT Electrical Drawings, Equipment Specifications, I/O List

Located in separate binder.