

DOT/FAA/TC-18/49

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Failure Mode and Effects Analysis on PEM Fuel Cell Systems for Aircraft Power Applications

February 2019

Final Report

This document is available to the U.S. public through the National Technical Information Services (NTIS), Springfield, Virginia 22161.

This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.



U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No. DOT/FAA/TC-18/49	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Failure Mode and Effects Analysis on PEM Fuel Cell Systems for Aircraft Power Applications		5. Report Date February 2019	
		6. Performing Organization Code	
7. Author(s) Michael Miller	8. Performing Organization Report No.		
9. Performing Organization Name and Address Teledyne Energy Systems, Inc. 10707 Gilroy Road Hunt Valley, Maryland 21031		10. Work Unit No. (TRAILS)	
		11. Contract or Grant No. DTFACT-16-C-00039	
12. Sponsoring Agency Name and Address FAA Seattle Headquarters 2200 S 216th St Des Moines, WA 98198		13. Type of Report and Period Covered Final Report	
		14. Sponsoring Agency Code AIR-671	
15. Supplementary Notes The FAA William J. Hughes Technical Center Aviation Research Division COR was Michael Walz.			
16. Abstract The safety issues for use of a proton exchange membrane fuel cell (PEMFC) system providing onboard electrical power for a commercial aircraft has been evaluated. Teledyne Energy Systems, Inc. performed a failure mode and effects analysis on each of two potential applications. One PEMFC system was designated and designed for an application inside the aircraft cabin area and the other outside the aircraft cabin. These applications represent systems that require different levels of integration into the aircraft structure and represent electrical power requirements that are either critical or nonessential to safe aircraft operation. The operational risks identified for each application are similar, but the overall safety consequences are significantly different.			
17. Key Words Proton Exchange Membrane fuel cell, Aviation use of PEM Fuel Cell, Safety Issues of PEM fuel cell in aviation. PEM fuel cell Aviation applications		18. Distribution Statement This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 90	22. Price

ACKNOWLEDGEMENTS

This project was supported by contract DTFACT-16-C-00039 with the FAA William J. Hughes Technical Center. We thank Mike Walz—the Contracting Officer's Technical Representative for the project—for his advice, guidance, and understanding.

We thank Charles Lo, Staff Engineer with Honeywell Aerospace, for his assistance in defining the configuration and operational requirements for the PEMFC Emergency Power System design and for participating with the team in all Failure Modes and Effects Analysis (FMEA) study sessions for the system.

We also thank a source who would like to remain anonymous for assistance in defining and reviewing the design configuration and requirements for the PEMFC Medevac Power System.

The author would like to acknowledge and thank the other members of the team from Teledyne Energy Systems, Inc.—Bob Wynne, Rob Utz, and Stu Pass—for their contributions in the FMEA team sessions, performing the validation testing and technical review of the results and reports.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ix
1. INTRODUCTION	1
2. APPLICATION SELECTION	1
2.1 Emergency Power System—EPS	2
2.1.1 EPS—Design Parameters	3
2.1.2 EPS – Modes of Operation	5
2.2 Medevac Power System – MPS	6
2.2.1 MPS—Design Parameters	8
2.2.2 MPS—Modes of Operation	9
3. FMEA ANALYSIS	10
3.1 FMEA Methodology	10
3.2 FMEA Categories	12
3.3 FMEA Results Summary	12
3.3.1 FMEA Results – EPS Summary	13
3.3.2 FMEA Results—MPS Summary	17
3.4 FMEA Detail Listings	19
4. RECOMMENDATIONS	19
4.1 Recommendations—EPS	20
4.2 Recommendations—MPS	29
5. TESTING	37
5.1 Purpose	37
5.2 Testing	38
5.3 Test Procedures and results	39
5.4 Overall conclusions	39
APPENDICES	
A—EPS P&ID	
B—MPS P&ID	
C—EPS PRE-FLIGHT WORKSHEETS	
D—EPS STANDBY WORKSHEETS	

E—EPS POWER-PRODUCTION WORKSHEETS
F—MPS STARTUP WORKSHEETS
G—MPS POWER-PRODUCTION WORKSHEETS
H—MPS SHUTDOWN WORKSHEETS
I—TEST RESULTS

LIST OF FIGURES

Figure		Page
1	EPS layout	3
2	MPS layout	7
3	Hydrogen leak time response	8
4	FMEA example worksheet	11
5	EPS overall risk ranking charts	13
6	MPS overall risk ranking charts	13
7	Baseline Polarization Curves	40

LIST OF TABLES

Table		Page
1	EPS interface capacities	4
2	MPS interface capacities	9
3	Category definitions	12
4	RPN definitions	12
5	EPS FMEA Statistics	14
6	EPS overall risk ranking by component	15
7	MPS FMEA statistics	17
8	MPS overall risk ranking by component	18
9	Detail listing appendices	19
10	Proposed Tests	38

LIST OF ACRONYMS

EPS	Emergency Power System
FMEA	Failure Modes and Effects Analysis
MPS	Medevac power system
P&ID	Piping and instrumentation diagram
PEM	Proton exchange membrane
PEMFC	PEM fuel cell
RAT	Ram Air Turbine
RPN	Risk priority number
TESI	Teledyne Energy Systems, Inc.

EXECUTIVE SUMMARY

Teledyne Energy Systems, Inc. (TESI) has been funded by the FAA to perform two failure mode and effects analyses (FMEAs) and associated validation testing for PEM Fuel Cells (PEMFC). The FMEAs serve as initial steps in identifying the risks associated with operating and maintaining a PEMFC system on a commercial aircraft.

The two applications for study were selected to represent contrasting applications to cover the broadest range of criteria relevant to aircraft safety. The two applications are:

- A PEMFC emergency power system (EPS) to replace the ram air turbine (RAT) currently used to generate emergency power from the airstream.
- A PEMFC medevac power system (MPS) to provide independent electrical power to the medical equipment on an aircraft dedicated to medevac service.

Each application represents an electrical power requirement that is either critical to aircraft safety for the EPS or nonessential to aircraft operation for the MPS. The operational risks identified for either application are in many cases similar, but the overall safety consequences identified are significantly different.

For the studies, TESI has developed air-independent PEMFC system configurations and defined the operational procedures supporting several modes of operation for the two applications. The PEMFC stack for each application was designed for the appropriate power. System components were selected and sized to support the stack. Reactant storage vessels were sized to meet the overall energy requirement for the application. A piping and instrumentation diagram (P&ID) has been developed for each system to show the relationship and function of all the components. The P&ID and a system block diagram are the principal references for each FMEA.

The customary team-based FMEA procedure with a standard data-recording format was used to perform the analysis. The team met for 3 hours once a week for numerous weeks to complete the analysis for each study. The data were captured with commercial FMEA software. Overall study statistics and the individual risk levels of individual components are present in the report.

The FMEAs provide recommendations on issues for which the FAA will need to specify requirements for suppliers requesting to certify PEMFC systems for commercial aircraft service. The worksheets from the FMEA studies and a list of the recommendations are presented in the appendices.

Following the analysis, a list of prospective tests was generated to support some of the assumptions used in the studies and some of the results from each of the FMEAs. The objective of these tests is to validate the causes and effects used for the various failure modes. Testing was completed on 14 of the 17 tests proposed. The procedures and results are in the last appendix. Despite being exposed to extreme and severe conditions, the PEMFC performance held up, and some cases exceeded expectations.

1. INTRODUCTION

There is increasing interest in using fuel cell (FC) power systems on aircraft. Proton exchange membrane fuel cell (PEMFC) systems are maturing and used in automotive and industrial applications. For the aircraft industry, there are potential fuel savings and carbon emission reductions, but there are also substantial challenges. Specific power (W/kg) is lower than most power systems currently used on aircraft, so it is potentially heavier, and it uses hydrogen fuel, so it creates unfamiliar hazards and operational considerations. In support of the FAA interest in realizing the use of proton exchange membrane fuel cell (PEMFC) systems onboard commercial aircraft, Teledyne Energy Systems, Inc. (TESI) has performed separate failure mode and effects analyses (FMEAs) on two potential applications for commercial aircraft. A conceptual design has been developed for each PEMFC system, including component sizing and selection. A separate FMEA has been performed on each design to identify high-risk failure modes. Design improvements have been recommended to lower the high-risk failure modes, and component-level testing has been performed to validate the effect of select failure modes.

The two applications were selected to represent contrasting applications for the broadest range of criteria and those most relevant to the FAA. The PEMFC systems were designed to provide electrical power for one application inside the aircraft cabin area and one outside the aircraft cabin. The applications represent systems requiring different levels of integration into the aircraft structure. They also represent electrical power requirements, which can be considered either critical or nonessential to safe aircraft operation. The operational risks, identified for either application, are similar, but the overall safety consequences are significantly different. Failure of the nonessential application does not affect aircraft safety. Critical system failure prevents continued safe flight.

After selecting the two target applications, TESI contacted several aircraft and aircraft-component manufacturers to provide system performance and operation requirements and to help evaluate how to integrate each system design into the aircraft. Possibly due to the nature of the project, a study of failure modes of onboard equipment, there was much reluctance from those in the aircraft industry to participate. Finally with the help of the FAA, TESI was able to get one participant for each application. Based on input from the aircraft manufacturers, the PEMFC systems were sized and designed to provide power for two commercial aircraft applications.

2. APPLICATION SELECTION

The PEMFC system designs and the modes of operation chosen for each of the applications formed the basis for the FMEAs. The PEMFC stack for each application was designed for the appropriate power, and supporting components were selected and sized to support the stack. Reactant storage vessels were sized to meet the overall energy requirement for the application. A piping and instrumentation diagram (P&ID) has been developed for each system to show the relationship and function of all the components. This is an important reference for use in performing the FMEA. The P&ID with the design parameters and operation limits, along with a listing of the components and their features, have been created as part of the design effort. Also a list of system interfaces and a system layout block diagram have been developed. The descriptions that follow provide the assumptions selected for operation of the PEMFC systems specifically for each application.

TESI has performed an FMEA on each PEM fuel cell (PEMFC) system design for two different aircraft applications. The first application studied is an emergency power PEMFC system that replaces the present ram air turbine (RAT) on a narrow-body commercial aircraft platform (B737 or A320 class). This application requires a high level of integration into the aircraft, providing a critical source of reserve power. The reserve power is required for only 1 hour but must be available to provide full power in 6 seconds. The quick-start requirement makes it necessary to have the PEMFC system in a continuous, warm standby condition. The permanent standby condition is unusual for a PEMFC application and became a major consideration in the FMEA. In addition to the continuous standby and very short power-production modes of operation, a pre-flight check mode has been specified and studied to ensure system availability when needed.

The second PEMFC application studied is power for use with a medevac system on a mid- to large-size business class jet aircraft. This system provides continuous independent power for up to 8 hours. The system is portable, not constrained to the aircraft, so it can be installed and then removed to allow the aircraft to be used for other functions. The system runs with the conventional startup, continuous power production, and shutdown modes of PEMFC operation. A standby condition is not required for the medevac application.

Both applications are run as air-independent PEMFC systems, using pressurized hydrogen and oxygen gas for reactants. The use of pressurized tanks for H₂ is currently the most advanced and simplest form of H₂ storage. Tanks and associated valves and instrumentation have been developed for pressures up to 700 bar (10,000 psia) for use in the automotive market. A more conservative H₂ storage pressure of 350 bar (5000 psia) has been selected for use in the two aircraft applications studied here. There is a greater availability of tanks and components rated at this pressure. Both designs use Type 3 vessels, which include an aluminum liner to minimize hydrogen loss by diffusion.

The use of pressurized O₂ allows the PEMFC systems to run independently of the aircraft air-pressure system. This enables self-sufficient operation at high altitude without the need for an air compressor. Air-independent operation with a closed oxygen cathode loop eliminates the need for humidifiers on an incoming air stream. The only interaction the reactants have with the environment is a periodic purge of accumulated inert gases, which build up over time. The direct use of oxygen also ensures high-efficiency energy conversion, which minimizes the amount of heat required to be rejected. An O₂ storage pressure of 200 bar (3000 psia) has been selected for both applications. This pressure is currently the maximum allowable for most industrial gaseous oxygen systems.

2.1 EMERGENCY POWER SYSTEM—EPS

The EPS is located in the space currently occupied by the RAT emergency power system.

Figure 1 outlines the main components. The H₂ and O₂ tanks are fixed in the system structure and are filled in place. The liquid to air heat exchanger is part of a self-contained thermal control system that rejects process heat to the ambient conditions in the unconditioned space surrounding the system. The design of the fuel cell stack allows the coolant to contain a glycol antifreeze. The antifreeze coolant prevents freezing in the heat exchanger, coolant tank, coolant circuit

components, and fuel cell stack when the system is not in the active standby condition. The P&ID in appendix A details all the system components that were considered in the FMEA.

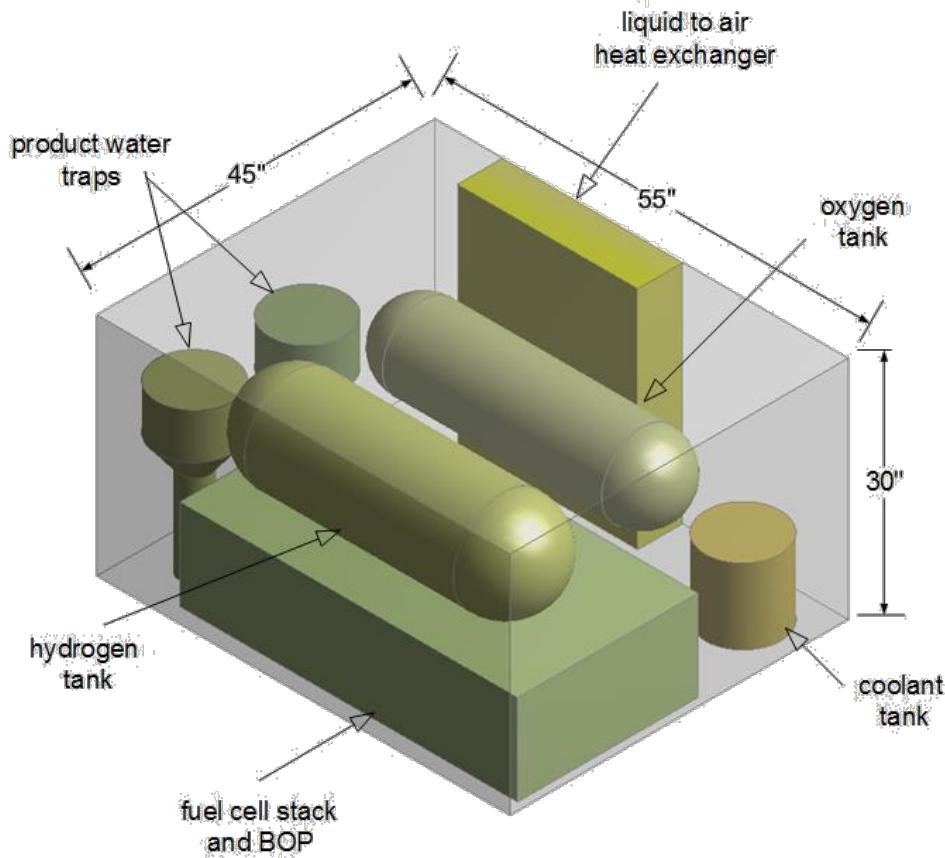


Figure 1. EPS layout

The EPS must be ready to come online immediately and provide up to 30kW of critical emergency power at 230 Vac. The system operates outside of the conditioned cabin and receives reactants from pressurized hydrogen and oxygen storage. Both product water and hydrogen, and oxygen from system relief valves, are vented overboard. The hydrogen and oxygen vent purge valves are vented to the ambient-air environment surrounding the system. The system uses a self-contained thermal control system, which rejects heat to the same surrounding air environment.

2.1.1 EPS—Design Parameters

The overall system design parameters and operational limits used for the EPS system design and referenced by the FMEA are listed as follows:

- Air independent—H₂ and O₂ reactants
- System physically located in unconditioned area of the aircraft currently containing the RAM
- Volume envelope = 45" x 55" x 30"
- Weight of selected components = 330 lb

- Maximum output power = 30kW (10kW to electric buss, 20kW to power hydraulic pump motor)
- Load profile is constant at maximum power
- System output voltage = 230V
- High pressure, Type 3 gas reactant storage – 3.23 lb H₂ at 5000 psia, 25.8 lb O₂ at 3000 psia
- Self-contained, system level thermal control, liquid coolant to air heat exchanger
- Heat rejection sink – ambient ram air at 110 knots per hour, -65°F to 140°F
- Altitude—sea level to 43,000 ft
- Autonomous process control with remote alarm indication
- Cockpit interface panel for remote startup and standby and alarm indication
- Startup time—6 seconds full power from standby
- Standby duration—6 hours, coolant system active with auxiliary coolant heater power on
- Active power delivery duration—1 hour producing 30kW

The system interfaces and their required capacities are listed in table 1.

Table 1. EPS interface capacities

Interface	Capacity
hydrogen storage fill	3.23 lb H ₂ at 5000 psia
oxygen storage fill	25.8 lb O ₂ at 3200 psia
coolant tank fill	3 gal at 1 atm
relief valve RV1 vent	up to 3.23 lb H ₂ at > 5300 psia
relief valve RV2 vent	up to 25.8 lb O ₂ at > 3200 psia
relief valve RV3 vent	up to 3.23 lb H ₂ at > 50 psia
relief valve RV4 vent	up to 25.8 lb O ₂ at > 50 psia
solenoid vent valve SV5	H ₂ at < 50 psia
solenoid vent valve SV6	O ₂ at < 50 psia
solenoid drain valve SV3	H ₂ O at < 50 psia
solenoid drain valve SV4	H ₂ O at < 50 psia
coolant tank drain	3 gal at 1 atm
product water tank drain	3.54 gal at 1 atm
heat exchanger air	27kW at up to 600 cfm

The amount of ventilation through the space surrounding the system is currently undefined so that it was not possible for the study to assess the allowable level of a hydrogen leak that remains below an acceptable lower explosion limit (LEL). This issue resulted in a recommendation (EPS Recommendation Reference #8) for further review of the ventilation features of the space and an acceptable method of detecting the hydrogen concentration level.

2.1.2 EPS – Modes of Operation

Three modes of operation are defined for the PEMFC EPS. They include the following:

- Pre-flight—check for fluid fills and to verify FC stack functionality
- Standby—maintain the system operating temperature for immediate full power availability
- Emergency power production—provide independent FC stack power for flight control

The pre-flight fluid check is intended to verify that the reactant and the coolant subsystems are filled with fluids. Additionally, the functionality of many of the EPS components is checked before placing the system in the standby mode. Pressure and temperature readings are checked to be within an acceptable range to confirm that they are functioning. Electrical power for the pre-flight mode originates from the main power of the aircraft.

The pre-flight check monitors the reactant storage pressure transducers (PT1, PT2) for correct reactant storage pressure and the inlet pressure transducers (PT5, PT6) for correct reactant pressures at the FC inlets. The coolant pump (M3) is operated, and the level sensor (L3) and flow sensor (FS1) are monitored for acceptable coolant level and flow. The coolant tank heater (HT1) is turned on to check that it is functioning, and the temperature sensors (T1 and T2) are monitored to check that they are responding.

The inlet isolation valves (SV1, SV2) are opened and the vent valves (SV5, SV6) are closed to allow the reactants to pressurize the FC stack. Following the stack pressurization process, the individual cell voltages are monitored for acceptable levels at the open-circuit condition. With the stack pressurized, the reactant pumps (M1, M2) are operated momentarily, and the current draw on each pump motor is monitored to verify pump operation.

After an acceptable pre-flight check, the FC stack is evacuated. The inlet valves (SV1, SV2) and vent valves (SV5, SV6) are closed. A small resistance load is applied to the FC stack, and the reactants are consumed. As the pressure in the stack drops the hydrogen inlet isolation valve (SV1) is cycled to provide enough hydrogen to maintain a stoichiometric mix for complete reaction. When the evacuation is complete, the system enters the standby mode.

In the standby mode, the EPS continues to use main aircraft power. The coolant pump remains on, and the heater in the coolant tank is turned on. The coolant subsystem remains active, allowing the temperature to rise to the operating temperature. When the temperature reaches the operating point at the inlet temperature sensor (T3), it is actively controlled and maintained by cycling the heater on and off to maintain the system at the operating temperature.

The inlet isolation valves (SV1, SV2) and the vent valves (SV5, SV6) remain closed in the standby mode. All the EPS instrumentation remains active, monitoring the conditions in each reactant subsystem and the coolant subsystem. The standby mode keeps the FC stack at the operating temperature, ready to quickly provide emergency power if needed.

When main aircraft power is lost and emergency power is requested, a battery in the FC control subsystem initiates independent FC control. The inlet isolation valves (SV1, SV2) are open to

pressurize the FC stack subsystem. The pressurization procedure takes several seconds, after which FC control power is maintained autonomously by the FC system itself. Full power can be delivered to the aircraft electrical load at this time. The reactants can provide 30kW of continuous power for 1 hour. The coolant subsystem provides active thermal control. The water management components (WT1, WT2, LS1, LS2) process and monitor the product water. The vent and drain valves (SV3, SV4, SV5, SV6) remain active.

Shutdown of the system is initiated by the consumption of all stored reactants or removal of all control power to the FC system. The normally closed inlet valves (SV1, SV2) isolate the FC stack from the reactant supply. The normally closed vent valves (SV5, SV6) capture any remaining reactants in the FC stack.

2.2 MEDEVAC POWER SYSTEM – MPS

The MPS is located in the rear luggage compartment, which is accessible from the cabin. It is removable so that the aircraft can be reconfigured for applications other than medevac. The MPS is installed and removed through the luggage compartment exterior access hatch. Figure 2 outlines the main components. Exchangeable H₂ and O₂ tanks are used for refueling.

The liquid-to-air heat exchanger is part of a self-contained thermal control system, which rejects processed heat to the ambient conditions in the luggage compartment and the adjacent cabin. The aircraft HVAC system can handle a supplemental heat load of up to 5kW. The PEMFC system rejects 4300W.

Air-independent operation of the PEMFC allows a closed loop, oxygen reactant system to be used. This eliminates the need to consume cabin oxygen content. The use of oxygen also maximizes energy conversion efficiency, which minimizes heat load to the aircraft HVAC system. The P&ID in appendix B details all the system components that were considered in the FMEA for the medevac system.

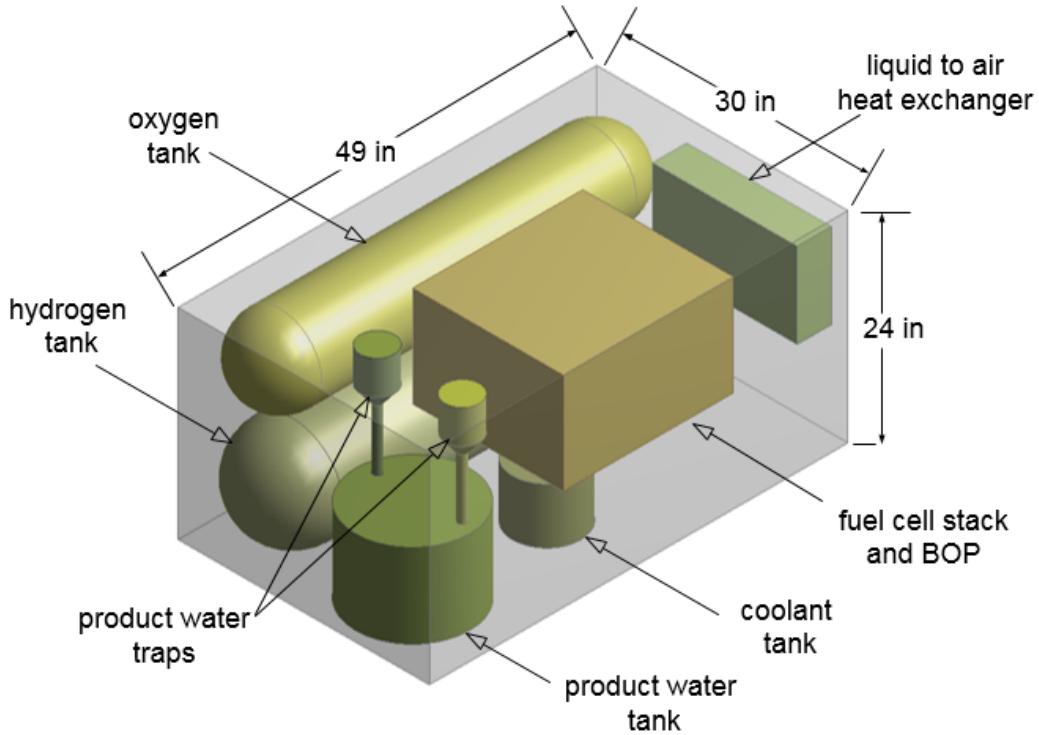


Figure 2. MPS layout

The gas-venting locations—including high-pressure venting for the reactant storage, system relief valves, and H₂ purge—were selected for a specific aircraft. The high-pressure H₂ vent leaves behind the rear-mounted engines to avoid dumping H₂ into the engine intake. The high-pressure O₂ vent is through the luggage compartment hatch. The intermittent low-pressure H₂ purge also vents through the hatch. The low-pressure O₂ purge vents into the luggage compartment. A tank to contain the water produced by the system is included in the system. This tank is drained when the system is refueled.

The PEMFC system for the MPS application is self-controlled with alarms and shutdowns for individual failure modes. H₂ detection in the luggage compartment is interlocked to the FC system to provide system shutdown if a hydrogen concentration of 2% (50% LEL) is exceeded and to provide an alarm at 25% LEL.

The conditioned interior space of the aircraft, including the cabin and luggage compartment, is approximately 1150 ft³. It is ventilated to meet the 0.55 lbm/min per occupant requirement (FAR25) for fresh air. This is equivalent to 100 cu ft/min for standard aircraft air conditions (10.9 psia, 72°F) when certified for 10 occupants. At this rate of ventilation, an H₂ leak of up to 2 cu ft/min will remain under the allowable 50% LEL (2%) concentration. The time response for this leak (designated as 1x) and leaks of 2x and 4x are shown in figure 3. The time durations for leaks of 1x, 2x, and 4x to reach 50% LEL are 1 hour, 8 minutes, and 4 minutes, respectively. As a point of reference, these volumetric leak rates can be compared to the total hydrogen consumption rate of the PEMFC at full power. This represents a leak rate equivalent to all the hydrogen required for producing power. At standard aircraft conditions (10.9 psia, 72°F) this rate is 2.4 cu ft/min.

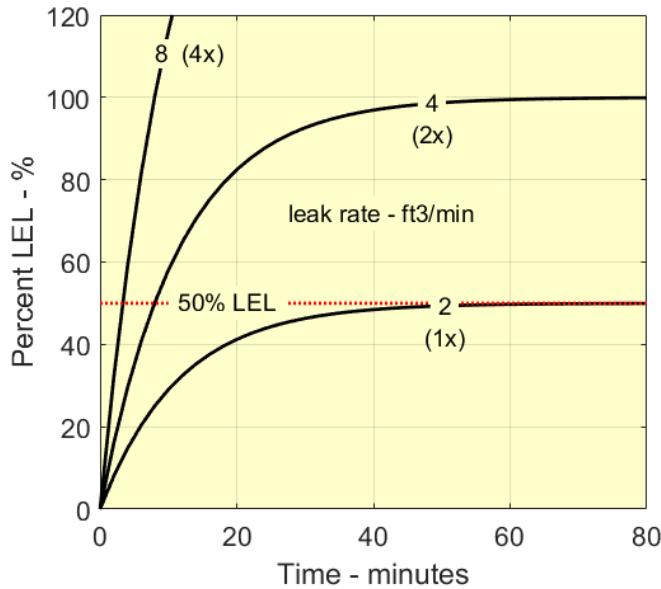


Figure 3. Hydrogen leak time response

2.2.1 MPS—Design Parameters

The overall system-design parameters and operational limits used for the MPS system design and referenced by the FMEA are listed as follows. The system interfaces and their required capacities are listed in table 2.

- Air independent—H₂ and O₂ reactants
- Removable system is located in luggage compartment accessible from cabin area
- Volume envelope = 49 in x 30 in x 24 in
- Weight of selected components = 208 lb
- Maximum output power = 5kW
- Load profile is assumed constant at maximum power
- System output voltage = 28Vdc
- High pressure, type 3 gas reactant storage—4.27 lb H₂ at 5000 psia, 34.1 lb O₂ at 3000 psia
- Self-contained, system-level thermal control, liquid coolant to air heat exchanger
- Heat rejection sink—conditioned cabin air
- Product water from PEMFC is captured and stored onboard
- Altitude—sea level to 43,000 ft
- Autonomous process control
- Local startup and shutdown control, automated process control alarms and shutdowns with remote manual shutdown
- Startup time—10 minutes to full power from cold start
- Active power delivery duration—8 hour producing 5kW

Table 2. MPS interface capacities

Interface	Capacity
hydrogen storage fill	4.27 lb H ₂ at 5000 psia
oxygen storage fill	34.1 lb O ₂ at 3000 psia
coolant tank fill	1 gal at 1 atm
relief valve RV1 vent	up to 4.27 lb H ₂ at > 5300 psia
relief valve RV2 vent	up to 34.1 lb O ₂ at > 3000 psia
relief valve RV3 vent	up to 4.27 lb H ₂ at > 50 psia
relief valve RV4 vent	up to 34.1 lb O ₂ at > 50 psia
solenoid vent valve SV5	H ₂ at < 50 psia
solenoid vent valve SV6	O ₂ at < 50 psia
solenoid drain valve SV3	H ₂ O at < 50 psia
solenoid drain valve SV4	H ₂ O at < 50 psia
coolant tank drain	1 gal at 1 atm
product water tank drain	4.65 gal at 1 atm
heat exchanger air	4.3kW at 100 cfm

2.2.2 MPS—Modes of Operation

Three conventional modes of operation are defined for the PEMFC medevac power system (MPS). They are the following:

- Startup—pressurize fuel cell stack and bring system up to operating temperature
- Power production—provide independent FC stack power for medevac service
- Shutdown—safely remove load and depressurize system

Battery power, required only for initial MPS startup, is maintained in the controls subsystem located within the fuel-cell stack and BOP envelope. Before energizing the FC stack, the reactant storage pressures (PT1, PT2) and the coolant liquid level (LS3) are checked for the proper amounts. Activating the FC stack begins by opening the normally closed inlet valves (SV1, SV2) to pressurize the stack with reactants. Individual cell voltages are monitored for acceptable level at the open circuit condition. After initial startup, system controls are powered by the fuel cell. Startup continues with an electrical load applied to the FC stack from the bootstrap heater in the coolant tank. The heater brings the system up to operating temperature, at which time the coolant subsystem begins to provide active thermal control.

The startup process also provides an opportunity for all the instrumentation in the MPS to be monitored for accuracy. Pressure, temperature, level, and flow readings should be within their acceptable range. Errant readings can cause system alarms, which may lead to diagnostic procedures for instrument calibration.

Following startup the MPS provides direct 28Vdc power to the medevac service load from 1.5 to 5 kW for up to 8 hours. The coolant subsystem provides active thermal control, rejecting heat from a liquid to air heat exchanger (HX1) to the ambient air conditions in the aircraft. The product water traps within the FC subsystem (WT1, WT2) collect and deliver excess product water into a product water tank (V4).

After removing the medevac service load the MPS production is shut down by closing the reactant supply. Isolation valves (SV1, SV2) and vent valves (SV5, SV6) are allowed to go to their normally closed position. The stack is evacuated by applying a small resistance load to the FC stack and allowing the reactants to be fully consumed. The stack remains in the vacuum state until the next startup process.

3. FMEA ANALYSIS

An FMEA is a methodology described as a systematic group of activities intended to recognize and evaluate the potential failures of a product or process and its effects. A potential failure mode is defined as the manner in which an item (component or system) could potentially fail to meet the function or design intent of the item. Often defined as anti-functions, failure modes are identified as specifically as possible and described in physical terms. The analysis lists all potential failure modes for each item and item function. Potential effects of failure are defined as the effect of the failure on the function of the item. Effects may also extend to the higher sub-system or system level. The goal is to identify actions that could eliminate or reduce the probability of the potential failure occurring.

It is important to have a logging system in place to document the analysis as it progresses in real time. TESI uses FMEA-Pro8, a process hazardous analysis software package from Dyadem, to record and track the results as the analysis progresses. The software also provides various reports and charts to summarize the analysis and identify the failures with the highest risk.

3.1 FMEA METHODOLOGY

The FMEA begins by dividing the system into workable nodes. These nodes are identified as sections or subsystems with similar process functions on a process schematic or a P&ID. The P&IDs for both the EPS and MPS are divided in to four nodes: hydrogen storage, oxygen storage, fuel-cell sub-system, and coolant sub-system. The normal design conditions are listed for each node. All components subject to potential failure are listed in FMEA-Pro8 for each node, as called out on the P&ID.

The main activity of the FMEA process is accomplished with a team. A group of individuals familiar with the system is assembled to investigate potential failures for each of the components. The team determines causes, effects, and controls for each failure mode. Effects are determined without consideration of any controls that may be in place and assigned a numerical severity. Causes for each potential failure mode are assigned probability of occurrence. A level of detection is also assigned representing the probability that the deviation will be discovered. The product of the severity, occurrence, and detection levels is the numerical risk or the risk priority number (RPN). The process continues for each component.

Recommendations are required to be recorded for all elevated failure risks. The recommendations are intended to offer suggestions for further study to provide design improvements that will mitigate the high risk. In some cases, recommendations were recorded for lower-level risks to indicate potential design enhancements or to note and explain existing features that are currently in place.

The study data are entered into a worksheet in the FMEA-Pro8 software. An example worksheet is shown in figure 4. The process is repeated for the entire system for each of the system operating modes. The operational modes for the EPS and MPS are listed and described in sections 2.1.2 and 2.2.2.

Design System:	PEMFC Emergency Power - Power Production							
Items:	Fuel cell stack anode FC1-H2							
Item Functions:	reacts H2 to create protons and electrons							
Comments:								
Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause / Mechanism of Failure	Occ	Current Design Controls (Detection)	Det	RPN	Recommendations
external H2 gas leak	decrease in pressure at cell	2	internal failure at cell	1	alarm low cell voltage	3	12	Investigate detection methods for external H2 leak
	loss of reactant	3						Examine risk of continued operation during slow reactant leak
	external H2 reaction	4						
	voltage decay at cell	2						
cross leak H2 to coolant	loss of reactant	3	internal failure at cell	1	none	4	12	Research coolant alternatives for operation in low ambient temps
	H2 into coolant	2						Investigate method to detect a H2 leak into coolant
cross leak H2 to cathode	voltage decay at cell	2	internal failure at cell	1	alarm low cell voltage	1	2	
	reaction with O2	2	MEA degradation	1	alarm low cell voltage	1	2	
water blocking anode reactant path	voltage decay at cell	2	excess condensation in cell	1	alarm low cell voltage	1	2	
			loss of hydrophobicity in cell	1	alarm low cell voltage	1	2	
dehydrated cell - anode	voltage decay at cell	2	over effective product water removal	1	alarm low cell voltage	1	2	
inert gas buildup - anode	voltage decay at cell	2	reactant purity	3	monitor cell voltage and amp-hr for purge	1	6	Compute at what impurity level a purge is needed for 1 hour mission

Figure 4. FMEA example worksheet

The FMEA team for the EPS application included the following individuals: Mike Miller, Bob Wynne, Rob Utz, all of whom are TESI employees, and Charles Lo, who is with Honeywell Aerospace. The team met for 3 hours once a week for 7 weeks during April and May 2017. The team studied all the components in all four system nodes of the EPS (hydrogen storage, oxygen storage, fuel cell sub-system, and coolant sub-system), operating in three different modes (pre-flight, standby, and power production).

The team for the MPS application included: Mike Miller, Bob Wynne, Rob Utz, and Stu Pass, all from TESI. The team met for 3 hours once a week for 5 weeks during July and August 2017. The team studied all the components in all four system nodes of the MPS in three different operating modes (startup, power production, and shutdown).

3.2 FMEA CATEGORIES

The number of levels of severity (S) for each deviation and the number of levels of occurrence (O) and detection (D) must be large enough to provide reasonable differentiation but not too large to be overly cumbersome and time consuming during the team sessions. For this FMEA, TESI used four levels for each category with a corresponding definition increasing the significance at each level. The four levels with their definition for each category are listed in table 3.

Table 3. Category definitions

Level	Severity	Occurrence	Detection
1	No damage to equipment	Not expected to occur during system life	Almost certain, detected 98%
2	Minor damage or runs at reduced capacity	Could occur once during system life	High, detected 90%
3	Moderate damage or runs for limited time	Could occur several times during system life	Moderate, detected 70%
4	Total failure	Could occur on each use	Low, detected 50%

The product of the severity (S), occurrence (O), and detection (D) is defined as the Risk Priority Number ($S \times O \times D = RPN$). The numerical ranges for the four RPN levels and their definitions are listed in table 4.

Table 4. RPN definitions

RPN	Description
1–4	Acceptable—No risk-control measures are needed
6–12	Acceptable With Control—Risk-control measures are in place
16–36	Not Desirable—Risk-control measures need to be introduced
36–64	Unacceptable

3.3 FMEA RESULTS SUMMARY

Results for both studies in each of their three operational modes are summarized in the following sections. The numbers in the overall statistics tables include totals, averages, and maximum values in several categories for each mode of operation. The statistics show the broad scope of the studies and the overall risk for each of the operational modes. For either application, the numbers indicate only a slight difference in overall risk between the three modes of operation. The overall risk-ranking charts (figures 5 and 6) show the overall risk for various levels of severity and occurrence. Again, the overall levels and trends are similar for each of the three modes of operation for both applications.

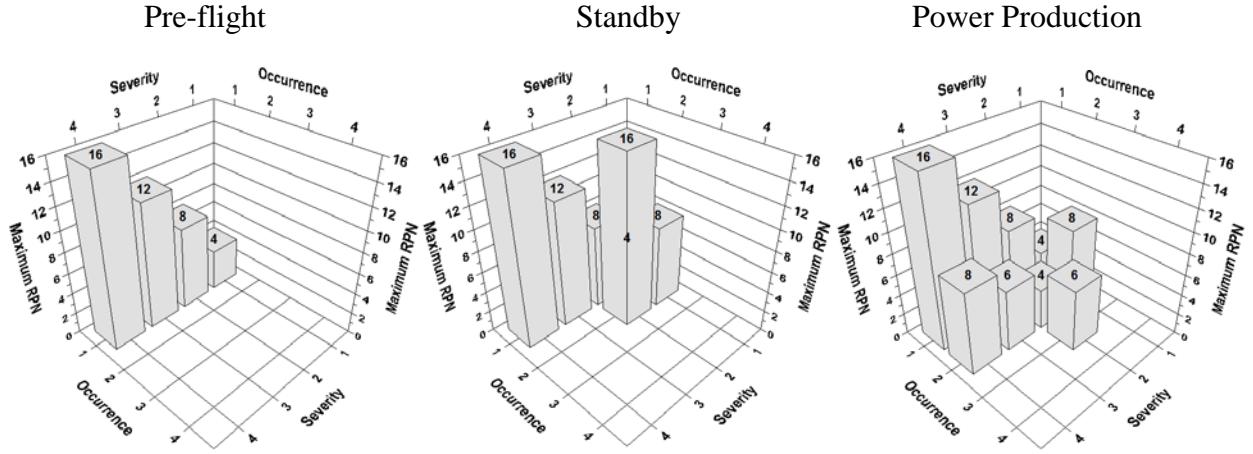


Figure 5. EPS overall risk ranking charts

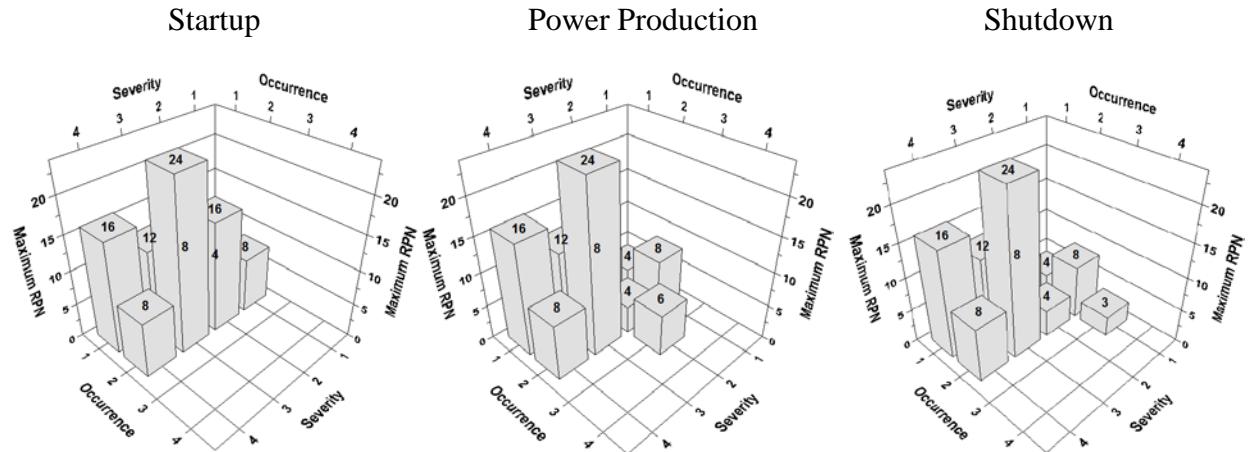


Figure 6. MPS overall risk ranking charts

The importance of the pre-flight mode and the long standby mode condition for the EPS application is even more evident when looking at the overall component risk rankings in table 6. The higher number of maximum RPNs for both pre-flight and standby emphasize a need to focus on the higher risk components regardless of the operational mode.

A significant difference in risk is more evident when comparing the risk ranking by component tables (tables 6 and 8). These tables show the importance of conducting the FMEA on a detailed component-by-component basis for all operational modes. The risk ranking by component tables show a significant difference in risk for some components depending on the mode of operation. Recommendations for follow-on design and analysis are made based on high risk failures identified for the individual components.

3.3.1 FMEA Results – EPS Summary

The EPS application requires power production for only a short period. The preparation during pre-flight and the system condition during standby are important for reliable operation during this critically short time. The overall statistics shown in table 5 indicate that although the number of

failure modes, effects, and causes are fewer for the pre-flight and standby modes, the average risk per cause is higher. This is partly due to a higher number of maximum RPNs for these two modes. The 3D plots in figure 5 show a wider distribution of overall severity and occurrence for the power-production mode, but the maximum RPNs are the same. The statistics indicate the importance for considering both pre-flight and standby issues in the EPS design.

Table 5. EPS FMEA Statistics

Operational Mode	Pre-flight	Standby	Power Production
Number of Study Items	45	45	45
Potential Failure Modes	135	119	141
Potential Effects of Failure	174	164	239
Potential Causes of Failure	159	165	195
Current Design Controls	182	174	249
Sum Total of RPN	830	781	468
Average RPN per Cause	5.2	4.7	3.9
Max RPN Value	16	16	16
Number of Max RPN	12	18	9
Number of Recommendations	11	21	22

Table 6. EPS overall risk ranking by component

Part Description	P&ID No.	Pre-Flight	Standby	Power
1. H2 storage tank relief valve RV1	RV1	4	4	4
2. O2 storage tank relief valve RV2	RV2	4	4	4
3. H2 delivery relief valve RV3	RV3	4	9	12
4. O2 delivery relief valve RV4	RV4	4	9	12
5. H2 delivery inlet solenoid valve, NC SV1	SV1	4	16	4
6. O2 delivery inlet solenoid valve, NC SV2	SV2	4	16	4
7. H2 water trap drain solenoid valve, NC SV3	SV3	12	4	6
8. O2 water trap drain solenoid valve, NC SV4	SV4	12	4	6
9. H2 vent solenoid valve, NC SV5	SV5	8	4	8
10. O2 vent solenoid valve, NC SV6	SV6	8	4	8
11. H2 storage manual isolation valve, MV4	MV4	4	16	4
12. H2 storage manual fill valve MV1	MV1	4	4	4
13. O2 storage manual isolation valve MV2	MV2	4	16	4
14. O2 storage manual fill valve MV3	MV3	4	4	4
15. H2 delivery pressure regulator FPR1	FPR1	4	16	4
16. O2 delivery pressure regulator FPR2	FPR2	4	16	4

Table 6. EPS overall risk ranking by component (continued)

Part Description	P&ID No.	Pre-Flight	Standby	Power
17. H2 storage pressure transmitter PT1	PT1	16	12	12
18. O2 storage pressure transmitter PT2	PT2	16	12	12
19. H2 stack pressure transmitter PT3	PT3	4	4	4
20. O2 stack pressure transmitter PT4	PT4	4	4	4
21. H2 delivery pressure transmitter PT5	PT5	4	4	1
22. O2 delivery pressure transmitter PT6	PT6	4	1	1
23. H2 storage temperature transmitter T1	T1	4	4	4
24. O2 storage temperature transmitter T2	T2	4	4	4
25. Coolant inlet temperature transmitter T3	T3	3	3	3
26. Coolant outlet temperature transmitter T4	T4	1	1	1
27. H2 water trap level switch LS1	LS1	16	8	8
28. O2 water trap level switch LS2	LS2	16	8	8
29. Coolant tank level switch LS3	LS3	16	8	8
30. Coolant flow switch FS1	FS1	4	1	4
31. H2 recirculation pump M1	M1	12	4	16
32. O2 recirculation pump M2	M2	12	4	12
33. Coolant circulation pump M3	M3	4	2	3
34. H2 water trap WT1	WT1	2	2	4
35. O2 water trap WT2	WT2	2	2	4
36. H2 storage tank V1	V1	4	4	4
37. O2 storage tank V2	V2	4	4	4
38. Coolant reservoir V3	V3	2	2	3
39. System heat exchanger HTX1	HTX1	16	2	3
40. H2 storage fill port check valve CV1	CV1	4	4	4
41. Fuel cell stack anode FC1-H2	FC1-H2	16	2	12
42. Fuel cell stack cathode FC1-O2	FC1-O2	16	1	12
43. Fuel cell stack coolant FC1-C	FC1-C	4	12	3
44. O2 storage fill port check valve CV2	CV2	4	4	4
45. Coolant tank heater HT1	HT1	4	3	4

3.3.2 FMEA Results—MPS Summary

Throughout the mission cycle of the application, the operational modes of the MPS are typical of most PEM fuel cell applications. Short startup and shutdown operational modes precede and follow a longer power-production mode. The overall statistics for MPS study are shown in table 7. The number of causes, effects, and failure modes are higher for the extended power-production mode; however, the average RPN per cause is lower because of the higher number of design controls that exist during power production. The 3D plots in figure 6 show a similar distribution of overall severity and occurrence and the same maximum RPN for all three operational modes.

Table 7. MPS FMEA statistics

Operational Mode	Startup	Power Production	Shutdown
Number of Study Items	43	43	43
Potential Failure Modes	122	136	126
Potential Effects of Failure	186	228	155
Potential Causes of Failure	166	180	168
Current Design Controls	213	252	177
Sum Total of RPN	909	811	867
Average RPN per Cause	5.5	4.5	5.2
Max RPN Value	24	24	24
Number of Max RPN	2	2	2
Number of Recommendations	33	31	14

Similar to table 6, table 8 shows the importance of looking at the overall risks for individual components operating in modes other than power production. The larger number of high RPNs for both startup and shutdown emphasize a need to concentrate on all the high-risk components.

Table 8. MPS overall risk ranking by component

Part Description	P&ID No.	Startup	Power	Shutdown
1. H2 storage tank relief valve RV1	RV1	6	6	6
2. O2 storage tank relief valve RV2	RV2	6	6	4
3. H2 delivery relief valve RV3	RV3	9	4	4
4. O2 delivery relief valve RV4	RV4	9	4	4
5. H2 delivery inlet solenoid valve, NC SV1	SV1	16	4	16
6. O2 delivery inlet solenoid valve, NC SV2	SV2	16	4	16
7. H2 water trap drain solenoid valve, NC SV3	SV3	4	6	8
8. O2 water trap drain solenoid valve, NC SV4	SV4	4	6	8
9. H2 vent solenoid valve, NC SV5	SV5	16	8	8
10. O2 vent solenoid valve, NC SV6	SV6	8	8	8
11. H2 storage manual fill valve MV1	MV1	16	4	16
12. O2 storage manual fill valve MV2	MV2	16	4	4
13. H2 delivery pressure regulator FPR1	FPR1	4	4	16
14. O2 delivery pressure regulator FPR2	FPR2	4	4	16
15. H2 storage pressure transmitter PT1	PT1	3	3	3
16. O2 storage pressure transmitter PT2	PT2	3	3	3
17. H2 stack pressure transmitter PT3	PT3	16	16	16
18. O2 stack pressure transmitter PT4	PT4	16	16	16
19. Coolant inlet temperature transmitter T1	T1	4	3	3
20. Coolant outlet temperature transmitter T2	T2	1	1	1
21. H2 water trap level switch LS1	LS1	4	8	2
22. O2 water trap level switch LS2	LS2	4	8	2
23. Coolant tank level switch LS3	LS3	8	8	8
24. Coolant flow switch FS1	FS1	4	4	4
25. H2 recirculation pump M1	M1	16	16	12
26. O2 recirculation pump M2	M2	12	12	12
27. Coolant circulation pump M3	M3	4	3	4
28. H2 water trap WT1	WT1	2	4	4
29. O2 water trap WT2	WT2	2	4	4
30. H2 Leak Detector A1	A1	24	24	24
31. H2 delivery manual isolation valve MV3	MV3	16	4	4

Table 8. MPS overall risk ranking by component (continued)

Part Description	P&ID No.	Startup	Power	Shutdown
32. O2 delivery manual isolation valve MV4	MV4	16	4	16
33. H2 storage tank V1	V1	4	4	4
34. O2 storage tank V2	V2	4	4	4
35. Coolant reservoir V3	V3	4	3	1
36. Product water tank	V4	12	12	8
37. System heat exchanger HTX1	HTX1	3	3	4
38. Fuel cell stack anode FC1-H2	FC1-H2	12	12	4
39. Fuel cell stack cathode FC1-O2	FC1-O2	12	12	4
40. Fuel cell stack coolant FC1-C	FC1-C	3	3	3
41. Coolant tank heater HT1	HT1	4	4	4
42. H2 storage pressure gauge PG1	PG1	1	4	4
43. O2 storage pressure gauge PG2	PG2	1	4	4

3.4 FMEA DETAIL LISTINGS

The details developed and recorded in the worksheets for the FMEAs are provided in the appendixes. The listings are divided into the three operational modes for each of the two applications for a total of six listings. Table 9 identifies the mode and application for each of the appendices

Table 9. Detail listing appendices

Application	Operational Mode	Appendix
EPS	Pre-flight	C
EPS	Standby	D
EPS	Power Production	E
MPS	Startup	F
MPS	Power Production	G
MPS	Shutdown	H

4. RECOMMENDATIONS

Detailed recommendation statements are the final product of the FMEA. The recommendations are in most cases related to specific design issues that resulted from failure modes with the higher risk (RPN) values. They are actions that should be taken in the product-development phase to further refine the design to reduce the risk. In some cases, the recommendation references a

standard design process, procedure, or control in place that minimizes any expected risk from the failure mode being considered.

Each recommendation has an EPS or MPS reference number followed by a short descriptive phase. A reference to the component numbers used in the system P&ID and the modes of operation being considered are also listed. Some similar failure modes from the two studies resulted in the same recommendations. Some recommendations for each study are repeated in the following sections to maintain the complete set of recommendations for each application

4.1 RECOMMENDATIONS—EPS

EPS Reference #1—Consider adding filter downstream of reactant pump.

(M1, M2)—Power production mode

A failure mode can occur where the reactant pumps (M1 or M2) fail and produce contaminants that can then enter the FC stack. Adding a filter downstream of the reactant pumps will protect the FC stack from these contaminants. An additional filter should be considered at the exit of the FC reactant lines to protect the solenoid valves and reactant pumps from particles that could exit the FC stack, such as carbon fibers from the GDLs.

EPS Reference #2—Consider redundancy, also look at maintenance issues.

(MV2, MV4)—Standby mode

A failure can occur where the manual valves feeding the fuel cell system, located at the exit of the reactant storage tanks, fail closed. These valves are closed during refueling to isolate the filling process from the FC system. When the valves are closed, the downstream pressure will be maintained so there is no way to verify that the valve actually reopened. Adding a second manual valve in parallel with the existing ones will decrease the risk of a valve failing closed.

EPS Reference #3—Consider redundant level switches in water separators.

(LS1, LS2)—Power-production mode

A failure can occur if the level switch detects water when there is none. This will continually open SV3 or SV4 resulting in loss of reactant or reactant pressure at the FC stack. A second level switch can be added to minimize occurrence. An option to adding a second switch is to generate an algorithm that will close the solenoid valves after a predetermined time even if the level switch detects water. To ensure the solenoid valve is not plugged, the algorithm can wait for a corresponding loss in FC reactant pressure prior to closing the solenoid valve.

EPS Reference #4—Consider second PT to indicate adequate flow as indicated by pressure drop
(M1, M2)—Power production mode.

A failure can occur where the reactant pump(s) stop operating and the fuel cell performance decays because of flooding. Adding pressure transducers at the FC reactant outlet lines allows the system to monitor differential pressure across the FC to ensure adequate velocity to remove product water.

These additional pressure transducers also give redundancy for the existing ones. A second option is to measure reactant pump electrical current draw to indicate pump RPM, which relates to flow.

EPS Reference #5—Include a monitor for current draw on reactant recirculation pump.

(M1, M2)—Power production mode

See Reference #4 above

EPS Reference #6—Include a thermal switch on V3 for redundancy.

(HT1)—Power production and standby modes

Currently, there is not a temperature sensor in the coolant tank where the coolant heaters are located. The temperature sensor at the fuel cell coolant inlet controls the coolant heater. An over temperature thermal switch will provide an additional safety factor to ensure the coolant tank never overheats.

EPS Reference #7—Include a way to verify reactant tank PT accuracy.

(PT1, PT2)—Pre-flight mode

See reference #34 below

EPS Reference #8—Investigate detection methods for external H₂ leak.

(M1, WT1, V1, FC1-H2)—Power production and standby modes

A failure can occur if a hydrogen leak develops that increases the environmental hydrogen concentration to a dangerous level and ignites. A hydrogen-detection method would provide valuable information. A continuous flow of atmospheric air would purge the space around the FC system and a hydrogen detector placed where the flow exits (ideally at the top of the space). Testing may be necessary to ensure a COTS hydrogen detector will work effectively at the temperatures and ventilation flow rates the system will be exposed to.

EPS Reference #9—Investigate water-trap freezing possibility.

(WT1, WT2)—Standby mode

A failure can occur after the FC system has been operating, and residual water remains in the water separator well. When the aircraft is not in use and the ambient temperatures fall below 0°C, the water will freeze and potentially damage the water separator. Provisions must be allowed for freezing temperatures by either draining all residual water during pre-flight checkouts or by making the water separators freeze-tolerant. An algorithm can be developed that opens each water separator solenoid drain valve towards completion of the pre-flight check-outs, ensuring they are empty. Alternatively, the water separators may be designed so that, as the residual water in the separators freezes, it has the ability to expand without damaging the separator.

EPS Reference #10—Monitor coolant flow and stack temp for presence of coolant.

(LS3) – Standby mode

A failure can occur if the coolant tank level sensor stops working and the true coolant level is unknown. Using a coolant flow sensor (FS1) will provide evidence that there is adequate coolant to operate the system. Monitoring the coolant flow sensor along with the FC stack temperature provides an indication of sufficient coolant volume for near-term operation.

EPS Reference #11—Compute total product water available for worst-case flooding risk.

(WT1, WT2)—Power-production mode

The failure of the product water trap in either the hydrogen or oxygen recirculation circuits could allow the direct release of product water from the traps and cause flooding externally into the system enclosure. The worst-case level of flooding is determined by the amount of reactants available to produce water. The short mission of this application limits the amount of onboard reactants. The mass of onboard reactants total about 13 kg, which could produce 13 liters of water. This volume is slightly more than 1% of the total volume of the EPS PEMFC system enclosure. Although this volume is small, the location of components in overall system design should be addressed to prevent flooding of sensitive components.

EPS Reference #12—Consider monitoring stack pressure rise for detecting coolant leak.

(FC1-C)—Standby mode

During the lengthy standby mode, the anode and cathode half cells of the fuel cell stack are left in vacuum condition while the adjacent coolant sections of the stack maintain stack operating temperature with flowing, heated coolant. Major leakage of the coolant into either the anode or cathode could flood the stack, or a minor leak of a coolant containing antifreeze coolant could possibly poison the catalyst. This recommendation raises the question of whether a detectable increase in pressure is present from a coolant leak. Can the result of the vapor pressure from a coolant leak be detected? This should be calculated or simulated. If this pressure is significant enough to detect, then testing could be done to validate the results.

EPS Reference #13—Describe control to limit product water accumulation based on amp-hr count and its use as a secondary control/alarm.

(LS1, LS2)—Power-production mode

The failure of the level switch on either the hydrogen or oxygen water trap could lead to the drain valve not being actuated and the water trap overflowing. This would lead to excess water in the reactant recirculation circuit and flood of the fuel cell stack. TESI uses a control algorithm to compute product water production. Fuel cell amperage is directly proportional to the consumption rate of the hydrogen and oxygen reactants and the production rate of product water. The controller stores accumulated fuel cell amperage over time and determines when to open the drain valve. The drain event is allotted a certain amount of time. If the level switch does not reset after this event, an alarm will normally trigger a shutdown due to a defective level switch. However, for this critical application, the control algorithm should continue to run to extend the run time as long as possible.

EPS Reference #14—Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load.

(HT1)—Power-production, standby, and preflight modes

The coolant heater for this application is more than the standard bootstrap heater used for providing quick system startup. The heater is independently powered and must be sized to provide continuous heat to maintain the fuel cell system at its operating temperature in a high-altitude environment to provide immediate full power to the power-production mode from standby. The liquid-to-air heat exchanger for the system must be sized to remove the heat supplied by the coolant heater in a wide range of environmental conditions, including all ground-based environments to which the aircraft may be exposed.

EPS Reference #15—Describe how to size RV3/RV4 for full high-pressure storage flow.

(FPR1, FPR2)—Power-production and standby modes

Relief valves RV3 and RV4 protect the FC system from potential high-pressure exposure due to the failure of either of the forward pressure regulators, FPR1 or FPR2. These relief valves must be sized large enough to prevent excessive pressure buildup at the inlets of the isolation solenoid valves SV1 or SV2. If fully opened, when the failed flow condition of the selected FPRs is not restricted enough, a flow-restriction orifice may need to be added downstream of each FPR.

EPS Reference #16—Describe sizing orifice restriction to allow low-pressure operation.

(SV3, SV4, SV5, & SV6)—Power-production mode

If any of the vent or drain valves downstream of the fuel stack fail open, there will be a large loss of reactants out of those vents. The use of flow-control orifices at all gas outlets will minimize the loss of reactants and allow longer run time than without the orifice. These orifices can be sized to limit flow to the sonic, choked flow condition when the pressure drop to the environment is high, such as at the higher altitudes.

EPS Reference #17—Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.

(LS3)—Power-production mode.

For this critical application, the system should continue to operate if the coolant level switch indicates low coolant. An alternate method of monitoring adequate coolant flow volume should be developed based on the inlet and outlet stack coolant temperature difference. The monitor should consider the fuel cell output and the temperature difference to estimate the thermal capacitance and resulting coolant flow.

EPS Reference #18—Examine heater vs. fan thermal control (or both) while on standby.

(HTX1)—Standby mode

Power for maintaining the operational temperature of the fuel cell coolant during standby originates from main aircraft power. During the power-production mode, the power for thermal control is independently provided by the fuel cell system. Several possible thermal control configurations during the standby mode should be considered during system design.

- Coolant pump power and on/off control of the coolant heater power provided by an aircraft control system using remote temperature sensors from the fuel cell.
- Coolant pump and heater power provided by the aircraft. On/off control of the coolant heater power performed by the fuel cell control system using power supplied from the aircraft.
- Coolant pump and heater power provided by the aircraft. On/off control of the coolant heat exchanger fan performed by the fuel cell control system using power supplied from the aircraft.
- A combination of 2 and 3. Heat is supplied by heater and removed by heat exchanger.

EPS Reference #19—Examine risk of continued operation during slow reactant leak.

(M1, M2, WT1, FC1-H2 &O2)—Power production and standby modes

The risk associated with a slow external hydrogen leak is both a safety and a shortened run-time risk. The risk associated with a slow oxygen leak is a reduced run-time risk. Monitoring storage pressure will provide an indication of the level of the leak. In the standby mode, a decline in storage pressure is a direct indication of leak. In the power-production mode, the rate of consumption needs to be included in the controls computation for potential reactant leakage.

EPS Reference #20—Include a short pressure release to verify vent valve function.

(SV5, SV6)—Preflight mode

During the preflight check, the system is pressurized to check that the system is leak free. This recommendation proposes a short pressure release be included in the preflight check to verify vent valve function. Before the final stack evacuation process, the isolation valves are closed and the vent valves are cycled to produce a small, uniform pressure release in both the anode and cathode sides of the fuel cell stack. After an acceptable pressure release, the FC can be fully evacuated before entering the standby mode.

EPS Reference #21—Include DP alarm PT5/PT6.

(FPR1, FPR2)—Standby mode

During the standby mode, the forward pressure regulators, FPR1 and FPR2, are expected to maintain the correct reactant inlet pressure to the fuel cell stack. This recommendation proposes that the differences of the downstream pressure of the two FPRs be monitored for consistency. A shift in this pressure difference may produce an alarm indicating a potential fault in one of the FPRs.

EPS Reference #22—Include PT redundancy check in controls.

(PT1, PT2, PT3, PT4, PT5, PT6)—Power-production mode

The need for redundant PTs on reactant storage tanks is addressed in recommendation reference #34. The four pressure transducers in the reactant lines downstream of the FPRs can also provide a certain degree of redundancy during the power-production mode. If functioning correctly, all four should read relatively close. A single out-of-range reading probably indicates a defective instrument. Dual readings for the same reactant, which are in agreement but out of range, probably indicates a shortage of reactant.

EPS Reference #23—Investigate method to detect an H₂ leak into coolant.

(FC1-H₂)—Power-production and preflight modes

The interface material between the reactant cavities and the coolant cavities within the TESI fuel cell stack is solid, nonporous graphite. Any possible leakage of hydrogen into the coolant would potentially come from the sealing surfaces between the manifolds of the stack. The present coolant system is not a tightly sealed configuration. A large leak would be detected as a loss of reactant test pressure during the preflight check but would not be detected during operation. Small leaks would not be detected as reactant pressure changes. A sealed coolant system could be considered as a means to detect a pressure change due to reactant leakage into the coolant.

EPS Reference #24—Investigate method to detect an O₂ leak into coolant.

(FC1-O₂)—Power-production mode

See reference #23. The larger oxygen molecule is less likely to leak into the coolant; however, a sealed coolant system should be considered.

EPS Reference #25—Investigate water trap freezing possibility.

(SV3, SV4, WT1, WT2)—Standby mode

Generally, a small amount of product water is left in the bottom of the sump of the water trap to prevent the loss of reactant when water is pushed out during the draining process. The possibility of this water freezing seems remote because the fuel cell system is heated during the standby mode. However, there may be occasions when the aircraft is grounded, without power, in a subfreezing environment. A method of eliminating all of the water in the trap sump during the preflight mode should be investigated and implemented.

EPS Reference #26—Keep product water removal control active during pump circulation.

(SV3, SV4)—Preflight mode

When operating the reactant pumps during the preflight check, excess water held up in the fuel cell stack could collect in the water trap. This recommendation proposes keeping the water-removal process active during this event to prevent any chance of overflow. Following this event, the recommendation in reference 25 would be implemented to eliminate all product water.

EPS Reference #27—Research coolant alternatives for operation in low ambient temps.

(FC1-H2, FC1-O2, FC1-C)—Power-production mode

When the aircraft is grounded, without power in a subfreezing environment, a water coolant could possibly freeze up. The TESI stack design with bordered MEAs can utilize an antifreeze mixture for the coolant. Other coolant alternatives should also be investigated.

EPS Reference #28—Consider small flow to indicate regulator function.

(FPR1, FPR2)—Standby mode

A failure mode can occur where the pressure regulator for either the hydrogen or the oxygen gas supply (FPR1 or FPR2) fails closed during standby mode. Because the gas lines between the pressure regulators and the solenoid valves at the fuel cell stack (SV1 or SV2) will already be pressurized from the preflight mode, and there is no active flow of gas in standby mode, a closed pressure regulator would be undetectable. One way to ensure that the pressure regulator is open and functioning properly during standby mode would be to open the solenoid valves periodically, pressurizing the system and allowing the gas to flow through the pressure regulator. The problem with this solution is that some gas will be consumed by the fuel cell in the process, wasting reactant supply and generating water that will need to be cleared when the EPS is needed for power.

EPS Reference #29—Develop a method or algorithm to test level switch.

(LS1, LS2, LS3)—Preflight mode

A failure mode can occur where the level switch fails set (showing that water/coolant is always present) or open (showing that water/coolant is not always present). This can cause a problem for both the water trap level switches and the coolant tank level switch. The coolant tank level switch, if failed set during standby, would not prompt the maintenance activity of refilling the coolant tank if the level is low. The water trap level switch has issues with failing set and failing open. Clearing all water from the water traps is a step in the preflight sequence. Proper level switch operation ensures that this process does complete as planned. A method of verifying level switch function during preflight must be established to ensure proper function of the water traps.

At this time, we have not determined an effective way of performing the preflight check on the water trap level switches. The process must be simple enough to be performed by the operators with little prior knowledge and user involvement but be effective at ensuring level switch success. Below are some options to consider:

- Manually fill the water trap with water. Check that the level switch is set. Trigger opening of the water trap solenoid. Check that the level switch opens when the water is completely drained. This requires system modifications to isolate the area and allow manual filling.
- Isolate the water trap section from the fuel cell, remove, and test separately. This requires system modifications to isolate.
- Eliminate the level sensor. In other words, look for alternate methods of signaling to the controller that the water trap contains water and needs to be cleared.

EPS Reference #30—Consider redundant inlet valves.

(SV1, SV2, FPR1, FPR2)—Standby mode

There are multiple failure modes along the reactant path between the storage tanks and the inlet valves that result in the inability of the fuel cell stack to receive the gasses needed to produce power. Detection for some of these failure modes depends on the presence of flow, making detection difficult if not impossible. Adding a parallel reactant path with duplicate components would provide a measure of redundancy to allow for successful power generation when transitioning out of standby and into power-production mode in the event that the fuel cell inlet solenoid (SV1 or SV2) or pressure regulator (FPR1 or FPR2) are stuck closed. This option may be superior to the other solution (reference #28) in that no reactant supply is wasted but at the expense of an increase in the number of components, which negatively impacts weight, cost, and system complexity. Tests can be run on dual gas supply lines with identical components to test the concept with simulated failures of components and normal operation configurations.

EPS Reference #31—Compute at what impurity level a purge is needed for the 1 hour mission (FC1-H₂, FC1-O₂)—Power-production mode.

Because of the short duration of the power-production mode for the EPS application, fuel cell performance loss from impurity build up may not be a significant factor. With the knowledge of the fuel cell stack gas volume and stack current, the performance loss can be calculated over the mission duration. If the impact is insignificant, this application may not require a reactant purge process to clear the inert gas that builds up in the flow channels. The system design would still need to include parts and controls to perform gas purges for maintenance purposes and in the event that stack performance is impacted by other degradation mechanisms. The control algorithm could be simplified if purges are not required.

EPS Reference #32—Consider a check valve to prevent backflow.

(SV3, SV5, SV6)—Standby mode

If SV3 or SV5 fail fully open, air can flow into the anode flow channels of the fuel cell stack if a check valve is not present. The air would then react with hydrogen entering the anode flow channels upon the next pressurization of the stack during operation or preflight, creating a dangerous mixture and damaging the catalyst in the fuel cell stack. Inserting a check valve upstream of the solenoid valves would eliminate this problem and require the failure of two parts to create the issue instead of one part. Inserting a check valve would not influence system operation as it currently stands.

EPS Reference #33—Consider air-flow sensor.

(HTX1)—Preflight mode

As the system design currently stands, there is no provision for checking the successful operation of the fan on the heat exchanger during preflight mode. The fan is needed during power-production mode to remove the heat generated by the fuel cell stack when it is providing power. Without the fan, the fuel cell stack would overheat and be irreparably damaged. Adding an air flow sensor to

the heat exchanger would be a simple solution to performing a preflight check on the fan. Any issues resulting in a lack of airflow or reduced air flow could be identified, diagnosed, and fixed on the ground.

EPS Reference #34—Consider redundant PTs on reactant storage tanks.

(PT1, PT2)—All modes

Diagnosing a faulty pressure transducer when the signal fails to full scale or to zero scale is rather simple. Signal drift by a pressure transducer is a more probable failure mode that is much more difficult to diagnose. The pressure transducers used for monitoring reactant storage pressure (PT1 and PT2) are critical for the EPS application because they are the primary method of calculating system run time, which the operator needs to know at all times. Any drift in these sensors would provide incorrect information to the operator, which could result in poor decision-making during an emergency flight situation. Installing a second pressure transducer on the reactant tank would provide an additional verification of reactant supply without much additional cost or complexity.

EPS Reference #35—Develop a backup thermal control scheme using T4.

(T3)—All modes

The control algorithm as it currently exists uses T3 to control the fuel cell temperature. T4 can be used as a backup in case T3 is not working at all or providing incorrect information because it also provides useful information about the stack temperature. The control algorithm should be updated to use T4 in the event that T3 is no longer sufficient.

EPS Reference #36—Develop an algorithm to compute the remaining run time because of a slow loss of reactant.

(RV3, RV4)—Power production and standby modes

If a leak at a relief valve (RV3, RV4) or any other location occurs, then the tank pressure will no longer be a direct indicator of EPS run time. An algorithm can be developed that takes into account a detected leak rate when computing EPS run time. In standby mode, detecting a slow and steady loss in pressure will signal a leak, and the effect on run time can be easily computed by subtracting the projected amount of hydrogen lost during operation from the existing hydrogen in the storage tank. In power-production mode, a constant pressure decay rate exists for the system based on the stack power level. If the pressure decay rate is higher than the known value, then a leak is suspected. An adjusted remaining run time can be calculated based on the tank pressure, known stack consumption rate, and calculated leak rate with an algorithm similar to that used during standby mode.

EPS Reference #37—Investigate the potential severity of a high-pressure O₂ leak.

(V2)—Power-production and standby modes

An external gas leak from the oxygen storage tank could produce a small jet of oxygen in the energy system compartment. It is unclear what the severity of this failure would be in that environment. High-purity oxygen can be highly reactive with certain materials. The level of severity would also be dependent on the system configuration inside the compartment. This threat should be evaluated in more detail once the system is more specifically defined.

EPS Reference #38—Periodic RV check is only means to detect failed closed condition.

(RV1, RV2, RV3, RV4)—Preflight mode

Storage and fuel cell system relief valves must be checked for functionality and accuracy as part of the periodic maintenance schedule. The failed closed occurrence is very rare and there is no effect as a single point failure. However as part of a multipoint failure, the effect could lead to total failure.

4.2 RECOMMENDATIONS—MPS

MPS Reference #1—Consider adding filter downstream of reactant pump.

(M1, M2)—Power-production mode

A failure mode can occur where the reactant pumps (M1 or M2) fail and produce contaminants that can then enter the FC stack. Adding a filter downstream of the reactant pumps will protect the FC stack from these contaminants. An additional filter should be considered at the exit of the FC reactant lines to protect the solenoid valves and reactant pumps from particles that could exit the FC stack, such as carbon fibers from the GDLs.

MPS Reference #2—Consider second PT to indicate adequate flow as indicated by pressure drop
(M1, M2)—Power production and startup mode.

A failure can occur where the reactant pump(s) stop operating and the fuel cell performance decays because of flooding. Adding pressure transducers at the FC reactant outlet lines allows the system to monitor differential pressure across the FC to ensure adequate velocity to remove product water. These additional pressure transducers also give redundancy for the existing ones. A second option is to measure reactant pump electrical current draw to indicate pump RPM, which relates to flow.

MPS Reference #3—Include a monitor for current draw on reactant recirculation pump.

(M1, M2)—Power-production and startup mode

See reference #2 above

MPS Reference #4—Include a thermal switch on V3 for redundancy.

(HT1)—Power-production and startup mode

Currently, there is not a temperature sensor in the coolant tank where the coolant heaters are located. The temperature sensor at the fuel cell coolant inlet controls the coolant heater. An over

temperature thermal switch will provide an additional safety factor to ensure the coolant tank never overheats.

MPS Reference #5—Need redundant pressure indicator for reactant; consider second PT at reactant FC outlet.

(PT3, PT4)—All Modes

Diagnosing a faulty pressure transducer when the signal fails to full scale or to zero scale is rather simple. Signal drift by a pressure transducer is a more probable failure mode that is much more difficult to diagnose. The pressure transducers used for monitoring reactant pressure (PT3 and PT4) are critical for the MPS application. Any drift in these sensors would provide incorrect information to the system control, which could result in inappropriate shutdown. Installing a 2nd pressure transducer on each FC outlet would provide an additional verification of reactant supply without much additional cost or complexity.

MPS Reference #6—Investigate detection methods for external H₂ leak.

(M1, WT1, FC1-H₂)—Power-production and startup mode

A failure can occur if a hydrogen leak develops that increases the environmental hydrogen concentration to a dangerous level and ignites. A hydrogen-detection method will provide valuable information. A continuous flow of atmospheric air would purge the space around the FC system and a hydrogen detector placed where the flow exits (ideally at the top of the space). Testing may be necessary to ensure a COTS hydrogen detector will work effectively at the temperatures the system will be exposed to.

MPS Reference #7—Compute total product water available for worst case flooding risk.

(WT1, WT2)—Power-production mode

The failure of the product water trap in either the hydrogen or oxygen recirculation circuits could allow the direct release of product water from the traps and cause flooding external into system enclosure. The worst-case level of flooding is determined by the amount of reactants available to produce water. The short mission of this application limits the amount of onboard reactants. The mass of onboard reactants total about 17 kg, which could produce 17 liters of water. This volume is slightly less than 3% of the total volume of the EPS PEMFC system enclosure. Although this volume is small, the location of components in the overall system design should be addressed to prevent flooding of sensitive components.

MPS Reference #8—Describe control to limit product water accumulation based on amp-hr count and its use as a secondary control/alarm.

(LS1, LS2)—Power-production and startup mode

The failure of the level switch on either the hydrogen or oxygen water trap could lead to the drain valve not being actuated and the water trap overflowing. This would lead to excess water in the reactant recirculation circuit and flood of the fuel cell stack. TESI uses a control algorithm to

compute product water production. Fuel cell amperage is directly proportional to the consumption rate of the hydrogen, oxygen reactants, and the production rate of product water. The controller stores accumulated fuel cell amperage over time and determines when to open the drain valve. The drain event is allotted a certain amount of time. If the level switch does not reset after this event, normally an alarm will trigger a shutdown due to a defective level switch. However, for this application, the control algorithm should continue to run to extend the run time for as long as possible.

MPS Reference #9—Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load.

(HT1)—Power-production and startup mode

The coolant heater for this application is the standard bootstrap heater used during system startup. The heater is powered by the FC providing a sizable electrical load for the system and adding that electrical load as supplemental heat directly to the coolant for quick startup. After reaching operating temperature, the heater is turned off. In the event of a heater failing to turn off, the liquid-to-air heat exchanger for the system must be sized to remove the process heat at expected max load plus the heat supplied by the failed coolant heater.

MPS Reference #10—Describe how to size RV3/RV4 for full high-pressure storage flow.

(FPR1, FPR2)—Power-production and startup modes

Relief valves RV3 and RV4 protect the FC system from potential high-pressure exposure because of the failure of either of the forward pressure regulators, FPR1 or FPR2. These relief valves must be sized large enough to prevent excessive pressure buildup at the inlets of the isolation solenoid valves SV1 or SV2. If fully opened when the failed flow condition of the selected FPRs is not restricted enough, a flow-restriction orifice may need to be added downstream of the each FPR.

MPS Reference #11—Consider sizing orifice restriction to allow low-pressure operation.

(SV3, SV4, SV5 & SV6)—Power-production mode

If any of the vent or drain valves downstream of the fuel stack fail open, there will be a large loss of reactants out of those vents. The use of flow-control orifices at all gas outlets will minimize the loss of reactants and allow longer run time than without the orifice. These orifices can be sized to limit flow to the sonic, choked flow condition when the pressure drop to the environment is sufficiently high, such as at higher altitudes.

MPS Reference #12—Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.

(LS3)—All modes

For this critical application, the system should continue to operate if a failed coolant level switch indicates low coolant. An alternate method of monitoring adequate coolant flow volume can be developed based on the inlet and outlet stack-coolant temperature difference. The monitor can

consider the fuel cell output and the temperature difference to estimate the thermal capacitance and resulting coolant flow.

MPS Reference #13—Examine risk of continued operation during slow reactant leak—look at H₂ concentration time response.

(RV1, RV2, M1, M2, WT1, FC1-H₂ &O₂)—Power-production and startup modes

The risk associated with a slow external hydrogen leak is both a safety and a shortened run-time risk. Monitoring storage pressure will provide an indication of the level of the leak. The hydrogen leak detector provides an ambient H₂ concentration reading shutting down the FC system and venting the H₂ storage at the 50% low-explosion level (LEL) set point. The time to reach a 25% LEL warning and the 50% LEL shutdown depends on the size of the leak, volume of the cabin, and the cabin ventilation rate, which is based on the FAA ventilation-per-occupant requirement. The aircraft used in this medevac application allowed a warning (25% LEL) time of 8 minutes and then equilibrated and remained at the shutdown level (50% LEL) after 50 minutes with a hydrogen leak of 57 standard liters per minute.

MPS Reference #14—Investigate method to detect an H₂ leak into coolant.

(FC1-H₂)—Power-production and startup modes

The interface material between the reactant cavities and the coolant cavities within the TESI fuel cell stack is solid, nonporous graphite. Any possible leakage of hydrogen into the coolant would potentially come from the sealing surfaces between the manifolds of the stack. The present coolant system is not a tightly sealed configuration. A large leak would be detected as a loss of reactant test pressure during the maintenance check but would not be detected during operation. Small leaks would not be detected as reactant pressure changes. A sealed coolant system could be considered as a means to detect a pressure change due to reactant leakage into the coolant.

MPS Reference #15—Investigate method to detect an O₂ leak into coolant.

(FC1-O₂)—Power-production and startup modes

See reference #14. The larger oxygen molecule is less likely to leak into the coolant; however, a sealed coolant system could be considered.

MPS Reference #16—Compute purge frequency and quantity versus reactant impurity level.

(FC1-H₂, FC1-O₂)—Power-production mode

Because of the relatively short duration of the power-production mode for the MPS application, fuel cell performance loss from impurity buildup may not be a significant factor. With the knowledge of the fuel cell stack gas volume and stack current, the performance loss can be calculated over the mission duration. If the impact is insignificant, this application may not require a reactant purge process to clear the inert gas that builds up in the flow channels. The system design would still need to include parts and controls to perform gas purges for maintenance purposes and

in the event that stack performance is impacted by other degradation mechanisms. The control algorithm could be simplified if purges are not required.

MPS Reference #17—Develop a backup thermal control scheme using T2.

(T1)—Power-production and startup modes

The control algorithm as it currently exists uses T1 to control the fuel cell temperature. T2 can be used as a backup in case T1 is not working at all or providing incorrect information because it also provides useful information about the stack temperature. The control algorithm should be updated to use T2 in the event that T1 is no longer effective.

MPS Reference #18—Periodic RV check is only means to detect failed closed condition.

(RV1, RV2, RV3, RV4)—All modes

Storage and fuel cell system relief valves must be checked for functionality and accuracy as part of the periodic maintenance schedule. The failed closed occurrence is very rare, and there is no effect as a single point failure. However, as part of a multipoint failure, the effect could lead to total failure.

MPS Reference #19—Appropriate procedures for handling high-pressure reactant tanks must be in place.

(V1, V2)—All modes

The reactant tanks are high-pressure tanks, 5000 psig H₂ and 3000 psig O₂, fitted with high-pressure fittings and instrumentation. Filled reactant tanks, both hydrogen and oxygen, will be installed separately from the system installation for the initial reactant charge and then removed and replaced with filled tanks when the system is recharged. Handling and connecting these tanks separate from the system requires that the appropriate procedures and practices be in place to prevent equipment damage or personnel injury.

MPS Reference #20—Check accuracy of PGs at 200-hr maintenance interval.

(PT1, PT2, PG1, PG2)—All modes

The pressure transducers used for monitoring reactant storage pressure (PT1 and PT2) are the primary method of calculating system run time, which the operator needs to know at all times. Diagnosing a faulty pressure transducer when the signal fails to full scale or to zero scale is rather simple. Signal drift by a pressure transducer is a more probable failure mode that is much more difficult to diagnose. Each reactant tank has a pressure gauge installed as a redundant pressure indicator. The accuracy of these gauges should be checked at the regular maintenance interval to insure a true reference.

MPS Reference #21—Consider a control override to allow a cold start without heater load.

(HT1)—Startup mode

The system is designed to provide a quick heat-up start using the bootstrap heater as a load before applying the external load. Failure of the bootstrap heater should not prevent system startup. The system controls should allow an override to permit an external load to be manually applied for a cold startup. The override would include provisions to limit load current until the FC stack has reached operating temperature.

MPS Reference #22—Consider a timeout for not completing shutdown.

(All SVs, MV1, MV3, PT3, PT4)—Shutdown mode

The shutdown mode removes all reactants. This involves a process for consuming reactants to create a vacuum in the stack. During the process, the reactant valves sequence on and off, and the pressure transducers remain active to maintain the correct stoichiometric ratio while the reactants are being consumed. The pressure in the stack decreases while staying within the allowable anode to cathode pressure difference. Failure of one of the active components to provide the correct control during the process could result in the process being held up in part of the sequence indefinitely. A timeout alarm should be considered if the shutdown process has exceeded a specified time limit, indicating a potential component failure.

MPS Reference #23—Consider burp test for vent SVs at startup after pressure test.

(SV5, SV6)—Startup mode

Vent valves SV5 and SV6 are used during the power-production mode to purge the inert gases that have built up and during shutdown to depressurize the system to begin the vacuum process. This recommendation suggests a simple test of these valves during the startup mode to check that they are functional. Following the static leakdown test, each valve can be quickly opened and closed. The corresponding reactant pressure is monitored for an acceptable pressure decay indicating a functional solenoid valve.

MPS Reference #24—Consider manual override to check fan operation.

(HTX1)—Startup mode

The liquid-to-air heat exchanger uses an axial fan to move air across tubes for rejecting processed heat to the ambient air. Without the fan, the output of the FC system would be limited. A simple functional check of the fan is suggested by using a manual override to activate the fan with the operator physically observing the air flow.

MPS Reference #25—Consider redundant H₂ leak detector.

(A1)—All modes

The hydrogen leak detector is interlocked with the FC system, preventing FC operation in the absence of an H₂ concentration reading from the detector. The detection system is subject to drift in the accuracy of the H₂ concentration. The calibration must be checked and verified at regular intervals. If the accuracy drifts high, reading higher than the actual concentration, the safety risk to the aircraft is not affected, and only the operational risk will be impacted. The safety risk is a

concern if the accuracy drifts lower, and the actual H₂ concentration is higher than detected. The design should consider an additional hydrogen leak-detection device to address this issue.

MPS Reference #26—Describe control to limit reactant loss based on amp hr count and as a secondary control/alarm.

(LS1, LS2)—Power-production mode

The failure of the level switch to reset on either the hydrogen or oxygen water trap could lead to the drain valve remaining open. This would lead to continuous loss of reactant. TESI uses a control algorithm described in Reference #8 to compute product water production. A similar timing algorithm can be used as a secondary control to prevent the complete loss of reactant.

MPS Reference #27—Develop a response to a detectable H₂ tank gas leak; consider an emergency storage tank dump.

(V1)—All modes

A rapid increase in the measured H₂ concentration is an indication of a major leak in the H₂ tank or supply. This may be greater than the allowable leak that the aircraft ventilation can safely handle. The H₂ supply should consider a separate valve that can be operated to allow an emergency dump to avoid reaching a hazardous concentration level in the aircraft.

MPS Reference #28—Develop a response to a detectable O₂ tank gas leak; consider an emergency storage tank dump.

(V2)—All modes

An external gas leak from the oxygen storage tank could produce a small jet of oxygen into the cabin. It is unclear what the severity of this failure would be. High-purity oxygen can be highly reactive with certain materials. The level of severity would also be dependent on the system configuration inside the compartment. This threat should be evaluated in more detail once the system is more specifically defined.

MPS Reference #29—Discuss combining separation and water-storage functions to simplify product water management.

(V4)—Startup and power-production modes

The water produced by the reaction of the H₂ and O₂ is to be collected and held onboard the aircraft. The system has active level switches and drain valves. This recommendation proposes considering a design that would eliminate the level switches and valves and allow the product water to drain directly into separate pressurized tanks. The majority of product water is contained on the cathode side of the system. The cathode tank would be sized for the total product water quantity, and the anode tank would be sized much smaller.

MPS Reference #30—Discuss H₂ vent location—aft of engine intake.

(RV1, FPR1)—All modes

A high-pressure hydrogen release from either of the two H₂ relief valves could result in the release of large volumes of hydrogen. The hydrogen must be vented to the exterior. There is concern about releasing this large volume into an engine intake. To avoid this, the H₂ vent lines from the system relief valves are to be routed behind the aircraft engines.

MPS Reference #31—Discuss high-pressure O₂ release through luggage compartment hatch.

(RV1, FPR1)—All modes

A high-pressure oxygen release from either of the two H₂ relief valves could result in the release of large volumes of oxygen. Large volumes of oxygen must be vented to the exterior. To minimize vent line penetrations through the aircraft fuselage, the high-pressure vent lines from the O₂ relief valves are to be routed through the luggage compartment hatch.

MPS Reference #32—Discuss methods to detect/contain overflow.

(V4)—Startup and power-production modes

In this application, the water produced by the PEMFC is captured in the product water tank. The mass of onboard reactants totals approximately 17 kg, which could produce 17 liters of water. In the event of a leaking product water tank, it is recommended that a method of containing a leak be implemented or a method of detecting a leak be used to provide an alarm for operator action. A secondary overflow pan or basin could be used and could include a water leak sensor.

MPS Reference #33—Discuss the requirement for a stack pressurization timeout.

(RV3, RV4, SV1, SV2, MV1, MV2, FPR1, FPR2)—Startup mode

The startup mode provides a controlled process to pressurize the FC stack. During the process, the reactant valves sequence on and off and the pressure transducers remain active to maintain the allowable anode to cathode pressure difference while the reactants are pressurizing the stack. Failure of one of the active components to provide the correct control during the process could result in the process being held up in part of the sequence indefinitely. A timeout alarm should be considered if the startup process has exceeded a specified time limit indicating a potential component failure.

MPS Reference #34—Explain FS1 as an alarm indicator, not a shutdown control.

(FS1)—Startup mode

The loss of coolant flow will result in the FC overheating and shutting down at a high temperature. Flow switch FS1 is an alarm indicator for this condition but is not used as a shutdown control. Monitoring the FC stack temperature provides an indication of sufficient coolant flow for near-term operation.

MPS Reference #35—Explain that the vacuum condition should be maintained until startup.

(WT1, WT2, FC1-H2, FC1-O2)—Startup mode

When the PEMFC system is shutdown, the inlet and vent valves go to normally closed positions. System pressure is released through the water trap drain valves to drain the trap sumps. A small resistive load is applied to the FC stack to cause consumption of the remaining reactants trapped in the stack. The inlet valves are cycled open and closed to maintain the minimum allowable delta pressure within the stack until a vacuum state is reached. Once the shutdown process is complete, manual valves MV1, MV2, MV3, and MV4 are closed.

The PEMFC should remain in the vacuum state until it is restarted. If there is no longer a vacuum on either gas circuit, the system should be pressure checked for leaks. Atmospheric air that has bled back into the FC stack indicates a potential leak. This is especially a concern on the anode, the hydrogen side of the stack.

MPS Reference #36—H₂ leak detector calibration must be constantly checked.

(A1)—All modes

See Reference #25 above.

MPS Reference #37—Include a visual level indicator.

(LS3, V4)—Startup and shutdown modes

It is recommended that a simple, visual level indicator be included on both the coolant tank and the product water tank. At startup, the coolant tank should be checked for a fully filled condition and the product water tank for empty. When the system is shutdown, the visual indicator will confirm that the product water tank has been emptied.

MPS Reference #38—Recommend cell voltage check at full load.

(RV3, RV4, SV1, SV2, MV1, MV2, MV3, MV4)—Startup mode

The startup procedure includes a check of individual cell voltages at an open circuit, no load condition. This verifies that all the cells are receiving reactant and are responding. It is recommended that a check of individual cell voltages also be checked at full load to verify expected cell performance. Acceptable cell performance will maintain minimum allowable cell voltage differences between adjacent cells. An unacceptable individual cell voltage is cause for further evaluation.

5. TESTING

5.1 PURPOSE

The FMEA analysis relies on making certain assumptions for modes of operation outside what is normally experienced. The analysis requires the use of engineering judgement based on basic engineering or scientific principles. Acceptance testing of fuel cell system products is typically done under very controlled conditions. Warning alarms and shutdowns prevent operational

parameters to stray outside, beyond allowable ranges. The purpose of the FMEA-related testing is to validate some of the assumptions that lead to high RPNs and potential failure modes. This, however, requires test procedures that push the operational parameters beyond the acceptable range.

A list of prospective tests is shown in table 10. These tests were selected to support some of the assumptions used in the studies and some of the results from each of the two FMEAs. Each test listing shows the failed component P&ID reference number in the last column.

Table 10. Proposed Tests

Study	Test No.	Description	Component
EPS	1	Reactant Recirculation	M1, M2
EPS	2	Pressure Difference, Supply	SV1, SV2, RV3, RV4
EPS	3	High-Temperature Operation	HX1, M3, V3
EPS	4	Excess Product Water	LS1, LS2, SV3, SV4
EPS	5	Frozen Startup	HT1
EPS	6	Pressure Difference, Downstream	SV3, SV4, SV5, SV6
EPS	7	Reactant Impurity	FC1-H2, FC1-O2
EPS	8	Backup Thermal Control	T3
EPS	9	Fuel Cell Stack Evacuation	FC1
MPS	1	Reactant Recirculation	M1, M2
MPS	2	High-Temperature Operation	HX1, M3, V3
MPS	3	Excess Product Water	LS1, LS2, SV3, SV4
MPS	4	Pressure Difference, Downstream	SV3, SV4, SV5, SV6
MPS	5	Coolant Flow	FS1
MPS	6	Reactant Impurity	FC1-H2, FC1-O2
MPS	7	Backup Thermal Control	T1
MPS	8	Cold Startup	HT1

5.2 TESTING

The test procedures were designed to simulate the out-of-range condition for the subject failure mode. The tests focused on the effect of the failure on fuel cell stack operation. The test procedures directed the operation of the fuel cell stacks under conditions that would be imposed by a specific system component failure.

Testing was completed for 14 of the 17 tests proposed in table 10. Twelve of these tests used four cell short stacks running on an in-house TESI Medusa fuel cell test station for system simulation. These are open, flow-through test systems. The test procedures were designed to simulate the closed-system operation of the aircraft systems. The three tests not run were the Coolant Flow MPS Test #5 and the Backup Thermal Control Tests EPS #8 and MPS #7. These three tests require standalone control systems with extensive reprogramming capability, which was not available at

the time. The Fuel Cell Stack Evacuation EPS Test #9 and the Cold Startup MPS Test #8 were performed on a 64-cell stack to test the effect on a full-size stack. To minimize irreversible damage to the fuel cell test articles, the tests were prioritized in order of expected severity.

The membrane electrode assemblies (MEA) in all 14 of the original tests used carbon-supported platinum catalyst on the anode. This is a less-expensive option than an anode with a pure platinum black catalyst. Poor performance with this catalyst, when running with inert contaminated reactant in the anode, terminated the completion of several runs of the EPS Test #7 and MPS Test #6 Reactant Impurity Tests. These tests were later rerun with a 2-cell stack using a platinum black anode catalyst.

5.3 TEST PROCEDURES AND RESULTS

Several of the tests proposed in table 10 are similar for the two applications. This reduces the actual number of test procedures performed, although the results have different consequences depending on the application. Each test procedure is presented in appendix I, followed by charted results and the significance for each application.

To have enough data for the results to be meaningful, the test procedure may have required multiple runs of the test at different conditions. The testing sequence for multiple runs started with a less-severe condition and progressed in severity to determine an effect or a threshold.

Tests of the stack were run at baseline conditions after each test. Baseline polarization data were used to determine any performance degradation.

5.4 OVERALL CONCLUSIONS

Despite the deliberate abuse that the initial 4-cell stack endured over the 4-month period of testing, the unit did not fail or even lose any of its initial performance. All of the post-test, baseline polarization tests run during this period showed a consistently close data grouping. The baseline polarization data curves are shown in figure 7. The lower curves represent the first tests on the newly assembled stack. As expected, the performance improved during the first several tests as the cells were broken in and fully activated. Throughout the testing, the polarization curves tightly indicated very little change in performance. As the tests grew increasingly more severe with freezing temperature extremes and high-temperature operation, performance was not degraded.

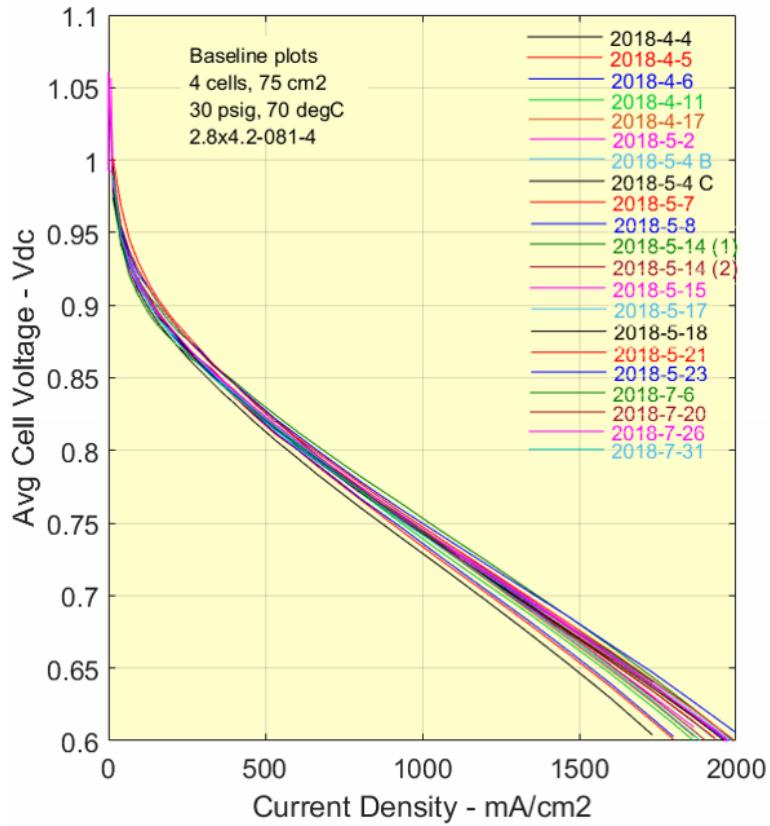
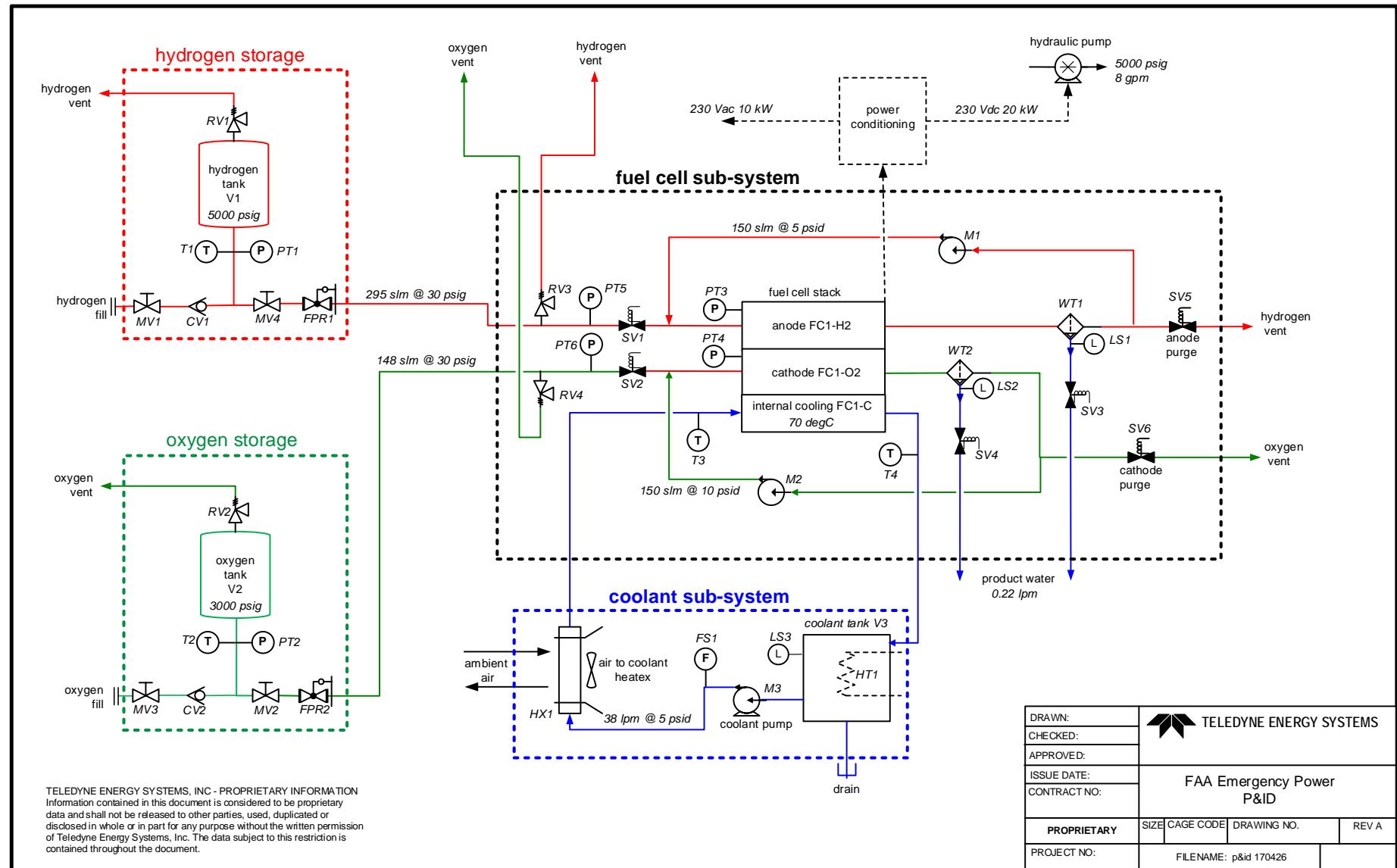


Figure 7. Baseline Polarization Curves

The results validate the assumptions used in the FMEA analysis. They indicate that the fuel cell stack can operate well beyond the alarm limits presently imposed by the supporting system. It should be noted that these tests represent the duration of operation of the fuel cell stack based on the aircraft applications selected for this study. Longer operation at off-limit conditions would very likely produce different results.

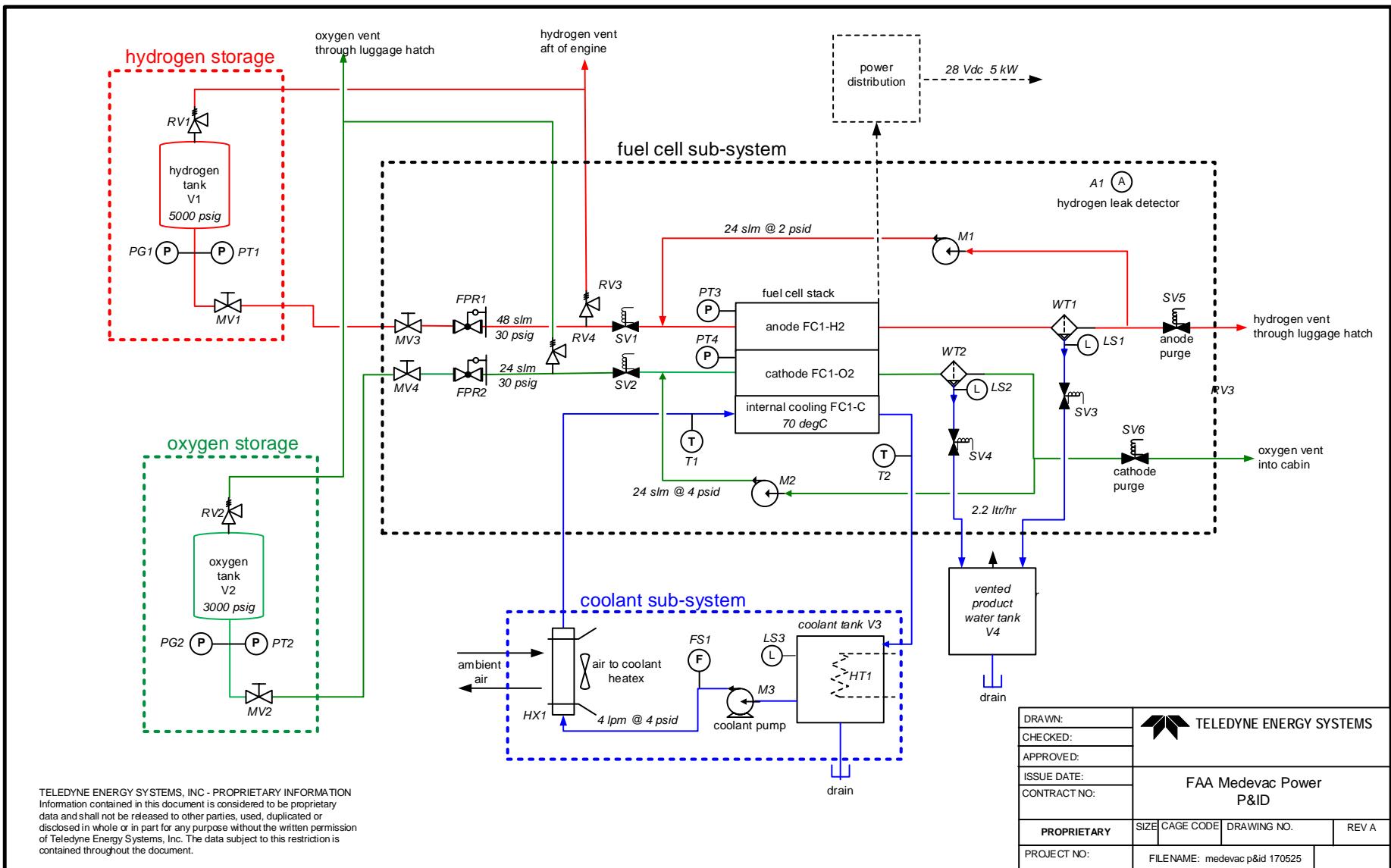
APPENDIX A—EPS P&ID



TELEDYNE ENERGY SYSTEMS, INC - PROPRIETARY INFORMATION
 Information contained in this document is considered to be proprietary data and shall not be released to other parties, used, duplicated or disclosed in whole or in part for any purpose without the written permission of Teledyne Energy Systems, Inc. The data subject to this restriction is contained throughout the document.

APPENDIX B—MPS P&ID

B 1



TELEDYNE ENERGY SYSTEMS, INC - PROPRIETARY INFORMATION
Information contained in this document is considered to be proprietary data and shall not be released to other parties, used, duplicated or disclosed in whole or in part for any purpose without the written permission of Teledyne Energy Systems, Inc. The data subject to this restriction is contained throughout the document.

APPENDIX C—EPS PRE-FLIGHT WORKSHEETS

C-1

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		2. fail partially open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		3. fail closed	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	10. periodic RV check is only means to detect failed closed condition
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT2	1	4	
		2. fail partially open	1. loss of reactant	4	1. internal failure	1	1. alarm PT2	1	4	
		3. fail closed	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	10. periodic RV check is only means to detect failed closed condition
3. H2 delivery relief valve RV3	RV3	1. fail closed	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	10. periodic RV check is only means to detect failed closed condition
		2. fail fully open	1. loss of reactant	3	1. internal failure	1	1. alarm PT5 or PT3	1	4	
			2. loss of pressure	4			2. alarm dP PT3/PT4			
			3. high dP on stack	3						
		3. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT5 or PT3	1	3	
			2. loss of pressure	2			2. alarm dP PT3/PT4			
			3. high dP on stack	1						
4. O2 delivery relief valve RV4	RV4	1. fail closed	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	10. periodic RV check is only means to detect failed closed condition
		2. fail fully open	1. loss of reactant	3	1. internal failure	1	1. alarm PT6 or PT4	1	4	
			2. loss of pressure	4			2. alarm dP PT3/PT4			
			3. high dP on stack	3						
		3. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT6 or PT4	1	3	
			2. loss of pressure	2			2. alarm dP PT3/PT4			
			3. high dP on stack	1						
5. H2 delivery inlet solenoid valve, NC SV1	SV1	1. fail closed	1. not able to pressurize stack FC1	4	1. internal failure	1	1. alarm PT3	1	4	
		2. fail fully open	1. high dP on stack	4	1. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	
		3. fail partially open	1. high dP on stack	4	1. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	
6. O2 delivery inlet solenoid valve, NC SV2	SV2	1. fail closed	1. not able to pressurize stack FC1	4	1. internal failure	1	1. alarm PT4	1	4	
		2. fail fully open	1. high dP on stack	4	1. internal failure	1	1. alarm PT4 2. alarm dP PT3/PT4	1	4	
		3. fail partially open	1. high dP on stack	4	1. internal failure	1	1. alarm PT4 2. alarm dP PT3/PT4	1	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
7. H ₂ water trap drain solenoid valve, NC SV3	SV3	1. fail fully open—open drain	1. loss of reactant	3	1. internal failure	1	1. alarm PT3	1	4	6. Keep product water removal control active during pump circulation	
			2. fail leak check	4							
			3. backflow of air	3							
			4. high dP	4							
		2. fail partially open	1. loss of reactant	2	1. internal failure	1	1. alarm PT3	1	4		
			2. fail leak check	4							
			3. backflow of air	3							
			4. high dP	4							
		3. fail closed—closed drain	1. flood stack during pump operation	3	1. internal failure	1	1. none	4	12		
8. O ₂ water trap drain solenoid valve, NC SV4	SV4	1. fail fully open—open drain	1. loss of reactant	3	1. internal failure	1	1. alarm PT4	1	4	6. Keep product water removal control active during pump circulation	
			2. fail leak check	4							
			3. backflow of air	1							
			4. high dP	4							
		2. fail partially open	1. loss of reactant	2	1. internal failure	1	1. alarm PT4	1	4		
			2. backflow of air	1							
			3. fail leak check	4							
			4. high dP	4							
		3. fail closed—closed drain	1. flood stack during pump operation	3	1. internal failure	1	1. none	4	12		
9. H ₂ vent solenoid valve, NC SV5	SV5	1. fail fully open—open vent	1. loss of reactant	3	1. internal failure	1	1. alarm PT3	1	4	7. Include a short pressure release to verify vent valve function	
			2. backflow of air	3							
			3. fail leak check	4							
			4. high dP	4							
		2. fail partially open	1. loss of reactant	2	1. internal failure	1	1. alarm PT3	1	4		
			2. backflow of air	3							
			3. fail leak check	4							
			4. high dP	4							
		3. fail closed—closed vent	1. voltage decay	2	1. internal failure	1	1. none	4	8		
10. O ₂ vent solenoid valve, NC SV6	SV6	1. fail fully open—open vent	1. loss of reactant	3	1. internal failure	1	1. alarm PT4	1	4	7. Include a short pressure release to verify vent valve function	
			2. backflow of air	1							
			3. fail leak check	4							
			4. high dP	4							
		2. fail partially open	1. loss of reactant	2	1. internal failure	1	1. alarm PT4	1	4		
			2. backflow of air	1							
			3. fail leak check	4							

C-2

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
			4. high dP	4						
		3. fail closed—closed vent	1. voltage decay	2	1. internal failure	1	1. none	4	8	7. Include a short pressure release to verify vent valve function
11. H2 storage manual isolation valve, MV4	MV4	1. fail close	1. not able to pressurize stack FC1	4	1. internal failure	1	1. no response PT1	1	4	
		2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
12. H2 storage manual fill valve MV1	MV1	1. fail close	1. not able to fill storage	4	1. internal failure	1	1. no response PT1	1	4	
		2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none for pre-flight	1	2. blockage partial	1	1. none	4	4	
13. O2 storage manual isolation valve MV2	MV2	1. fail close	1. not able to pressurize stack FC1	4	1. internal failure	1	1. no response PT2	1	4	
		2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
14. O2 storage manual fill valve MV3	MV3	1. fail close	1. not able to fill storage	4	1. internal failure	1	1. no response PT2	1	4	
		2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none for pre-flight	1	2. blockage partial	1	1. none	4	4	
15. H2 delivery pressure regulator FPR1	FPR1	1. fail closed, no outlet press	1. not able to pressurize stack FC1	4	1. internal failure	1	1. no response PT5	1	4	
		2. fail partial closed, low outlet press	1. not able to fully pressurize FC1	4	1. internal failure	1	1. alarm PT5	1	4	
		3. fail open, high outlet press	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
16. O2 delivery pressure regulator FPR2	FPR2	1. fail closed, no outlet press	1. not able to pressurize stack FC1	4	1. internal failure	1	1. alarm PT6	1	4	
		2. fail partial closed, low outlet press	1. not able to fully pressurize FC1	4	1. internal failure	1	1. no response PT6	1	4	
		3. fail open, high outlet press	1. loss of reactant	4	1. internal failure	1	1. alarm PT6	1	4	
17. H2 storage pressure transmitter PT1	PT1	1. fail high—high electrical output	1. unknown reactant pressure	4	1. internal failure	1	1. out of range PT1	1	4	
		2. fail low—low electrical output	1. unknown reactant pressure	4	2. electrical control failure	1	1. out of range PT1	1	4	
					1. internal failure	1	1. out of range PT1	1	4	
					2. electrical control failure	1	1. out of range PT1	1	4	

C-3

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		3. drift high or low	1. unknown reactant pressure	4	1. internal failure 2. electrical control failure	1 1	1. none 1. none	4 4	16 16	5. Consider redundant PTs on reactant storage tanks 5. Consider redundant PTs on reactant storage tanks
18. O2 storage pressure transmitter PT2	PT2	1. fail high—high electrical output 2. fail low—low electrical output 3. drift high or low	1. unknown reactant pressure	4	1. internal failure 2. electrical control failure 1. internal failure 2. electrical control failure 1. internal failure 2. electrical control failure	1 1 1 1 1	1. out of range PT1 1. out of range PT1 1. out of range PT1 1. out of range PT1 1. none	1 1 1 1 4	4 4 4 4 16	
19. H2 stack pressure transmitter PT3	PT3	1. fail high—high electrical output 2. fail low—low electrical output 3. drift high or low	1. false alarm high pressure	4	1. electrical control failure 2. internal failure	1 1	1. out of range PT3 1. out of range PT3	1 1	4 4	
			1. false alarm low pressure	4	1. electrical control failure 2. internal failure	1 1	1. out of range PT3 1. out of range PT3	1 1	4 4	
			1. high dP on stack	3	1. electrical control failure 2. internal failure	1 1	1. alarm PT5 1. alarm PT5	1 1	3 3	
20. O2 stack pressure transmitter PT4	PT4	1. fail high—high electrical output 2. fail low—low electrical output 3. drift high or low	1. false alarm high pressure	4	1. electrical control failure 2. internal failure	1 1	1. out of range PT4 1. out of range PT4	1 1	4 4	
			1. false alarm low pressure	4	1. electrical control failure 2. internal failure	1 1	1. out of range PT4 1. out of range PT4	1 1	4 4	
			1. high dP on stack	3	1. electrical control failure 2. internal failure	1 1	1. alarm PT6 1. alarm PT6	1 1	3 3	
21. H2 delivery pressure transmitter PT5	PT5	1. fail high—high electrical output 2. fail low—low electrical output 3. drift high or low	1. false alarm high pressure	4	1. internal failure 2. electrical control failure	1 1	1. out of range PT5 1. out of range PT5	1 1	4 4	
			1. false alarm low pressure	4	1. internal failure 2. electrical control failure	1 1	1. out of range PT5 1. out of range PT5	1 1	4 4	
			1. false alarm pressure set point	4	1. internal failure 2. electrical control failure	1 1	1. reference PT5 to FPR1 set point 1. reference PT5 to FPR1 set point	1 1	4 4	
22. O2 delivery pressure transmitter PT6	PT6	1. fail high—high electrical output	1. false alarm high pressure	4	1. internal failure 2. electrical control failure	1 1	1. out of range PT6 1. out of range PT6	1 1	4 4	

C-4

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Severity	Potential Cause/Mechanism of Failure	Occurrence	Current Design Controls (Detection)	Detected	RPN	Recommendations
C-5		2. fail low—low electrical output	1. false alarm high pressure	4	1. internal failure	1	1. out of range PT6	1	4	
					2. electrical control failure	1	1. out of range PT6	1	4	
		3. drift high or low	1. false alarm high pressure	4	1. internal failure	1	1. reference PT6 to FPR2 set point	1	4	
					2. electrical control failure	1	1. reference PT6 to FPR2 set point	1	4	
	23. H2 storage temperature transmitter T1	1. fail high—high electrical output	1. false alarm high temperature	4	1. internal failure	1	1. temperature out of instrument range	1	4	
					2. electrical control failure	1	1. temperature out of instrument range	1	4	
		2. fail low—low electrical output	1. false alarm low temperature	4	1. internal failure	1	1. temperature out of instrument range	1	4	
					2. electrical control failure	1	1. temperature out of instrument range	1	4	
	24. O2 storage temperature transmitter T2	3. drift high or low	1. inaccurate storage temperature	3	1. internal failure	1	1. reference to ambient temperature	1	3	
					1. internal failure	1	1. temperature out of instrument range	1	4	
		1. fail high—high electrical output	1. false alarm high pressure	4	2. electrical control failure	1	1. temperature out of instrument range	1	4	
					1. internal failure	1	1. temperature out of instrument range	1	4	
		2. fail low—low electrical output	1. false alarm low pressure	4	2. electrical control failure	1	1. temperature out of instrument range	1	4	
					1. internal failure	1	1. temperature out of instrument range	1	4	
	25. Coolant inlet temperature transmitter T3	3. drift high or low	1. inaccurate storage temperature	3	1. internal failure	1	1. reference to ambient temperature	1	3	
					1. internal failure	1	1. check T4 for redundant alarm	1	1	8. Develop a backup thermal control scheme using T4.
		1. fail high—high electrical output	1. false alarm high temperature	1	2. electrical control failure	1	2. check FS1 for flow	1	1	
					1. internal failure	1	1. check T4 for redundant alarm	1	1	
		2. fail low—low electrical output	1. high-temperature stack FC1	3	2. electrical control failure	1	2. check FS1 for flow	1	3	8. Develop a backup thermal control scheme using T4.
					1. internal failure	1	1. check T4 for acceptable temp	1	3	
		3. drift high or low	1. false alarm high temperature	1	2. electrical control failure	1	2. check FS1 for flow	1	3	
					1. internal failure	1	1. T4 redundant	1	1	8. Develop a backup thermal control scheme using T4.
	T4		1. false delta T alarm	1	1. internal failure	1	2. check FS1	1	1	
			1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
26. Coolant outlet temperature transmitter T4		1. fail high—high electrical output		1	2. electrical control failure	1	1. check FS1 for flow	1	1	
		2. fail low—low electrical output	1. false delta T alarm		1. internal failure	1	1. check FS1 for flow	1	1	
		3. drift high or low	1. false delta T alarm		2. electrical control failure	1	1. check FS1 for flow	1	1	
27. H2 water trap level switch LS1	LS1	1. fail set—electrically set filled	1. none for pre-flight	4	1. internal failure	1	1. none	4	16	4. Develop a method or algorithm to test level switch
			2. loss of reactant during operation	4						
		2. fail open—electrically open empty	1. none for pre-flight	4	1. internal failure	1	1. none	4	16	4. Develop a method or algorithm to test level switch
			2. flood stack during operation	4						
28. O2 water trap level switch LS2	LS2	1. fail set—electrically set filled	1. none for pre-flight	4	1. internal failure	1	1. none	4	16	4. Develop a method or algorithm to test level switch
			2. flood stack during operation	4						
		2. fail open—electrically open empty	1. none for pre-flight	4	1. internal failure	1	1. none	4	16	4. Develop a method or algorithm to test level switch
			2. flood stack during operation	4						
29. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none for pre-flight	1	1. internal failure	1	1. none	4	16	4. Develop a method or algorithm to test level switch
			2. false fill during standby	4						
30. Coolant flow switch FS1	FS1	1. failed closed—indicates flow	1. false flow indication	4	1. internal failure	1	1. monitor initial zero flow	1	4	
					2. electrical control failure	1	1. monitor initial zero flow	1	4	
		2. failed open—indicates no flow	1. false alarm no flow	4	1. internal failure	1	1. monitor for low stack temperature	1	4	
					2. electrical control failure	1	1. monitor for low stack temperature	1	4	
31. H2 recirculation pump M1	M1	1. stop pumping—no recirculation	1. flood stack	4	1. electrical control failure	1	1. motor current draw	1	4	
					2. internal failure	1	1. motor current draw	1	4	
		2. external gas leak	1. loss of reactant	4	1. mechanical failure	1	1. alarm PT3	1	4	
			2. external H2 reaction	4						
		3. internal leak—reduced flow	1. flood stack	4	1. internal failure	1	1. motor current draw	3	12	3. Consider second PT to indicate adequate flow as indicated by pressure drop
		4. mechanical degradation	1. stack contamination	4	1. internal failure	1	1. motor current draw	3	12	3. Consider second PT to indicate adequate flow as indicated by pressure drop
32. O2 recirculation pump M2	M2	1. stop pumping—no recirculation	1. flood stack	4	1. electrical control failure	1	1. motor current draw	1	4	
					2. internal failure	1	1. motor current draw	1	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		2. external gas leak	1. loss of reactant	4	1. mechanical failure	1	1. alarm PT4	1	4	
		3. internal leak—reduced flow	1. flood stack	4	1. internal failure	1	1. motor current draw	3	12	3. Consider second PT to indicate adequate flow as indicated by pressure drop
		4. mechanical degradation	1. stack contamination	4	1. internal failure	1	1. motor current draw	3	12	3. Consider second PT to indicate adequate flow as indicated by pressure drop
33. Coolant circulation pump M3	M3	1. pumping stops	1. low-temperature stack FC1	4	1. internal failure	1	1. alarm low-temperature TC3	1	4	
		2. pumping reduced	1. over heat coolant tank	4	1. internal failure	1	2. alarm low flow FS1	1	4	
			2. low-temperature stack FC1	4			1. alarm low-temperature TC3			
		3. external coolant leak	1. low-temperature stack FC1	4	1. mechanical failure	1	2. alarm low flow FS1	1	4	
34. H2 water trap WT1	WT1	1. external gas leak	1. backflow of air	2	1. mechanical failure	1	1. alarm dP PT3/PT4	1	2	11. Investigate water trap freezing possibility
			2. high dP	2			1. alarm dP PT3/PT4			
			3. dehydration of membrane	2			1. alarm dP PT3/PT4			
35. O2 water trap WT2	WT2	1. external gas leak	1. backflow of air	2	1. mechanical failure	1	1. alarm dP PT3/PT4	1	2	11. Investigate water trap freezing possibility
			2. high dP	2			1. alarm dP PT3/PT4			
			3. dehydration of membrane	2			1. alarm dP PT3/PT4			
36. H2 storage tank V1	V1	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT1	1	4	12. Examine risk of continued operation during slow reactant leak
			2. external H2 reaction	4			1. alarm PT1			
		2. tank rupture	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT1	1	4	13. Investigate detection methods for external H2 leak
			2. external H2 reaction	4			1. alarm PT1			
37. O2 storage tank V2	V2	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT2	1	4	14. Investigate the potential severity of a high-pressure O2 leak
			2. external O2 reaction	4			1. alarm PT2			
		2. tank rupture	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT2	1	4	14. Investigate the potential severity of a high-pressure O2 leak
			2. external O2 reaction	4			1. alarm PT2			
38. Coolant reservoir V3	V3	1. external coolant leak	1. low-temperature stack FC1	2	1. mechanical failure	1	1. alarm low level LS3	1	2	
			2. damage to HT1	2			1. alarm low level LS3			
			3. flood system	1			1. alarm low level LS3			
		2. blocked coolant outlet/inlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
	HTX1	1. external coolant leak		4	1. mechanical failure	1	1. alarm low level LS3	1	4	

C-7

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
39. System heat exchanger HTX1		1. low-temperature stack FC1	1. low-temperature stack FC1	4	1. mechanical failure	1	2. alarm low-temperature TC3	1	4	
			2. blocked coolant outlet				1. alarm low level LS3 2. alarm low-temperature TC3			
		3. blocked coolant inlet	1. low-temperature stack FC1	4	1. mechanical failure	1	1. alarm low level LS3 2. alarm low-temperature TC3	1	4	
			4. no air flow	4	1. mechanical failure 2. electrical control failure	1	1. none 1. none	4 4	16 16	2. Consider air flow sensor
		5. reduced air flow	1. high-temperature stack FC1	4	1. mechanical failure	1	1. none	4	16	2. Consider air flow sensor
40. H2 storage fill port check valve CV1	CV1	1. fail close	1. not able to fill storage	4	1. internal failure	1	1. no response PT1	1	4	
		2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
					2. blockage partial	1	1. none	4	4	
		3. fail fully open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
41. Fuel cell stack anode FC1-H2	FC1-H2	1. external H2 gas leak	1. decrease in pressure at cell	1	1. internal failure at cell	1	1. alarm PT3	1	4	
			2. loss of reactant	4			2. monitor cell voltage			
			3. external H2 reaction	4	1. internal failure at cell	1	1. none	4	16	1. Investigate method to detect a H2 leak into coolant
			4. voltage decay at cell	4			1. monitor cell voltage			
		2. cross leak H2 to coolant	1. loss of reactant	4	1. internal failure at cell	1	1. none	4	16	1. Investigate method to detect a H2 leak into coolant
			2. H2 into coolant	4			1. monitor cell voltage			
		3. cross leak H2 to cathode	1. voltage decay at cell	4	1. internal failure at cell	1	1. monitor cell voltage	3	12	
			2. reaction with O2	4	1. internal failure at cell	1	1. monitor cell voltage	2	8	
42. Fuel cell stack cathode FC1-O2	FC1-O2	1. external O2 gas leak	1. decrease in pressure at cell	1	1. internal failure	1	1. alarm PT4	1	4	
			2. loss of reactant	4			2. monitor cell voltage			
			3. external O2 reaction	1	1. internal failure	1	1. none	4	16	
			4. voltage decay at cell	4			1. monitor cell voltage			
		2. cross leak O2 to coolant	1. loss of reactant	4	1. internal failure	1	1. none	4	16	
			2. O2 into coolant	4	1. internal failure	1	1. monitor cell voltage			
43. Fuel cell stack coolant FC1-C	FC1-C	1. cross leak coolant to anode	1. voltage decay at cell	4	1. internal failure at cell	1	1. monitor cell voltage	1	4	
			2. flood stack	4			1. monitor cell voltage			
		2. cross leak coolant to cathode	1. flood stack	4	1. internal failure at cell	1	1. monitor cell voltage	1	4	
			2. voltage decay at cell	4			1. monitor cell voltage			

C-8

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations	
43. Coolant tank stack FC1		3. external coolant leak	1. low-temperature stack FC1	4	1. internal failure at cell	1	1. alarm low level LS3	1	4		
			2. flood system	3			2. alarm low-temperature TC3				
		4. blocked coolant inlet	1. low-temperature stack FC1	4	1. internal failure at cell	1	1. alarm low flow FS1	1	4		
							2. alarm low-temperature TC3				
		5. blocked coolant outlet	1. low-temperature stack FC1	4	1. internal failure at cell	1	1. alarm low flow FS1	1	4		
							2. alarm low-temperature TC3				
		44. O2 storage fill port check valve CV2	1. fail close	1. not able to fill storage	4	1. internal failure	1	1. no response PT2	1	4	
			2. fail partially open	1. none for pre-flight	1	1. internal failure	1	1. none	4	4	
			3. fail fully open	1. none for pre-flight	1	2. blockage partial	1	1. none	4	4	
		45. Coolant tank heater HT1	1. fail on—continuous heat	1. high-temperature stack FC1	4	1. electrical control failure	1	1. alarm high temp TC3/4	1	4	9. Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load
			2. fail off—no heat	1. low-temperature stack FC1	4	1. internal failure	1	1. alarm low-temperature TC3	1	4	
						2. electrical control failure	1	1. alarm low-temperature TC3	1	4	

C-9

APPENDIX D—EPS STANDBY WORKSHEETS

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT1	1	3	
		3. fail closed	1. none on standby	1	1. internal failure	1	1. none	4	4	
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT2	1	4	
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT2	1	3	
		3. fail closed	1. none on standby	1	1. internal failure	1	1. none	4	4	
3. H2 delivery relief valve RV3	RV3	1. fail closed	1. none on standby	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT5	1	4	
			2. loss of pressure	4						
			3. high dP on stack	3						
		3. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT5	3	9	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			2. loss of pressure	2						
			3. high dP on stack	1						
4. O2 delivery relief valve RV4	RV4	1. fail closed	1. none on standby	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT6	1	4	
			2. loss of pressure	4						
			3. high dP on stack	3						
		3. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT6	3	9	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			2. loss of pressure	2						
			3. high dP on stack	1						
5. H2 delivery inlet solenoid valve, NC SV1	SV1	1. fail closed	1. reactant not available	4	1. internal failure	1	1. none	4	16	12. Consider redundant inlet valves
		2. fail fully open	1. high dP on stack	4	2. electrical control failure	1	1. none	4	16	12. Consider redundant inlet valves
					1. internal failure	1	1. alarm PT3	1	4	
		3. fail partially open	1. high dP on stack	4	2. electrical control failure	1	1. alarm PT3	1	4	
					1. internal failure	1	1. alarm PT3	1	4	
					2. blockage partial	1	1. alarm PT3	1	4	
6. O2 delivery inlet solenoid valve, NC SV2	SV2	1. fail closed	1. reactant not available	4	1. internal failure	1	1. none	4	16	12. Consider redundant inlet valves
		2. fail fully open	1. high dP on stack	4	2. electrical control failure	1	1. none	4	16	12. Consider redundant inlet valves
					1. internal failure	1	1. alarm PT4	1	4	
		3. fail partially open	1. high dP on stack	4	2. electrical control failure	1	1. alarm PT4	1	4	
					1. internal failure	1	1. alarm PT4	1	4	
					2. blockage partial	1	1. alarm PT4	1	4	

D-1

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
7. H2 water trap drain solenoid valve, NC SV3	SV3	1. fail fully open—open drain	1. backflow of air	2	1. electrical control failure	1	1. alarm dP PT3/PT4	1	2	17. Consider a check valve to prevent backflow
			2. high dP	2	2. internal failure	1	1. alarm dP PT3/PT4	1	2	18. Investigate water trap freezing possibility
			3. dehydration of membrane	2						
		2. fail partially open	1. backflow of air	2	1. blockage	1	1. alarm dP PT3/PT4	1	2	
			2. high dP	2						
			3. dehydration of membrane	2						
		3. fail closed—closed drain	1. none on standby	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	1	1. none	4	4	17. Consider a check valve to prevent backflow
8. O2 water trap drain solenoid valve, NC SV4	SV4	1. fail fully open—open drain	1. backflow of air	1	1. electrical control failure	1	1. alarm dP PT3/PT4	1	2	18. Investigate water trap freezing possibility
			2. high dP	2	2. internal failure	1	1. alarm dP PT3/PT4	1	2	
			3. dehydration of membrane	2						
		2. fail partially open	1. backflow of air	2	1. blockage	1	1. alarm dP PT3/PT4	1	2	
			2. high dP	2						
			3. dehydration of membrane	1						
		3. fail closed—closed drain	1. none on standby	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	1	1. none	4	4	
9. H2 vent solenoid valve, NC SV5	SV5	1. fail fully open—open vent	1. backflow of air	2	1. electrical control failure	1	1. alarm dP PT3/PT4	1	2	17. Consider a check valve to prevent backflow
			2. high dP	2	2. internal failure	1	1. alarm high delta temp TC4/TC3	1	2	
			3. dehydration of membrane	2						
		2. fail partially open	1. backflow of air	2	1. blockage	1	1. alarm dP PT3/PT4	1	2	
			2. high dP	2						
			3. dehydration of membrane	2						
		3. fail closed—closed vent	1. none on standby	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	1	1. none	4	4	
10. O2 vent solenoid valve, NC SV6	SV6	1. fail fully open—open vent	1. backflow of air	1	1. electrical control failure	1	1. alarm dP PT3/PT4	1	2	17. Consider a check valve to prevent backflow
			2. high dP	2	2. internal failure	1	1. alarm dP PT3/PT4	1	2	
			3. dehydration of membrane	2						
		2. fail partially open	1. backflow of air	1	1. blockage	1	1. alarm dP PT3/PT4	1	2	

D-2

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
D-3	MV4	3. fail closed—closed vent	2. high dP	2						
			3. dehydration of membrane	2						
			1. none on standby	1		1. electrical control failure	1. none	4	4	
		2. internal failure	1. none on standby	1		2. internal failure	1. none	4		
			2. loss of pressure on operation	4		1. internal failure	1. none	4	16	10. Consider redundancy, also look at maintenance issues
		2. fail partially open	1. none on standby	1		1. internal failure	1. none	4	16	10. Consider redundancy, also look at maintenance issues
			2. decrease in pressure on operation	4						
		3. fail fully open	1. none	1	1. internal failure	1. none	4	4		
	MV1	1. fail close	1. none on standby	1	1. internal failure	1. none	4	4		
		2. fail partially open	1. none on standby	1	1. internal failure	1. none	4	4		
		3. fail fully open	1. none on standby	1	1. internal failure	1. none	4	4		
D-3	MV2	1. fail close	1. none on standby	1	1. internal failure	1. none	4	16		10. Consider redundancy, also look at maintenance issues
			2. loss of pressure on operation	4						
		2. fail partially open	1. none on standby	1	1. internal failure	1. none	4	16		10. Consider redundancy, also look at maintenance issues
			2. loss of pressure on operation	4						
		3. fail fully open	1. none	1	1. internal failure	1. none	4	4		
D-3	MV3	1. fail close	1. none on standby	1	1. internal failure	1. none	4	4		
		2. fail partially open	1. none on standby	1	1. internal failure	1. none	4	4		
		3. fail fully open	1. none on standby	1	1. internal failure	1. none	4	4		
D-3	FPR1	1. fail closed, no outlet press	1. loss of pressure	4	1. internal failure	1. none	4	16	11. Consider small flow to indicate regulator function	
					2. blockage					
		2. fail partial closed, low outlet press	1. decrease in pressure	2	1. internal failure	1. none	4	8	15. Include dP alarm PT5/PT6	
			2. high dP	2	2. blockage	1. none	4	8	15. Include dP alarm PT5/PT6	
			3. setpoint drift	2	3. setpoint drift	1. none	4	16	12. Consider redundant inlet valves	
		3. fail open, high outlet press	1. loss of reactant	4	1. internal failure	1. alarm PT5	1	4	8. Describe how to size RV3/RV4 for full high-pressure storage flow	
					2. setpoint drift	1. alarm PT5	1	4	8. Describe how to size RV3/RV4 for full high-pressure storage flow	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
16. O2 delivery pressure regulator FPR2	FPR2	1. fail closed, no outlet press	1. loss of pressure	4	1. internal failure	1	1. none	4	16	11. Consider small flow to indicate regulator function
					2. blockage	1	1. none	4	16	12. Consider redundant inlet valves
					1. decrease in pressure	1	1. none	4	8	11. Consider small flow to indicate regulator function
		2. fail partial closed, low outlet press	2. high dP	2	2. blockage	1	1. none	4	8	12. Consider redundant inlet valves
					3. setpoint drift	2	1. none	4	16	15. Include dP alarm PT5/PT6
					1. loss of reactant	1	1. alarm PT6	1	4	15. Include dP alarm PT5/PT6
		3. fail open, high outlet press		4	2. setpoint drift	1	1. alarm PT6	1	4	12. Consider redundant inlet valves
					1. internal failure	1				8. Describe how to size RV3/RV4 for full high-pressure storage flow
					2. setpoint drift	1				8. Describe how to size RV3/RV4 for full high-pressure storage flow
D-4	PT1	1. fail high—high electrical output	1. incorrect storage amount	3	1. electrical control failure	1	1. none	4	12	3. Consider redundant PTs on reactant storage tanks
					2. internal failure	1	1. none	4	12	3. Consider redundant PTs on reactant storage tanks
		2. fail low—low electrical output	1. incorrect storage amount	4	1. electrical control failure	1	1. check for gas at PT5	1	4	3. Consider redundant PTs on reactant storage tanks
					2. internal failure	1	1. check for gas at PT5	1	4	3. Consider redundant PTs on reactant storage tanks
		3. drift high or low	1. incorrect storage amount	3	1. internal failure	1	1. none	4	12	3. Consider redundant PTs on reactant storage tanks
		18. O2 storage pressure transmitter PT2	1. incorrect storage amount	3	1. electrical control failure	1	1. none	4	12	3. Consider redundant PTs on reactant storage tanks
					2. internal failure	1	1. none	4	12	3. Consider redundant PTs on reactant storage tanks
					1. electrical control failure	1	1. check for gas at PT6	1	4	4. Include redundancy check in controls
		2. fail low—low electrical output	1. incorrect storage amount	4	2. internal failure	1	1. check for gas at PT6	1	4	4. Include redundancy check in controls
					1. internal failure	1				3. Consider redundant PTs on reactant storage tanks
19. H2 stack pressure transmitter PT3	PT3	1. fail high—high electrical output	1. none on standby	1	1. internal failure	1	1. none	4	4	
		2. fail low—low electrical output	1. none on standby	1	1. internal failure	1	1. none	4	4	
		3. drift high or low	1. none on standby	1	1. internal failure	1	1. none	4	4	
20. O2 stack pressure transmitter PT4	PT4	1. fail high—high electrical output	1. none on standby	1	1. internal failure	1	1. none	4	4	
		2. fail low—low electrical output	1. none on standby	1	1. internal failure	1	1. none	4	4	
		3. drift high or low	1. none on standby	1	1. internal failure	1	1. none	4	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
21. H2 delivery pressure transmitter PT5	PT5	1. fail high—high electrical output	1. false alarm high pressure	4	1. internal failure	1	1. check pressure decay at PT1	1	4		
		2. fail low—low electrical output	1. false alarm low pressure	4	1. internal failure	1	1. check pressure decay at PT1	1	4		
		3. drift high or low	1. false alarm high pressure	1	1. internal failure	1	1. check pressure decay at PT1	1	1		
			2. false alarm low pressure	1							
22. O2 delivery pressure transmitter PT6	PT6	1. fail high—high electrical output	1. false alarm high pressure	1	1. internal failure	1	1. check pressure decay at PT2	1	1		
		2. fail low—low electrical output	1. false alarm low pressure	1	1. internal failure	1	1. check pressure decay at PT2	1	1		
		3. drift high or low	1. false alarm high pressure	1	1. internal failure	1	1. check pressure decay at PT2	1	1		
			2. false alarm low pressure	1							
D-5 23. H2 storage temperature transmitter T1	T1	1. fail high—high electrical output	1. false alarm high temperature	1	1. electrical control failure	1	1. temperature out of instrument range	3	3		
					2. internal failure	1	1. temperature out of instrument range	3	3		
		2. fail low—low electrical output	1. false alarm low temperature	1	1. electrical control failure	1	1. temperature out of instrument range	3	3		
					2. internal failure	1	1. temperature out of instrument range	3	3		
		3. drift high or low	1. inaccurate storage temperature	1	1. internal failure	1	1. none	4	4		
24. O2 storage temperature transmitter T2	T2	1. fail high—high electrical output	1. false alarm high temperature	1	1. electrical control failure	1	1. temperature out of instrument range	3	3		
					2. internal failure	1	1. temperature out of instrument range	3	3		
		2. fail low—low electrical output	1. false alarm low temperature	1	1. electrical control failure	1	1. temperature out of instrument range	3	3		
					2. internal failure	1	1. temperature out of instrument range	3	3		
		3. drift high or low	1. Inaccurate storage temperature	1	1. internal failure	1	1. none	4	4		
25. Coolant inlet temperature transmitter T3	T3	1. fail high—high electrical output	1. false alarm high temperature	1	1. internal failure	1	1. check T4 for redundant alarm	1	1	20. Develop a backup thermal control scheme using T4.	
							2. check FS1 for flow				
				1	2. electrical control failure	1	1. check T4 for redundant alarm	1	1		
							2. check FS1 for flow				

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
D-6		2. fail low—low electrical output	1. High-temperature stack FC1	3	1. internal failure	1	1. check T4 for acceptable temp	1	3	20. Develop a backup thermal control scheme using T4.
							2. check FS1 for flow			
					2. electrical control failure	1	1. check T4 for acceptable temp	1	3	
							2. check FS1 for flow			
		3. drift high or low	1. false alarm high temperature	1	1. internal failure	1	1. T4 redundant	1	1	20. Develop a backup thermal control scheme using T4.
							2. check FS1			
		26. Coolant outlet temperature transmitter T4	T4	1. fail high—high electrical output	1. false delta T alarm	1	1. internal failure	1	1	
							2. electrical control failure	1	1	
				2. fail low—low electrical output	1. false delta T alarm	1	1. internal failure	1	1	
				2. electrical control failure			1. check FS1 for flow	1	1	
				3. drift high or low	1. false delta T alarm	1	1. internal failure	1	1	
	27. H2 water trap level switch LS1	LS1	1. fail set—SV3 remains open	1. none on standby	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
			2. fail open -SV3 remains closed	1. none on standby	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
	28. O2 water trap level switch LS2	LS2	1. fail set—SV4 remains	1. none on standby	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
			2. fail open -SV4 remains closed	1. none on standby	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
	29. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none on standby	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
			2. fail open—electrically open empty	1. false low level indication	1	1. electrical control failure	1	1. none	4	4
						2. internal failure	2	1. none	4 8	
	30. Coolant flow switch FS1	FS1	1. failed closed—indicates flow	1. none on standby	1	1. internal failure	1	1. none	4	
			2. failed open—indicates no flow	1. false alarm no flow	1	1. internal failure	1	1. check T3	1	1
31. H2 recirculation pump M1	M1	1. external gas leak	1. external leak	1	1. mechanical failure	1	1. none	4	4	
32. O2 recirculation pump M2	M2	1. external gas leak	1. external leak	1	1. mechanical failure	1	1. none	4	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	Det	RPN	Recommendations
33. Coolant circulation pump M3	M3	1. pumping stops	1. low-temperature stack FC1	2	1. electrical control failure	1	1. alarm low flow FS1	1	2	
					2. internal failure	1	1. alarm low flow FS1	1	2	
		2. pumping reduced	1. low-temperature stack FC1	2	1. blockage partial	1	1. alarm low temp TC4	1	2	
					2. electrical control failure	1	1. alarm low temp TC4	1	2	
					3. internal failure	1	1. alarm low temp TC4	1	2	
		3. external coolant leak	1. low-temperature stack FC1	2	1. mechanical failure	1	1. alarm low level LS3	1	2	
34. H2 water trap WT1	WT1	1. external gas leak	1. backflow of air	2	1. mechanical failure	1	1. alarm dP PT3/PT4	1	2	18. Investigate water trap freezing possibility
			2. high dP	2						
			3. dehydration of membrane	2						
35. O2 water trap WT2	WT2	1. external gas leak	1. backflow of air	1	1. mechanical failure	1	1. alarm dP PT3/PT4	1	2	18. Investigate water trap freezing possibility
			2. high dP	2						
			3. dehydration of membrane	2						
36. H2 storage tank V1	V1	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT1	1	4	2. Examine risk of continued operation during slow reactant leak
			2. external H2 reaction	4						
		2. tank rupture	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT1	1	4	16. Investigate detection methods for external H2 leak
			2. external H2 reaction	4						
37. O2 storage tank V2	V2	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT2	1	4	7. Investigate the potential severity of a high-pressure O2 leak
			2. external O2 reaction	4						
		2. tank rupture	1. loss of reactant	3	1. mechanical failure	1	1. alarm PT2	1	4	7. Investigate the potential severity of a high-pressure O2 leak
			2. external O2 reaction	4						
38. Coolant reservoir V3	V3	1. external coolant leak	1. low-temperature stack FC1	2	1. mechanical failure	1	1. alarm low level LS3	1	2	
			2. damage to HT1	2						
			3. flood system	1						
		2. blocked coolant outlet/inlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
39. System heat exchanger HTX1	HTX1	1. external coolant leak	1. low-temperature stack FC1	2	1. mechanical failure	1	1. alarm low level LS3	1	2	
		2. blocked coolant outlet	1. low-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		3. blocked coolant inlet	1. low-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		4. no air flow	1. high-temperature stack FC1	1	1. mechanical failure	1	1. alarm high temp TC4	1	1	13. Examine heater vs fan thermal control (or both) while on standby

D-7

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
					2. electrical control failure	1	1. alarm high temp TC4	1	1	
		5. reduced air flow	1. high-temperature stack FC1	1	1. mechanical failure 2. electrical control failure	1	1. alarm high temp TC4 1. alarm high temp TC4	1	1	
40. H2 storage fill port check valve CV1	CV1	1. fail close 2. fail partially open 3. fail fully open	1. none on standby	1	1. internal failure	1	1. none	4	4	
41. Fuel cell stack anode FC1-H2	FC1-H2	1. external gas leak	1. backflow of air	2	1. mechanical failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	2	
42. Fuel cell stack cathode FC1-O2	FC1-O2	1. external gas leak	1. backflow of air	1	1. mechanical failure	1	1. alarm PT4 2. alarm dP PT3/PT4	1	1	
D-8	FC1-C	1. cross leak coolant to anode	1. coolant poisoning of catalyst 2. flooding anode	3	1. internal failure	1	1. alarm low level LS3 2. alarm PT3	3	12	19. Consider monitoring stack pressure rise for detecting coolant leak
		2. cross leak coolant to cathode	1. coolant poisoning of catalyst 2. flooding anode	3	1. internal failure	1	1. alarm low level LS3 2. alarm PT4	3	12	19. Consider monitoring stack pressure rise for detecting coolant leak
		3. external coolant leak	1. low-temperature stack FC1	2	1. mechanical failure	1	1. alarm low level LS3	1	2	
		4. blocked coolant inlet	1. low-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		5. blocked coolant outlet	1. low-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
44. O2 storage fill port check valve CV2	CV2	1. fail close 2. fail partially open 3. fail fully open	1. none on standby	1	1. internal failure	1	1. none	4	4	
45. Coolant tank heater HT1	HT1	1. fail on—continuous heat 2. fail off—no heat	1. high-temperature stack FC1 1. low-temperature stack FC1	3	1. electrical control failure	1	1. alarm high temp TC3/4 1. alarm low temp TC4 1. alarm low temp TC4	1	3	5. Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load 6. Include thermal switch on V3 for redundancy

APPENDIX E—EPS POWER-PRODUCTION WORKSHEETS

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. alarm PT1	1	3	
		3. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		2. fail partially open	1. loss of reactant	4	1. internal failure	1	1. alarm PT1	1	4	
		3. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
E-1	RV3	1. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant	3	1. internal failure	1	1. alarm PT5 or PT3	1	4	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			2. loss of pressure	4			2. alarm dP PT3/PT4			
			3. high dP on stack	3			1. alarm PT5 or PT3	4	12	
		3. fail partially open	1. loss of reactant	3			2. alarm dP PT3/PT4			
			2. loss of pressure	2			1. alarm PT6 or PT4	1	4	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			3. high dP on stack	1			2. alarm dP PT3/PT4			
E-1	RV4	1. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant	3	1. internal failure	1	1. alarm PT6 or PT4	1	4	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			2. loss of pressure	4			2. alarm dP PT3/PT4			
			3. high dP on stack	3			1. alarm PT6 or PT4	4	12	
		3. fail partially open	1. loss of reactant	3			2. alarm dP PT3/PT4			
			2. loss of pressure	2			1. alarm PT6 or PT4	4	12	1. Develop an algorithm to compute remaining run time due to a slow loss of reactant.
			3. high dP on stack	1			2. alarm dP PT3/PT4			
E-1	SV1	1. fail closed	1. loss of pressure	4	1. internal failure	1	1. alarm PT3	1	4	
		2. high dP on stack	4	2. electrical control failure	1	1. alarm PT3	1	4		
		3. loss of power	4	1. alarm PT3	1	4				
		2. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
			2. electrical control failure	1	1. none	4	4			
			3. loss of power	4	1. none	4	4			
E-1	SV2	1. fail closed	1. loss of pressure	4	1. internal failure	1	1. alarm PT4	1	4	
		2. high dP on stack	4	2. electrical control failure	1	1. alarm PT4	1	4		
		3. loss of power	4	1. alarm PT4	1	4				

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
E-2	SV3	2. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4		
					2. electrical control failure	1	1. none	4	4		
		3. fail partially open	1. decrease in pressure	2	1. internal failure	1	1. alarm PT4	1	4		
			2. high dP on stack	2	2. blockage partial	1	1. alarm PT4	1	4		
			3. loss of power	4							
		1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3	1	4	13. Describe sizing orifice restriction to allow low-pressure operation	
			2. loss of reactant	3		1	2. alarm dP PT3/PT4				
			3. high dP on stack	3		1	3. alarm low cell voltage				
					2. internal failure	1	1. alarm PT3	1	4		
						1	2. alarm dP PT3/PT4	1	4		
						1	3. alarm low cell voltage	1	4		
		2. fail partially open	1. decrease in pressure	2	1. blockage	1	1. alarm PT3	1	6	13. Describe sizing orifice restriction to allow low-pressure operation	
			2. loss of reactant	3		2	2. alarm dP PT3/PT4				
			3. high dP on stack	2		2	3. alarm low cell voltage				
		3. fail closed—closed drain	1. overflow of WT1	3	1. electrical control failure	1	1. amp-hr check on water accumulation	1	3		
					2. internal failure	1	1. amp-hr check on water accumulation	1	3		
		SV4	1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT4	1	4	13. Describe sizing orifice restriction to allow low-pressure operation
				2. loss of reactant	3		1	2. alarm dP PT3/PT4			
				3. high dP on stack	3		1	3. alarm low cell voltage			
			2. fail partially open	1. decrease in pressure	2	2. internal failure	1	1. alarm PT4	1	4	13. Describe sizing orifice restriction to allow low-pressure operation
				2. loss of reactant	3		1	2. alarm dP PT3/PT4			
				3. high dP on stack	2		1	3. alarm low cell voltage			
						1. blockage	1	1. alarm PT4	1	6	13. Describe sizing orifice restriction to allow low-pressure operation
							2	2. alarm dP PT3/PT4			
							2	3. alarm low cell voltage			
			3. fail closed—closed drain	1. overflow of WT2	3	1. electrical control failure	1	1. amp-hr check on water accumulation	1	3	
						2	1. LS2 remains set	1	3		
						2	2. internal failure	1	3		
						1	1. amp-hr check on water accumulation	1	3		
						1	2. LS2 remains set	1	3		
		SV5	1. fail fully open—open vent	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3	1	4	13. Describe sizing orifice restriction to allow low-pressure operation
				2. loss of reactant	3		1	2. alarm dP PT3/PT4			
				3. high dP on stack	3		1	3. alarm low cell voltage			
						2. internal failure	2	1. alarm PT3	1	8	13. Describe sizing orifice restriction to allow low-pressure operation
							2	2. alarm dP PT3/PT4			

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
E-3	SV6	2. fail partially open	1. decrease in pressure 2. loss of reactant 3. high dP on stack	2	1. blockage	2	3. alarm low cell voltage	1	6	13. Describe sizing orifice restriction to allow low-pressure operation	
							1. alarm PT3				
							2. alarm dP PT3/PT4				
		3. fail closed—closed vent	1. decaying voltage—inert buildup	2	1. electrical control failure 2. internal failure	1	3. alarm low cell voltage	1	4		
							1. alarm low cell voltage				
							2. alarm low cell voltage				
		10. O2 vent solenoid valve, NC SV6	1. fail fully open—open vent	1. loss of pressure 2. loss of reactant 3. high dP on stack	4	1. electrical control failure	1	1. alarm PT4	1	4	
							2. alarm dP PT3/PT4				
							3. alarm low cell voltage				
		2. fail partially open	1. decrease in pressure 2. loss of reactant 3. high dP on stack	2	1. blockage	2	1. alarm PT4	1	6	13. Describe sizing orifice restriction to allow low-pressure operation	
							2. alarm dP PT3/PT4				
							3. alarm low cell voltage				
		11. H2 storage manual isolation valve, MV4	3. fail closed—closed vent	1. decaying voltage—inert buildup	2	1. electrical control failure 2. internal failure	1	1. alarm low cell voltage	1	2	
							2. alarm low cell voltage				
							1. alarm low cell voltage				
		12. H2 storage manual fill valve MV1	1. fail close	1. none on normal operation	1	1. internal failure	1	1. alarm PT5	1	4	
							1. alarm PT5				
							1. none	4	4		
		13. O2 storage manual isolation valve MV2	2. fail partially open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
							1. none				
							1. none				
		14. O2 storage manual fill valve MV3	3. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
							1. none				
							1. none				
	FPR1		1. loss of pressure	4	1. internal failure	1	1. alarm PT5 or PT3	1	4		

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
E-4	15. H2 delivery pressure regulator FPR1	1. fail closed, no outlet press	2. high dP on stack	3			2. alarm dP PT3/PT4			
					2. blockage	1	1. alarm PT5 or PT3 2. alarm dP PT3/PT4	1	4	
		2. fail partial closed, low outlet press	1. decrease in pressure	2	1. internal failure	1	1. alarm dP PT3/PT4	1	2	
			2. high dP on stack	2	2. blockage	1	1. alarm dP PT3/PT4	1	2	
					3. setpoint drift	2	1. alarm dP PT3/PT4	1	4	
		3. fail open, high outlet press	1. high dP on stack	4	1. internal failure	1	1. alarm PT5 or PT3 2. alarm dP PT3/PT4	1	4	
			2. high press on system components	4			3. pressure relief RV3			
			3. tube or component rupture	4	2. setpoint drift		1. alarm PT5 or PT3 2. alarm dP PT3/PT4 3. pressure relief RV3			20. Describe how to size RV3/RV4 for full high-pressure storage flow
	16. O2 delivery pressure regulator FPR2	1. fail closed, no outlet press	1. loss of pressure	4	1. internal failure	1	1. alarm PT6 or PT4 2. alarm dP PT3/PT4	1	4	
			2. high dP on stack	3	2. blockage	1	1. alarm PT6 or PT4 2. alarm dP PT3/PT4	1	4	
		2. fail partial closed, low outlet press	1. decrease in pressure	2	1. internal failure	1	1. alarm dP PT3/PT4	1	2	
			2. high dP on stack	2	2. blockage	1	1. alarm dP PT3/PT4	1	2	
					3. setpoint drift	2	1. alarm dP PT3/PT4	1	4	
		3. fail open, high outlet press	1. high dP on stack	4	1. internal failure	1	1. alarm PT6 or PT4 2. alarm dP PT3/PT4	1	4	
			2. high press on system components	4			3. pressure relief RV4			
			3. tube or component rupture	4	2. setpoint drift		1. alarm PT6 or PT4 2. alarm dP PT3/PT4 3. pressure relief RV4			
	17. H2 storage pressure transmitter PT1	1. fail high—high electrical output	1. incorrect storage amount	3	1. electrical control failure	1	1. amp-hr check on reactant consumption vs pressure	2	6	11. Include the need to verify reactant tank PT accuracy during pre-flight routine
					2. internal failure	1	1. amp-hr check on reactant consumption vs pressure	2	6	14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. incorrect storage amount	3	1. electrical control failure	1	1. check for gas at PT5	1	3	14. Include PT redundancy check in controls
					2. internal failure	1	1. check for gas at PT5	1	3	14. Include PT redundancy check in controls
		3. drift high or low	1. incorrect storage amount	3	1. internal failure	1	1. none	4	12	12. Consider including redundant PTs on reactant storage tanks

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
18. O2 storage pressure transmitter PT2	PT2	1. fail high—high electrical output	1. incorrect storage amount	3	1. electrical control failure 2. internal failure	1 1	1. amp-hr check on reactant consumption vs pressure 1. amp-hr check on reactant consumption vs pressure	2 2	6 6	11. Include the need to verify reactant tank PT accuracy during pre-flight routine 14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. incorrect storage amount	3	1. electrical control failure 2. internal failure	1 1	1. check for gas at PT6 1. check for gas at PT6	2 1	6 3	14. Include PT redundancy check in controls 14. Include PT redundancy check in controls
		3. drift high or low	1. incorrect storage amount	3	1. internal failure	1	1. none	4	12	12. Consider including redundant PTs on reactant storage tanks
19. H2 stack pressure transmitter PT3	PT3	1. fail high—high electrical output	1. false alarm high pressure 2. false alarm high dP	4 4	1. internal failure	1	1. alarm PT5	1	4	14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. false alarm low pressure 2. false alarm high dP	4 4	1. internal failure	1	1. alarm PT5	1	4	14. Include PT redundancy check in controls
		3. drift high or low	1. false alarm high pressure 2. false alarm low pressure 3. false alarm high dP	4 4 4	1. internal failure	1	1. alarm PT5	1	4	14. Include PT redundancy check in controls
20. O2 stack pressure transmitter PT4	PT4	1. fail high—high electrical output	1. false alarm high pressure 2. false alarm high dP	4 4	1. internal failure	1	1. alarm PT6	1	4	14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. false alarm high pressure 2. false alarm high dP	4 4	1. internal failure	1	1. alarm PT6	1	4	14. Include PT redundancy check in controls
		3. drift high or low	1. false alarm high pressure 2. false alarm low pressure 3. false alarm high dP	4 4 4	1. internal failure	1	1. alarm PT6	1	4	14. Include PT redundancy check in controls
21. H2 delivery pressure transmitter PT5	PT5	1. fail high—high electrical output	1. false alarm high pressure	1	1. internal failure	1	1. alarm PT3	1	1	14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. false alarm low pressure	1	1. internal failure	1	1. alarm PT3	1	1	14. Include PT redundancy check in controls
		3. drift high or low	1. false alarm high pressure 2. false alarm low pressure	1 1	1. internal failure	1	1. alarm PT3	1	1	14. Include PT redundancy check in controls

E-5

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
22. O2 delivery pressure transmitter PT6	PT6	1. fail high—high electrical output	1. false alarm high pressure	1	1. internal failure	1	1. alarm PT4	1	1	14. Include PT redundancy check in controls
		2. fail low—low electrical output	1. false alarm high pressure	1	1. internal failure	1	1. alarm PT4	1	1	14. Include PT redundancy check in controls
		3. drift high or low	1. false alarm high pressure	1	1. internal failure	1	1. alarm PT4	1	1	14. Include PT redundancy check in controls
			2. false alarm low pressure	1						
23. H2 storage temperature transmitter T1	T1	1. fail high—high electrical output	1. false alarm high temperature	1	1. electrical control failure	1	1. alarm out of operational range	3	3	
					2. internal failure	1	1. alarm out of operational range	3	3	
		2. fail low—low electrical output	1. false alarm low temperature	1	1. electrical control failure	1	1. alarm out of operational range	3	3	
					2. internal failure	1	1. alarm out of operational range	3	3	
		3. drift high or low	1. inaccurate storage temperature	1	1. internal failure	1	1. none	4	4	
24. O2 storage temperature transmitter T2	T2	1. fail high—high electrical output	1. false alarm high-temperature	1	1. electrical control failure	1	1. alarm out of operational range	3	3	
					2. internal failure	1	1. alarm out of operational range	3	3	
		2. fail low—low electrical output	1. false alarm low temperature	1	1. electrical control failure	1	1. alarm out of operational range	3	3	
					2. internal failure	1	1. alarm out of operational range	3	3	
		3. drift high or low	1. inaccurate storage temperature	1	1. internal failure	1	1. none	4	4	
25. Coolant inlet temperature transmitter T3	T3	1. fail high—high electrical output	1. false alarm high-temperature	1	1. internal failure	1	1. check T4 for redundant alarm 2. check FS1 for flow	1	1	22. Develop a backup thermal control scheme using T4.
					2. electrical control failure	1	1. check T4 for redundant alarm 2. check FS1 for flow			
		2. fail low—low electrical output	1. high temperature stack FC1	3	1. internal failure	1	1. check T4 for acceptable temp 2. check FS1 for flow	1	3	22. Develop a backup thermal control scheme using T4.
					2. electrical control failure	1	1. check T4 for acceptable temp 2. check FS1 for flow			
		3. drift high or low	1. false alarm high-temperature	1	1. internal failure	1	1. T4 redundant 2. check FS1 for flow	1	1	22. Develop a backup thermal control scheme using T4.
			2. false delta T alarm							

E-6

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
26. Coolant outlet temperature transmitter T4	T4	1. fail high—high electrical output	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
					2. electrical control failure	1	1. check FS1 for flow	1	1	
		2. fail low—low electrical output	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
		3. drift high or low	1. false delta T alarm	1	2. electrical control failure	1	1. check FS1 for flow	1	1	
27. H2 water trap level switch LS1	LS1	1. fail set—SV3 remains open after amp-hr count	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3	1	4	
			2. loss of reactant	3	2. internal failure	2	1. alarm PT3	1	8	13. Describe sizing orifice restriction to allow low-pressure operation
			3. high dP on stack	3						
		2. fail open -SV3 remains closed	1. overflow of WT1	3	1. electrical control failure	1	1. amp-hr check on water accumulation	1	3	
					2. internal failure	2	1. amp-hr check on water accumulation	1	6	7. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
28. O2 water trap level switch LS2	LS2	1. fail set—SV4 remains open after amp-hr count	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT4	1	4	
			2. loss of reactant	3	2. internal failure	2	1. alarm PT4	1	8	13. Describe sizing orifice restriction to allow low-pressure operation
			3. high dP on stack	3						
		2. fail open -SV4 remains closed	1. overflow of WT1	3	1. electrical control failure	1	1. amp-hr check on water accumulation	1	3	
					2. internal failure	2	1. amp-hr check on water accumulation	1	6	7. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
29. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none on normal operation	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	21. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.
		2. fail open—electrically open empty	1. false low level indication	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	21. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.
30. Coolant flow switch FS1	FS1	1. failed closed—indicates flow	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. failed open—indicates no flow	1. false alarm no flow	1	1. internal failure	1	1. alarm high delta temp TC4/TC3	1	1	
31. H2 recirculation pump M1	M1	1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	3	8. Consider second PT to indicate adequate flow as indicated by pressure drop
			2. flood stack	3	2. internal failure	1	1. alarm low cell voltage	1	3	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
E-8	M2	3. poor reactant mass transport	3. poor reactant mass transport	3						9. Include a monitor for current draw on reactant recirculation pump
			4. voltage decay at cell	2						
		2. external gas leak	1. external H ₂ reaction	4	1. mechanical failure	1	1. none	4	16	2. Investigate detection methods for external H ₂ leak
			2. loss of reactant	3						5. Examine risk of continued operation during slow reactant leak
		3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. flood stack	2						
			3. poor reactant mass transport	2						
		4. mechanical degradation	1. stack contamination	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. cell flow channel restriction	2	2. internal failure	1	1. none	4	8	10. Consider adding filter downstream of reactant pump
		1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	3	8. Consider second PT to indicate adequate flow as indicated by pressure drop
			2. flood stack	3	2. internal failure	1	1. alarm low cell voltage	1	3	9. Include a monitor for current draw on reactant recirculation pump
			3. poor reactant mass transport	3						
			4. voltage decay at cell	2						
		2. external gas leak	1. external O ₂ reaction	1	1. mechanical failure	1	1. none	4	12	5. Examine risk of continued operation during slow reactant leak
			2. loss of reactant	3						
		3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. flood stack	2						
			3. poor reactant mass transport	2						
		4. mechanical degradation	1. stack contamination	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. cell flow channel restriction	2	2. internal failure	1	1. none	4	8	10. Consider adding filter downstream of reactant pump
		1. pumping stops	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm low flow FS1	1	3	
			2. internal failure		1. internal failure	1	1. alarm low flow FS1	1	3	
		2. pumping reduced	1. high-temperature stack FC1	2	1. blockage partial	1	1. alarm high temp TC4	1	2	
			2. high delta temperature FC1				2. alarm high delta temp TC4/TC3			
				2	2. electrical control failure	1	1. alarm high temp TC4	1	2	
							2. alarm high delta temp TC4/TC3			

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
					3. internal failure	1	1. alarm high temp TC4 2. alarm high delta temp TC4/TC3	1	2	
		3. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
34. H2 water trap WT1	WT1	1. external gas leak	1. high dP on stack 2. loss of reactant 3. decrease in pressure	2	1. mechanical failure	1	1. alarm PT3 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	3	5. Examine risk of continued operation during slow reactant leak 2. Investigate detection methods for external H2 leak
		2. external water leak without gas	1. none on normal operation	1	1. internal failure	1	1. none	4	4	6. Compute total product water available for worst case flooding risk
		3. overflow—water in gas circuit	1. flood pump M1 2. flood stack	2	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
		4. overflow anode vent	1. product water out vent 2. less effective purge 3. no purge	1	1. blocked drain	1	1. amp-hr check on water accumulation	1	2	
E-9	WT2	1. external gas leak	1. high dP on stack 2. loss of reactant 3. decrease in pressure	2	1. mechanical failure	1	1. alarm PT4 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	3	
		2. external water leak without gas	1. none on normal operation	1	1. internal failure	1	1. none	4	4	6. Compute total product water available for worst case flooding risk
		3. overflow—water in gas circuit	1. flood pump M1 2. flood stack	2	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
		4. overflow cathode vent	1. product water out vent 2. less effective purge 3. no purge	1	1. blocked drain	1	1. amp-hr check on water accumulation	1	2	
36. H2 storage tank V1	V1	1. external gas leak	1. loss of reactant 2. external H2 reaction	3	1. mechanical failure	1	1. alarm PT1	1	4	2. Investigate detection methods for external H2 leak
		2. tank rupture	1. loss of reactant 2. external H2 reaction	4	1. mechanical failure	1	1. alarm PT1	1	4	
37. O2 storage tank V2	V2	1. external gas leak	1. loss of reactant 2. external O2 reaction	3	1. mechanical failure	1	1. alarm PT2	1	4	19. Investigate the potential severity of a high-pressure O2 leak
		2. tank rupture	1. loss of reactant 2. external O2 reaction	4	1. mechanical failure	1	1. alarm PT2	1	4	19. Investigate the potential severity of a high-pressure O2 leak
38. Coolant reservoir V3	V3	1. external coolant leak	1. high-temperature stack FC1 2. damage to HT1 3. flood system	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
		2. blocked coolant outlet/inlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm low flow FS1	1	3	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
39. System heat exchanger HTX1	HTX1	1. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
		2. blocked coolant outlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		3. blocked coolant inlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		4. no air flow	1. high-temperature stack FC1	3	1. mechanical failure 2. electrical control failure	1 1	1. alarm high temp TC4 1. alarm high temp TC4	1 1	3	
		5. reduced air flow	1. high-temperature stack FC1	2	1. mechanical failure 2. electrical control failure	1 1	1. alarm high temp TC4 1. alarm high temp TC4	1 1	2	
40. H2 storage fill port check valve CV1	CV1	1. fail close	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail partially open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
E-10	FC1-H2	1. external H2 gas leak	1. decrease in pressure at cell 2. loss of reactant 3. external H2 reaction 4. voltage decay at cell	2 3 4 2	1. internal failure at cell	1	1. alarm low cell voltage	3	12	2. Investigate detection methods for external H2 leak 5. Examine risk of continued operation during slow reactant leak
		2. cross leak H2 to coolant	1. loss of reactant 2. H2 into coolant	3 2	1. internal failure at cell	1	1. none	4	12	3. Research coolant alternatives for operation in low ambient temps 4. Investigate method to detect a H2 leak into coolant
		3. cross leak H2 to cathode	1. voltage decay at cell 2. reaction with O2	2 2	1. internal failure at cell 2. MEA degradation	1 1	1. alarm low cell voltage 1. alarm low cell voltage	1 1	2	
		4. Water-blocking anode reactant path	1. voltage decay at cell	2	1. excess condensation in cell 2. loss of hydrophobicity in cell	1 1	1. alarm low cell voltage 1. alarm low cell voltage	1 1	2	
		5. dehydrated cell— anode	1. voltage decay at cell	2	1. over effective product water removal	1	1. alarm low cell voltage	1	2	
		6. inert gas buildup— anode	1. voltage decay at cell	2	1. reactant purity	3	1. monitor cell voltage and amp-hr for purge	1	6	15. Compute at what impurity level a purge is needed for 1 hour mission
		42. Fuel cell stack cathode FC1-O2	1. external O2 gas leak	2	1. internal failure at cell	1	1. alarm low cell voltage	3	9	5. Examine risk of continued operation during slow reactant leak
		2. loss of reactant	3							
		3. external O2 reaction	1							
		4. voltage decay at cell	2							

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
E-11		2. cross leak O2 to coolant	1. loss of reactant	3	1. internal failure at cell	1	1. none	4	12	3. Research coolant alternatives for operation in low ambient temps
			2. O2 into coolant	2						16. Investigate method to detect an O2 leak into coolant
		3. cross leak O2 to anode	1. voltage decay at cell	2	1. internal failure at cell	1	1. alarm low cell voltage	1	2	
			2. reaction with H2	2	2. MEA degradation	1	1. alarm low cell voltage	1	2	
		4. water blocking cathode reactant path	1. voltage decay at cell	2	1. excess condensation in cell	1	1. alarm low cell voltage	1	2	
			2. loss of hydrophobicity in cell		1	1. alarm low cell voltage	1	2		
		5. dehydrated cell—cathode	1. voltage decay at cell	2	1. over effective product water removal	1	1. alarm low cell voltage	1	2	
		6. inert gas buildup—cathode	1. voltage decay at cell	2	1. reactant purity	3	1. monitor cell voltage and amp-hr for purge	1	6	15. Compute at what impurity level a purge is needed for 1 hour mission
43. Fuel cell stack coolant FC1-C	FC1-C	1. cross leak coolant to anode	1. decaying voltage	3	1. internal failure	1	1. alarm low cell voltage	1	3	3. Research coolant alternatives for operation in low ambient temps
			2. flood stack	3						
		2. cross leak coolant to cathode	1. decaying voltage	3	1. internal failure	1	1. alarm low cell voltage	1	3	3. Research coolant alternatives for operation in low ambient temps
			2. flood stack	3						
		3. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm high temp TC4	1	3	
44. O2 storage fill port check valve CV2	CV2	4. blocked coolant inlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
			1. high-temperature stack FC1	3						
			1. high-temperature stack FC1	3						
45. Coolant tank heater HT1	HT1	1. fail close	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail partially open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		1. fail on—continuous heat	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm high temp TC3/4	1	3	17. Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load
			1. high-temperature stack FC1							18. Include a thermal switch on V3 for redundancy
		2. fail off—no heat	1. none on normal operation	1	1. electrical control failure	1	1. none	4	4	
			2. mechanical failure		1	1. none	4	4		

APPENDIX F—MPS STARTUP WORKSHEETS

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT1	1	4	1. Discuss H2 vent location—aft of engine intake
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. check rate of pressure decay on PT1	2	6	1. Discuss H2 vent location—aft of engine intake 20. Examine risk of continued operation during slow reactant leak
		3. fail closed	1. none on startup	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT2	1	4	6. Discuss high-pressure O2 release through luggage compartment hatch
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. check rate of pressure decay on PT2	2	6	6. Discuss high-pressure O2 release through luggage compartment hatch 20. Examine risk of continued operation during slow reactant leak
		3. fail closed	1. none on startup		1. internal failure	1	1. none	4		2. Periodic RV check is only means to detect failed closed condition
3. H2 delivery relief valve RV3	RV3	1. fail closed	1. none on startup	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
		2. fail fully open	1. loss of reactant	4	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout
			2. loss of pressure	2			2. check rate of pressure decay on PT1			
		3. fail partially open	1. loss of reactant 2. reduced reactant flow 3. increased time to pressurize	3 2 2	1. internal failure	1	1. check rate of pressure decay on PT1	3	9	22. Recommend cell voltage check at full load
4. O2 delivery relief valve RV4	RV4	1. fail closed	1. none on startup	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
		2. fail fully open	1. loss of reactant	4	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout
			2. loss of pressure	2			2. check rate of pressure decay on PT2			
		3. fail partially open	1. loss of reactant 2. reduced reactant flow 3. increased time to pressurize	3 2 2	1. internal failure	1	1. check rate of pressure decay on PT2	3	9	22. Recommend cell voltage check at full load
5. H2 delivery inlet solenoid valve, NC SV1	SV1	1. fail closed	1. stack FC1 does not pressurize	4	1. internal failure 2. operator error	1 2	1. dP control prevents high dP alarm 2. dP control prevents high dP alarm	1 1	4 8	21. Discuss the requirement for a stack pressurization timeout 21. Discuss the requirement for a stack pressurization timeout

F-1

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
F-2	SV2	2. fail fully open	1. loss of dP control during pressurization	4	1. internal failure	1	1. alarm dP PT3/PT4 during pressurization	1	4	22. Recommend cell voltage check at full load	
			2. high dP on stack	2							
		3. fail partially open	1. increased time to pressurize	2	1. internal failure	1	1. none	4	8		
			2. reduced reactant flow	2	2. operator error	2	1. none	4	16		
		6. O2 delivery inlet solenoid valve, NC SV2	1. fail closed	1. stack FC1 does not pressurize	4	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout
			2. fail fully open			2	1. dP control prevents high dP alarm	1	8	21. Discuss the requirement for a stack pressurization timeout	
			1. loss of dP control during pressurization	4	1. internal failure	1	1. alarm dP PT3/PT4 during pressurization	1	4		
			2. high dP on stack	2							
	SV3	3. fail partially open	1. increased time to pressurize	2	1. internal failure	1	1. none	4	8	22. Recommend cell voltage check at full load	
			2. reduced reactant flow	2	2. operator error	2	1. none	4	16	22. Recommend cell voltage check at full load	
		7. H2 water trap drain solenoid valve, NC SV3	1. fail fully open—open drain	1. backflow of air on anode	2	1. electrical control failure	1	1. alarm PT3 out of range at startup	1	4	
			2. stack FC1 does not pressurize	4	2. internal failure	1	1. dP control prevents high dP alarm	1	4		
			2. fail partially open	1. backflow of air on anode	2	1. blockage	2	1. alarm PT3 out of range at startup	1	4	
			3. fail closed—closed drain	1. none on startup	1	1. electrical control failure	1	1. none	4	4	
	SV4	8. O2 water trap drain solenoid valve, NC SV4	1. fail fully open—open drain			2. internal failure	1	1. none	4	4	
			2. stack FC1 does not pressurize	4							
		2. fail partially open	1. backflow of air on cathode	2	1. blockage	2	1. alarm PT4 out of range at startup	1	4		
			2. stack FC1 does not pressurize	4	2. internal failure	1	1. dP control prevents high dP alarm	1	4		
	SV5	9. H2 vent solenoid valve, NC SV5	1. fail fully open—open vent	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3	1	4	
			2. loss of reactant	3	2. alarm dP PT3/PT4						
			3. high dP on stack	3	3. alarm low cell voltage						
		2. fail partially open	1. decrease in pressure	2	1. blockage	2	1. alarm PT3	1	6		

F-2

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
F-3	SV6	10. O2 vent solenoid valve, NC SV6	2. loss of reactant 3. high dP on stack	3			2. alarm dP PT3/PT4 3. alarm low cell voltage			27. Consider burp test for vent SVs at start up after pressure test	
				2			3. alarm low cell voltage				
			3. fail closed—closed vent	1	1. decaying voltage—inert buildup	1	1. none	4	8		
				2	1. electrical control failure 2. internal failure	2	1. none	4	16		
				3	1. electrical control failure 2. internal failure	1	1. none	1	4		
			1. fail fully open—open vent	4	1. electrical control failure	1	1. alarm PT4 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	4		
				3	1. electrical control failure	2	1. alarm PT4 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	8		
				3	2. internal failure	2	1. alarm PT4 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	8		
			2. fail partially open	2	1. decrease in pressure	1	1. blockage	1	6		
				3	2. loss of reactant	2	1. alarm PT4 2. alarm dP PT3/PT4 3. alarm low cell voltage	1	8		
				2	3. high dP on stack	3	1. alarm low cell voltage	1	8		
			3. fail closed—closed vent	1	1. decaying voltage—inert buildup	1	1. none	4	8		
				2	2. internal failure	1	1. none	4	8		
				3	1. electrical control failure 2. internal failure	1	1. none	1	4		
	MV1	11. H2 storage manual fill valve MV1	1. fail close	1. stack FC1 does not pressurize	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout	
						2	1. dP control prevents high dP alarm	1	8	21. Discuss the requirement for a stack pressurization timeout	
			2. fail partially open		1. internal failure	1	1. none	4	8	22. Recommend cell voltage check at full load	
					2. operator error	2	1. none	4	16	22. Recommend cell voltage check at full load	
			3. fail fully open	1. none on startup	1. internal failure	1	1. none	4	4		
	MV2	12. O2 storage manual fill valve MV2	1. fail close	1. stack FC1 does not pressurize	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout	
						2	1. dP control prevents high dP alarm	1	8	21. Discuss the requirement for a stack pressurization timeout	
			2. fail partially open		1. internal failure	1	1. none	4	8	22. Recommend cell voltage check at full load	
					2. operator error	2	1. none	4	16	22. Recommend cell voltage check at full load	
			3. fail fully open	1. none on startup	1. internal failure	1	1. none	4	4		
	FPR1	13. H2 delivery pressure regulator FPR1	1. fail closed, no outlet press	1. stack FC1 does not pressurize	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout	
			2. fail partial closed, low outlet press	1. stack FC1 does not pressurize	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout	
				1. increase in pressure	1. internal failure	1	1. alarm PT3	1	2		

F-3

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		3. fail partially open, high outlet press	2. high dP on stack	2			2. alarm dP PT3/PT4			
		4. fail fully open, high outlet press	1. loss of reactant, RV opens 2. high dP on stack	4 2	1. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	1. Discuss H2 vent location—aft of engine intake 23. Describe how to size RV3/RV4 for full high-pressure storage flow
14. O2 delivery pressure regulator FPR2	FPR2	1. fail closed, no outlet press 2. fail partial closed, low outlet press 3. fail partially open, high outlet press 4. fail fully open, high outlet press	1. stack FC1 does not pressurize 1. stack FC1 does not pressurize 1. increase in pressure 2. high dP on stack 1. loss of reactant, RV opens 2. high dP on stack	4 4 1 2 4 2	1. internal failure 1. internal failure 1. internal failure 1. internal failure	1 1 1 1	1. dP control prevents high dP alarm 1. dP control prevents high dP alarm 1. alarm PT4 2. alarm dP PT3/PT4 1. alarm PT4 2. alarm dP PT3/PT4	1 1 1 1	4 4 2 4	21. Discuss the requirement for a stack pressurization timeout 21. Discuss the requirement for a stack pressurization timeout 21. Discuss the requirement for a stack pressurization timeout 6. Discuss high-pressure O2 release through luggage compartment hatch 23. Describe how to size RV3/RV4 for full high-pressure storage flow
F-4	PT1	1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG1 1. signal out of range 2. check PG1	1	1	
		2. fail low—low electrical output	1. loss of leak detection		1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG1 1. signal out of range 2. check PG1	1	1	
		3. drift high or low	1. loss of leak detection	1	1. internal failure	1	1. check PG1 2. amp-hr check on reactant consumption vs pressure	3	3	3. Check accuracy of PGs at 200 hr maintenance interval
		1. fail high—high electrical output	1. loss of leak detection		1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG2 1. signal out of range 2. check PG2			
		2. fail low—low electrical output	1. loss of leak detection	1	1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG2 1. signal out of range 2. check PG2	1	1	
		3. drift high or low	1. loss of leak detection		1. internal failure	1	1. check PG2 2. amp-hr check on reactant consumption vs pressure	3	3	3. Check accuracy of PGs at 200 hr maintenance interval
		1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG2 1. signal out of range 2. check PG2			
		2. fail low—low electrical output	1. loss of leak detection		1. electrical control failure 2. internal failure	1	1. signal out of range 2. check PG2 1. signal out of range 2. check PG2			
		3. drift high or low	1. loss of leak detection		1. internal failure	1	1. check PG2 2. amp-hr check on reactant consumption vs pressure			

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
F-5	PT3	1. fail high—high electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm high pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		2. fail low—low electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm low pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		3. drift high or low	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm pressure	4						
	PT4	1. fail high—high electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm high pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		2. fail low—low electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm low pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		3. drift high or low	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm pressure	4						
F-6	T1	1. fail high—high electrical output	1. low-temperature stack FC1	4	1. internal failure	1	1. check T4 for redundant alarm	1	4	19. Develop a backup thermal control scheme using T4.
			2. false alarm high temperature	1	2. electrical control failure	1	2. check FS1 for flow	1	4	
		2. fail low—low electrical output	1. high-temperature stack FC1	4	1. internal failure	1	1. check T4 for redundant alarm	1	4	19. Develop a backup thermal control scheme using T4.
			2. electrical control failure	1	2. check FS1 for flow	1	2. check FS1 for flow	1	4	
		3. drift high or low	1. false alarm high temperature	1	1. internal failure	1	1. T4 redundant	1	1	19. Develop a backup thermal control scheme using T4.

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
			2. false delta T alarm	1			2. check FS1			
20. Coolant outlet temperature transmitter T2	T2	1. fail high—high electrical output	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
					2. electrical control failure	1	1. check FS1 for flow	1	1	
		2. fail low—low electrical output	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
					2. electrical control failure	1	1. check FS1 for flow	1	1	
		3. drift high or low	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
21. H2 water trap level switch LS1	LS1	1. fail set—SV3 remains open after amp-hr count	1. loss of pressure	4	1. internal failure	1	1. amp-hr count for water accumulation is longer than startup time	1	4	10. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
			2. loss of reactant	3						
			3. high dP on stack	3						
		2. fail open -SV3 remains closed	1. none on startup	1	1. internal failure	1	1. amp-hr count for water accumulation is longer than startup time	1	1	10. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
22. O2 water trap level switch LS2	LS2	1. fail set—SV4 remains open after amp-hr count	1. loss of pressure	4	1. internal failure	1	1. amp-hr count for water accumulation is longer than startup time	1	4	10. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
			2. loss of reactant	3						
			3. high dP on stack	3						
		2. fail open -SV4 remains closed	1. none on startup	3	1. internal failure	1	1. amp-hr count for water accumulation is longer than startup time	1	3	10. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
23. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none on startup	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	16. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp. 29. Include a visual level indicator
		2. fail open—electrically open empty	1. false low level indication	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	16. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp. 29. Include a visual level indicator
				1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	
24. Coolant flow switch FS1	FS1	1. failed closed—indicates flow	1. none on startup	1	1. internal failure	1	1. none	4	4	
		2. failed open—indicates no flow	1. false alarm no flow	1	1. internal failure	1	1. none	4	4	30. Explain FS1 as an alarm indicator not a shutdown control.
25. H2 recirculation pump M1	M1	1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	4	17. Consider second PT at outlet for redundancy
			2. flood stack	3	2. internal failure	1	1. alarm low cell voltage	1	4	18. Include a monitor for current draw on reactant recirculation pump
			3. poor reactant mass transport	3						

F-6

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations	
F-7			4. voltage decay at cell	4							
			2. external gas leak	1. external H ₂ reaction	4	1. mechanical failure	1	1. none	4	16	
			2. loss of reactant		3					9. Investigate detection methods and location for external H ₂ leak	
			3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. flood stack	2						13. Examine risk of continued operation during slow reactant leak.	
			3. poor reactant mass transport	2							
			26. O ₂ recirculation pump M2	1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	4
				2. flood stack	3	2. internal failure	1	1. alarm low cell voltage	1	4	
				3. poor reactant mass transport	3					18. Include a monitor for current draw on reactant recirculation pump	
				4. voltage decay at cell	4						
			2. external gas leak	1. external O ₂ reaction	1	1. mechanical failure	1	1. none	4	12	
				2. loss of reactant	3					13. Examine risk of continued operation during slow reactant leak.	
			3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure	1	1. alarm low cell voltage	1	2	
				2. flood stack	2						
				3. poor reactant mass transport	2						
			27. Coolant circulation pump M3	1. pumping stops	1. low-temperature stack FC1	4	1. electrical control failure	1	1. alarm low flow FS1	1	4
				2. internal failure		1	1. alarm low flow FS1	1	4		
			2. pumping reduced	1. high delta temperature FC1		1. blockage partial		1. alarm high temp TC4			
							1	2. alarm high delta temp TC4/TC3	1	2	
						2. electrical control failure	1	1. alarm high temp TC4	1	2	
							1	2. alarm high delta temp TC4/TC3			
						3. internal failure	1	1. alarm high temp TC4			
							1	2. alarm high delta temp TC4/TC3	1	2	
			3. external coolant leak	1. none on startup	1	1. mechanical failure	1	1. alarm low level LS3	1	1	
28. H ₂ water trap WT1	WT1	1. external gas leak	1. backflow of air	2	1. internal failure at cell	1	1. alarm PT3 out of range at startup	1	2	26. Explain that vacuum condition should be maintained until startup	
29. O ₂ water trap WT2	WT2	1. external gas leak	1. backflow of air	2	1. internal failure at cell	1	1. alarm PT4 out of range at startup	1	2	26. Explain that vacuum condition should be maintained until startup	
30. H ₂ Leak Detector A1	A1	1. fails off—no signal	1. reaction with H ₂	4	1. internal failure	1	1. interlocked with FC system	1	4		

F-7

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
31. H2 delivery manual isolation valve MV3	MV3	2. fails out of calibration—low 3. fails out of calibration—high	1. reaction with H2 1. false alarm high ambient H2	3 2 2	2. electrical control failure	1	1. interlocked with FC system	1	4	
					1. internal failure	2	1. none	4	24	32. H2 leak detector calibration must be constantly checked. 33. Consider redundant H2 leak detector
					1. internal failure	2	1. interlocked with FC system	1	4	
31. H2 delivery manual isolation valve MV3 32. O2 delivery manual isolation valve MV4	MV3 MV4	1. fail closed 2. fail fully open	1. stack FC1 does not pressurize	4	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout
					2. operator error	2	1. dP control prevents high dP alarm	1	8	21. Discuss the requirement for a stack pressurization timeout
		3. fail partially open	1. increased time to pressurize 2. reduced reactant flow	2 2	1. internal failure	1	1. none	4	8	22. Recommend cell voltage check at full load
					2. operator error	2	1. none	4	16	22. Recommend cell voltage check at full load
		1. fail closed 2. fail fully open	1. stack FC1 does not pressurize	4	1. internal failure	1	1. dP control prevents high dP alarm	1	4	21. Discuss the requirement for a stack pressurization timeout
					2. operator error	2	1. dP control prevents high dP alarm	1	8	21. Discuss the requirement for a stack pressurization timeout
33. H2 storage tank V1 34. O2 storage tank V2	V1 V2	1. external gas leak	1. loss of reactant 2. external H2 reaction	3 4	1. mechanical failure	1	1. check rate of pressure decay on PT1	1	4	7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump.
							2. check rate of pressure decay on PG1			
		2. tank rupture	1. loss of reactant 2. external H2 reaction	4 4	1. mechanical failure	1	1. check rate of pressure decay on PT1	1	4	4. Appropriate procedures for handling high-pressure reactant tanks must be in place
							2. check rate of pressure decay on PG1			7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump.
		1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. check rate of pressure decay on PT2	1	3	8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump.
		2. tank rupture	1. loss of reactant	4	1. mechanical failure	1	2. check rate of pressure decay on PG2			
							1. check rate of pressure decay on PT2	1	4	4. Appropriate procedures for handling high-pressure reactant tanks must be in place

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
							2. check rate of pressure decay on PG2			8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump.
35. Coolant reservoir V3	V3	1. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
			2. damage to HT1	1						
			3. flood system	1						
		2. blocked coolant outlet/inlet	1. low-temperature stack FC1	4	1. internal failure	1	1. alarm low flow FS1	1	4	
36. Product water tank	V4	1. external leak	1. flood system	2	1. mechanical failure	1	1. none	4	8	11. Discuss methods to detect/contain overflow
		2. blocked inlet	1. overflow of WT1	2	1. mechanical failure	1	1. none	4	12	12. Discuss combining separation and water storage functions to simplify product water management
			2. overflow of WT2	3						
37. System heat exchanger HTX1	HTX1	1. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
		2. blocked coolant outlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		3. blocked coolant inlet	1. high-temperature stack FC1	2	1. internal failure	1	1. alarm low flow FS1	1	2	
		4. no air flow	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm high temp TC4	1	3	31. Consider manual override to check fan operation
					2. electrical control failure	1	1. alarm high temp TC4	1	3	
38. Fuel cell stack anode FC1-H2	FC1-H2	1. external gas leak	1. backflow of air	2	1. internal failure at cell	1	1. alarm PT3 out of range at startup	1	2	26. Explain that vacuum condition should be maintained until startup
		2. cross leak H2 to coolant	1. loss of reactant	3	1. internal failure at cell	1	1. none	4	12	24. Investigate method to detect a H2 leak into coolant
			2. H2 into coolant	2						
39. Fuel cell stack cathode FC1-O2	FC1-O2	3. cross leak H2 to cathode	1. voltage decay at cell	2	1. internal failure at cell	1	1. alarm low cell voltage	1	2	
			2. reaction with O2	2						
		1. external gas leak	1. backflow of air	1	1. internal failure	1	1. alarm PT4 out of range at startup	1	1	26. Explain that vacuum condition should be maintained until startup
40. Fuel cell stack coolant FC1-C	FC1-C	2. cross leak O2 to coolant	1. loss of reactant	3	1. internal failure at cell	1	1. none	4	12	25. Investigate method to detect an O2 leak into coolant
			2. O2 into coolant	2						
		3. cross leak O2 to anode	1. voltage decay at cell	2	1. internal failure at cell	1	1. alarm low cell voltage	1	2	
			2. reaction with H2	2						

F-9

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
41. Coolant tank heater HT1	HT1	2. cross leak coolant to cathode	1. decaying voltage	3	1. internal failure	1	1. alarm low cell voltage	1	3	14. Describe how heater should be sized for system heat loss and minimum current density and how to size HTX1 for additional HT1 heat load 15. Consider a thermal switch on V3 for redundancy	
			2. flood stack	3							
		3. external coolant leak	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3		
		4. blocked coolant inlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3		
		5. blocked coolant outlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3		
42. H2 storage pressure gauge PG1	PG1	1. fail on—continuous heat	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm high delta temp TC4/TC3	1	3	14. Describe how heater should be sized for system heat loss and minimum current density and how to size HTX1 for additional HT1 heat load 15. Consider a thermal switch on V3 for redundancy	
		2. fail off—no heat	1. low-temperature stack FC1	1	1. electrical control failure	1	1. none	4	4		
			2. no load for FC startup	1	2. mechanical failure	1	1. none	4	4		
43. O2 storage pressure gauge PG2	PG2	1. fail out of range—high or low	1. none on startup	1	1. internal failure	1	1. reading out of range 2. check PT1	1	1	3. Check accuracy of PGs at 200 hr maintenance interval	
		2. out of calibration—low	1. none on startup	1	1. internal failure	1	1. reading out of range 2. check PT1	1	1		
		3. out of calibration—high	1. none on startup	1	1. internal failure	1	1. reading out of range 2. check PT1	1	1		

F-10

APPENDIX G—MPS POWER-PRODUCTION WORKSHEETS

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT1	1	4	1. Discuss H2 vent location—aft of engine intake
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. check rate of pressure decay on PT1	2	6	1. Discuss H2 vent location—aft of engine intake 28. Examine risk of continued operation during slow reactant leak
		3. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT2	1	4	6. Discuss high-pressure O2 release through luggage compartment hatch
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. check rate of pressure decay on PT2	2	6	6. Discuss high-pressure O2 release through luggage compartment hatch 28. Examine risk of continued operation during slow reactant leak
		3. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
3. H2 delivery relief valve RV3	RV3	1. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant 2. high dP on stack	4	1. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4 3. amp-hr check on reactant consumption vs pressure	1	4	
		3. fail partially open	1. decrease in pressure 2. loss of reactant 3. high dP on stack	2			1. alarm PT3 2. alarm dP PT3/PT4 3. amp-hr check on reactant consumption vs pressure			
4. O2 delivery relief valve RV4	RV4	1. fail closed	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. loss of reactant 2. high dP on stack	4	1. internal failure	1	1. alarm PT4 2. alarm dP PT3/PT4 3. amp-hr check on reactant consumption vs pressure	1	4	
		3. fail partially open	1. decrease in pressure 2. loss of reactant	2			1. alarm PT4 2. alarm dP PT3/PT4			

G-1

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
			3. high dP on stack	2			3. amp-hr check on reactant consumption vs pressure			
5. H2 delivery inlet solenoid valve, NC SV1	SV1	1. fail closed	1. loss of pressure	4	1. electrical control failure 2. high dP on stack	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	
			2. high dP on stack	4		1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	
		2. fail fully open	1. none on normal operation	1	1. electrical control failure	1	1. none	4	4	
			2. internal failure	1	2. internal failure	1	1. none	4	4	
		3. fail partially open	1. decrease in pressure	2	1. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	2	
			2. high dP on stack	2						
		1. fail closed	1. loss of pressure	4	1. electrical control failure 2. high dP on stack	1	1. alarm PT4 2. alarm dP PT3/PT4	1	4	
			2. high dP on stack	4		1	1. alarm PT4 2. alarm dP PT3/PT4	1	4	
			2. fail fully open	1	1. electrical control failure	1	1. none	4	4	
			2. internal failure	1	2. internal failure	1	1. none	4	4	
		3. fail partially open	1. decrease in pressure	2	1. internal failure	1	1. alarm PT4 2. alarm dP PT3/PT4	1	2	
			2. high dP on stack	2						
7. H2 water trap drain solenoid valve, NC SV3	SV3	1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	25. Consider sizing orifice restriction to allow low-pressure operation
			2. loss of reactant	3			3. alarm low cell voltage			
			3. high dP on stack	3			1. alarm PT3 2. alarm dP PT3/PT4	1	4	
		2. fail partially open	1. decrease in pressure	2	2. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	
			2. loss of reactant	3			3. alarm low cell voltage			
			3. high dP on stack	2			1. alarm PT3 2. alarm dP PT3/PT4	1	6	25. Consider sizing orifice restriction to allow low-pressure operation
		3. fail closed—closed drain	1. overflow of WT1	3	1. blockage	2	1. alarm PT3 2. alarm dP PT3/PT4	1	3	
			2. internal failure	1			3. alarm low cell voltage			
			1. electrical control failure	1	1. amp-hr check on water accumulation			1	3	
8. O2 water trap drain solenoid valve, NC SV4	SV4	1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT4 2. alarm dP PT3/PT4	1	4	25. Consider sizing orifice restriction to allow low-pressure operation
			2. loss of reactant	3			3. alarm low cell voltage			
			3. high dP on stack	3			1. alarm PT3 2. alarm dP PT3/PT4	1	4	
		2. internal failure	1. internal failure	1	1. alarm low cell voltage					
			2. internal failure	1	2. internal failure	1	1. alarm PT3 2. alarm dP PT3/PT4	1	4	

G-2

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
C-3	SV5	2. fail partially open	1. decrease in pressure	2	1. blockage	2	1. alarm PT4	1	6	25. Consider sizing orifice restriction to allow low-pressure operation
			2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. high dP on stack	2			3. alarm low cell voltage			
		3. fail closed—closed drain	1. overflow of WT2	3	1. electrical control failure	1	1. amp-hr check on water accumulation	1	3	
			2. internal failure			1	1. amp-hr check on water accumulation	1	3	
		1. fail fully open—open vent	1. loss of pressure	4	1. electrical control failure	1	1. alarm PT3	1	4	
			2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. high dP on stack	3			3. alarm low cell voltage			
			1. decrease in pressure	2	1. blockage	2	1. alarm PT3	1	8	25. Consider sizing orifice restriction to allow low-pressure operation
			2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. high dP on stack	2			3. alarm low cell voltage			
		3. fail closed—closed vent	1. decaying voltage—inert buildup	2	1. electrical control failure	1	1. alarm low cell voltage	1	2	
			2. internal failure			2	1. alarm low cell voltage	1	4	
			1. loss of pressure	4	1. electrical control failure	1	1. alarm PT4	1	4	
		1. fail fully open—open vent	2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. high dP on stack	3			3. alarm low cell voltage			
		2. fail partially open	1. decrease in pressure	2	2. internal failure	2	1. alarm PT4	1	8	25. Consider sizing orifice restriction to allow low-pressure operation
			2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. high dP on stack	2			3. alarm low cell voltage			
		3. fail closed—closed vent	1. decaying voltage—inert buildup	2	1. electrical control failure	1	1. alarm low cell voltage	1	2	
			2. internal failure			1	1. alarm low cell voltage	1	2	
			1. loss of pressure	4	1. internal failure	1	1. alarm PT3	1	4	
		1. fail close	2. high dP on stack	4			2. alarm dP PT3/PT4			
			1. reduced reactant flow	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			1. none on normal operation	1		1	1. none	4	4	
		1. fail close	1. loss of pressure	4	1. internal failure	1	1. alarm PT4	1	4	
			2. high dP on stack	4			2. alarm dP PT3/PT4			
		2. fail partially open	1. reduced reactant flow	2	1. internal failure	1	1. alarm low cell voltage	1	2	

C-3

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		3. fail fully open	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
13. H2 delivery pressure regulator FPR1	FPR1	1. fail closed, no outlet press	1. loss of pressure	4	1. internal failure	1	1. alarm PT3	1	4	
			2. high dP on stack	4			2. alarm dP PT3/PT4			
		2. fail partial closed, low outlet press	1. decrease in pressure	2	1. internal failure	1	1. alarm PT3	1	2	
			2. high dP on stack	2			2. alarm dP PT3/PT4			
		3. fail partially open, high outlet press	1. increase in pressure	1	1. internal failure	1	1. alarm PT3	1	2	
			2. high dP on stack	2			2. alarm dP PT3/PT4			
		4. fail fully open, high outlet press	1. loss of reactant, RV opens	4	1. internal failure	1	1. alarm PT3	1	4	1. Discuss H2 vent location—aft of engine intake
			2. high dP on stack	2			2. alarm dP PT3/PT4			29. Describe how to size RV3/RV4 for full high-pressure storage flow
14. O2 delivery pressure regulator FPR2	FPR2	1. fail closed, no outlet press	1. loss of pressure	4	1. internal failure	1	1. alarm PT4	1	4	
			2. high dP on stack	4			2. alarm dP PT3/PT4			
		2. fail partial closed, low outlet press	1. decrease in pressure	2	1. internal failure	1	1. alarm PT4	1	2	
			2. high dP on stack	2			2. alarm dP PT3/PT4			
		3. fail partially open, high outlet press	1. increase in pressure	1	1. internal failure	1	1. alarm PT4	1	2	
			2. high dP on stack	2			2. alarm dP PT3/PT4			
		4. fail fully open, high outlet press	1. loss of reactant, RV opens	4	1. internal failure	1	1. alarm PT4	1	4	6. Discuss high-pressure O2 release through luggage compartment hatch
			2. high dP on stack	2			2. alarm dP PT3/PT4			29. Describe how to size RV3/RV4 for full high-pressure storage flow
15. H2 storage pressure transmitter PT1	PT1	1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range	1	1	
					2. internal failure		2. check PG1			
		2. fail low—low electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range	1	1	
					2. internal failure		2. check PG1			
		3. drift high or low	1. loss of leak detection	1	1. internal failure	1	1. signal out of range	1	1	
					2. check PG1		2. amp-hr check on reactant consumption vs pressure			3. Check accuracy of PGs at 200 hr maintenance interval
16. O2 storage pressure transmitter PT2	PT2	1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range	1	1	
					2. internal failure		2. check PG2			
		2. fail low—low electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range	1	1	
							2. check PG2			

C-4

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
					2. internal failure	1	1. signal out of range 2. check PG2	1	1	
		3. drift high or low	1. loss of leak detection	1	1. internal failure	1	1. check PG2 2. amp-hr check on reactant consumption vs pressure	3	3	3. Check accuracy of PGs at 200 hr maintenance interval
17. H2 stack pressure transmitter PT3	PT3	1. fail high—high electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm high pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		2. fail low—low electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm low pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		3. drift high or low	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm pressure	4						
18. O2 stack pressure transmitter PT4	PT4	1. fail high—high electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm high pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		2. fail low—low electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm low pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
		3. drift high or low	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet
			2. false alarm pressure	4						
19. Coolant inlet temperature transmitter T1	T1	1. fail high—high electrical output	1. false alarm high temperature	1	1. internal failure	1	1. check T4 for redundant alarm 2. check FS1 for flow	1	1	26. Develop a backup thermal control scheme using T4.
			2. electrical control failure	1	2. electrical control failure	1	1. check T4 for redundant alarm 2. check FS1 for flow	1	1	
		2. fail low—low electrical output	1. high-temperature stack FC1	3	1. internal failure	1	1. check T4 for redundant alarm	1	3	26. Develop a backup thermal control scheme using T4.

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
					2. electrical control failure	1	1. check T4 for redundant alarm 2. check FS1 for flow	1	3	
		3. drift high or low	1. false alarm high temperature 2. false delta T alarm	1	1. internal failure	1	1. T4 redundant 2. check FS1	1	1	26. Develop a backup thermal control scheme using T4.
20. Coolant outlet temperature transmitter T2	T2	1. fail high—high electrical output	1. false delta T alarm	1	1. internal failure 2. electrical control failure	1	1. check FS1 for flow 1. check FS1 for flow	1	1	
		2. fail low—low electrical output	1. false delta T alarm	1	1. internal failure 2. electrical control failure	1	1. check FS1 for flow 1. check FS1 for flow	1	1	
		3. drift high or low	1. false delta T alarm	1	1. internal failure	1	1. check FS1 for flow	1	1	
21. H2 water trap level switch LS1	LS1	1. fail set—SV3 remains open after amp-hr count	1. loss of pressure 2. loss of reactant 3. high dP on stack 4. external H2 reaction	4 3 3 4	1. electrical control failure 2. internal failure	1 2	1. alarm PT3 1. alarm PT3	1 1	4 8	14. Describe control to limit reactant loss based on amp hr count and its use as a secondary control/alarm secondary control
		2. fail open -SV3 remains closed	1. overflow of WT1	3	1. electrical control failure 2. internal failure	1 2	1. amp-hr check on water accumulation 1. amp-hr check on water accumulation	1 1	3 6	13. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
22. O2 water trap level switch LS2	LS2	1. fail set—SV4 remains open after amp-hr count	1. loss of pressure 2. loss of reactant 3. high dP on stack	4 3 3	1. electrical control failure 2. internal failure	1 2	1. alarm PT4 1. alarm PT4	1 1	4 8	14. Describe control to limit reactant loss based on amp hr count and its use as a secondary control/alarm secondary control
		2. fail open -SV4 remains closed	1. overflow of WT1	3	1. electrical control failure 2. internal failure	1 2	1. amp-hr check on water accumulation 1. amp-hr check on water accumulation	1 1	3 6	13. Describe control to limit product water accumulation based on amp hr count and its use as a secondary control/alarm
23. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none on normal operation	1	1. electrical control failure 2. internal failure	1 2	1. none 1. none	4 4	4 8	21. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.
				1	1. electrical control failure	1	1. none	4	4	

C-6

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
		2. fail open—electrically open empty	1. false low level indication		2. internal failure	2	1. none	4	8	21. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp.
24. Coolant flow switch FS1	FS1	1. failed closed—indicates flow	1. none on normal operation	1	1. internal failure	1	1. none	4	4	
		2. failed open—indicates no flow	1. false alarm no flow	1	1. internal failure	1	1. alarm high delta temp TC4/TC3	1	1	
25. H2 recirculation pump M1	M1	1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	3	23. Consider second PT to indicate adequate flow as indicated by pressure drop
			2. flood stack	3	2. internal failure		1. alarm low cell voltage	1	3	24. Include a monitor for current draw on reactant recirculation pump
			3. poor reactant mass transport	3						
			4. voltage decay at cell	2						
		2. external gas leak	1. external H2 reaction	4	1. mechanical failure	1	1. none	4	16	9. Investigate detection methods and location for external H2 leak
			2. loss of reactant	3						17. Examine risk of continued operation during slow reactant leak.
		3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure		1. alarm low cell voltage	1	2	
			2. flood stack	2						
			3. poor reactant mass transport	2						
		4. mechanical degradation	1. stack contamination	2	1. internal failure	1	1. alarm low cell voltage	1	2	
			2. cell flow channel restriction	2	2. internal failure	1	1. none	4	8	22. Consider adding filter downstream of reactant pump
26. O2 recirculation pump M2	M2	1. stop pumping—no recirculation	1. localized dehydration of FC1	2	1. electrical control failure	1	1. alarm low cell voltage	1	3	23. Consider second PT to indicate adequate flow as indicated by pressure drop
			2. flood stack	3	2. internal failure		1. alarm low cell voltage	1	3	24. Include a monitor for current draw on reactant recirculation pump
			3. poor reactant mass transport	3						
			4. voltage decay at cell	2						
		2. external gas leak	1. external O2 reaction	1	1. mechanical failure	1	1. none	4	12	17. Examine risk of continued operation during slow reactant leak.
			2. loss of reactant	3						
		3. internal leak—reduced flow	1. localized dehydration of FC1	2	1. internal failure		1. alarm low cell voltage	1	2	
			2. flood stack	2						
			3. poor reactant mass transport	2						
		1. stack contamination	2	1. internal failure	1	1. alarm low cell voltage	1	2		

G-7

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		4. mechanical degradation	2. cell flow channel restriction	2	2. internal failure	1	1. none	4	8	22. Consider adding filter downstream of reactant pump
27. Coolant circulation pump M3	M3	1. pumping stops	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm low flow FS1	1	3	
					2. internal failure	1	1. alarm low flow FS1	1	3	
		2. pumping reduced	1. high-temperature stack FC1	2	1. blockage partial	1	1. alarm high temp TC4	1	2	
							2. alarm high delta temp TC4/TC3			
							1. alarm high temp TC4	1	2	
			2. high delta temperature FC1	2			2. alarm high delta temp TC4/TC3			
				2. electrical control failure	1	1. alarm high temp TC4	1	2		
						2. alarm high delta temp TC4/TC3				
					3. internal failure	1. alarm high temp TC4	1	2		
						2. alarm high delta temp TC4/TC3				
		3. external coolant leak	1. high-temperature stack FC1	3	1. mechanical failure	1	1. alarm low level LS3	1	3	
28. H2 water trap WT1	WT1	1. external gas leak	1. high dP on stack	2	1. mechanical failure	1	1. alarm PT3	1	3	17. Examine risk of continued operation during slow reactant leak.
			2. loss of reactant	3			2. alarm dP PT3/PT4			9. Investigate detection methods and location for external H2 leak
			3. decrease in pressure	2			3. alarm low cell voltage			
		2. external water leak without gas	1. none on normal operation	1	1. internal failure	1	1. none	4	4	27. Compute total product water available for worst case flooding risk
			1. flood pump M1	2	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
		3. overflow—water in gas circuit	2. flood stack	3			1. amp-hr check on water accumulation	1	2	
			1. product water out vent	1	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
			2. less effective purge	2			1. amp-hr check on water accumulation			
		4. overflow anode vent	3. no purge	2			1. amp-hr check on water accumulation			
29. O2 water trap WT2	WT2	1. external gas leak	1. high dP on stack	2	1. mechanical failure	1	1. alarm PT3	1	3	
			2. loss of reactant	3			2. alarm dP PT3/PT4			
			3. decrease in pressure	2			3. alarm low cell voltage			
		2. external water leak without gas	1. none on normal operation	1	1. internal failure	1	1. none	4	4	27. Compute total product water available for worst case flooding risk
			1. flood pump M1	2	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
		3. overflow—water in gas circuit	2. flood stack	3			1. amp-hr check on water accumulation	1	2	
			1. product water out vent	1	1. blocked drain	1	1. amp-hr check on water accumulation	1	3	
			2. less effective purge	2			1. amp-hr check on water accumulation			
			3. no purge	2			1. amp-hr check on water accumulation			
30. H2 Leak Detector A1	A1	1. fails off—no signal	1. reaction with H2	4	1. internal failure	1	1. interlocked with FC system	1	4	

C-8

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
30. H2 leak detector calibration must be constantly checked. 31. Consider redundant H2 leak detector				2. electrical control failure 1. reaction with H2 1. internal failure	1	1. interlocked with FC system	1	4		
					2	1. none	4	24		
					2	1. interlocked with FC system	1	4		
31. O2 delivery manual isolation valve MV4	MV4	1. fail close 2. fail partially open 3. fail fully open	1. loss of pressure 2. high dP on stack 1. reduced reactant flow 1. none on normal operation	4 4 2 1	1. internal failure 1. internal failure 1. internal failure	1 1 1	1. alarm PT4 2. alarm dP PT3/PT4 1. alarm low cell voltage 1. none	1 2 4		
32. H2 delivery manual isolation valve MV3	MV3	1. fail close 2. fail partially open 3. fail fully open	1. loss of pressure 2. high dP on stack 1. reduced reactant flow 1. none on normal operation	4 4 2 1	1. internal failure 1. internal failure 1. internal failure	1 1 1	1. alarm PT3 2. alarm dP PT3/PT4 1. alarm low cell voltage 1. none	1 2 4		
33. H2 storage tank V1	V1	1. external gas leak 2. tank rupture	1. loss of reactant 2. external H2 reaction 1. loss of reactant 2. external H2 reaction	3 4 4 4	1. mechanical failure 1. mechanical failure	1 1	1. amp-hr check on reactant consumption vs pressure 1. check rate of pressure decay on PT1	1 1	4 4	7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump. 4. Appropriate procedures for handling high-pressure reactant tanks must be in place 7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump.
34. O2 storage tank V2	V2	1. external gas leak 2. tank rupture	1. loss of reactant 1. loss of reactant	3 4	1. mechanical failure 1. mechanical failure	1 1	1. amp-hr check on reactant consumption vs pressure 1. check rate of pressure decay on PT2	1 1	3 4	8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump. 4. Appropriate procedures for handling high-pressure reactant tanks must be in place 8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump.
35. Coolant reservoir V3	V3	1. external coolant leak 2. blocked coolant outlet/inlet	1. high-temperature stack FC1 2. damage to HT1 3. flood system 1. high-temperature stack FC1	3 1 1 3	1. mechanical failure 1. internal failure	1 1	1. alarm low level LS3 1. alarm low flow FS1	1 1	3 3	
36. Product water tank	V4	1. external leak	1. flood system	2	1. mechanical failure	1	1. none	4	8	15. Discuss methods to detect and/or contain overflow

C-9

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		2. blocked inlet	1. overflow of WT1 2. overflow of WT2	2 3	1. mechanical failure	1	1. none	4	12	16. Discuss combining separation and water storage functions to simplify product water management
37. System heat exchanger HTX1	HTX1	1. external coolant leak 2. blocked coolant outlet 3. blocked coolant inlet 4. no air flow 5. reduced air flow	1. high-temperature stack FC1 1. high-temperature stack FC1 1. high-temperature stack FC1 1. high-temperature stack FC1 1. high-temperature stack FC1	3 2 2 3 2	1. mechanical failure 1. internal failure 1. internal failure 1. mechanical failure 1. mechanical failure	1 1 1 1 1	1. alarm low level LS3 1. alarm low flow FS1 1. alarm low flow FS1 1. alarm high temp TC4 1. alarm high temp TC4	1 1 1 1 1	3 2 2 3 2	
G-10	FC1-H2	1. external H2 gas leak 2. cross leak H2 to coolant 3. cross leak H2 to cathode 4. water blocking anode reactant path 5. dehydrated cell— anode 6. inert gas buildup— anode	1. decrease in pressure at cell 2. loss of reactant 3. external H2 reaction 4. voltage decay at cell 1. loss of reactant 2. H2 into coolant 1. voltage decay at cell 2. reaction with O2 1. voltage decay at cell 2. loss of hydrophobicity in cell 1. voltage decay at cell 2. over effective product water removal 1. reactant purity	2 3 4 2 3 2 2 2 2 2 2	1. internal failure at cell 1. internal failure at cell 1. internal failure at cell 1. excess condensation in cell 1. internal failure at cell	1 1 1 1 1 1 1 1 1 1 1	1. alarm low cell voltage 1. none 1. alarm low cell voltage 1. alarm low cell voltage 1. none 1. alarm low cell voltage 1. alarm low cell voltage 1. alarm low cell voltage 1. monitor cell voltage and amp-hr for purge	3 4 1 1 4 1 1 1 1	12 12 2 2 12 2 2 2 6	9. Investigate detection methods and location for external H2 leak 10. Examine risk of continued operation during slow reactant leak. Look at H2 concentration time response. 11. Investigate method to detect an H2 leak into coolant 12. Compute purge frequency and quantity versus reactant impurity level.
		1. external O2 gas leak	1. decrease in pressure at cell 2. loss of reactant 3. external O2 reaction 4. voltage decay at cell	2 3 1 2	1. internal failure at cell	1	1. alarm low cell voltage	3	9	17. Examine risk of continued operation during slow reactant leak.
		2. cross leak O2 to coolant	1. loss of reactant 2. O2 into coolant	3 2	1. internal failure at cell	1	1. none	4	12	18. Investigate method to detect an O2 leak into coolant
		3. cross leak O2 to anode	1. voltage decay at cell 2. reaction with H2	2 2	1. internal failure at cell 2. MEA degradation	1 1	1. alarm low cell voltage 1. alarm low cell voltage	1 1	2 2	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		4. water blocking cathode reactant path	1. voltage decay at cell	2	1. excess condensation in cell 2. loss of hydrophobicity in cell	1 1	1. alarm low cell voltage 1. alarm low cell voltage	1 1	2 2	
		5. dehydrated cell—cathode	1. voltage decay at cell	2	1. over effective product water removal	1	1. alarm low cell voltage	1	2	
		6. inert gas buildup—cathode	1. voltage decay at cell	2	1. reactant purity	3	1. monitor cell voltage and amp-hr for purge			
40. Fuel cell stack coolant FC1-C	FC1-C	1. cross leak coolant to anode	1. decaying voltage 2. flood stack	3 3	1. internal failure	1	1. alarm low cell voltage	1	3	
		2. cross leak coolant to cathode	1. decaying voltage 2. flood stack	3 3	1. internal failure	1	1. alarm low cell voltage	1	3	
		3. external coolant leak	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
		4. blocked coolant inlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
		5. blocked coolant outlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
41. Coolant tank heater HT1	HT1	1. fail on—continuous heat	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm high delta temp TC4/TC3	1	3	19. Describe how heater should be sized for system heat loss and how to size HTX1 for additional HT1 heat load
		2. fail off—no heat	1. none on normal operation	1	1. electrical control failure 2. mechanical failure	1 1	1. none 1. none	4 4	4 4	20. Consider a thermal switch on V3 for redundancy
42. H2 storage pressure gauge PG1	PG1	1. fail out of range—high or low	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		2. out of calibration—low	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		3. out of calibration—high	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
43. O2 storage pressure gauge PG2	PG2	1. fail out of range—high or low	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		2. out of calibration—low	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		3. out of calibration—high	1. none on normal operation	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval

G-11

APPENDIX H—MPS SHUTDOWN WORKSHEETS

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
1. H2 storage tank relief valve RV1	RV1	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT1	1	4	1. Discuss H2 vent location—aft of engine intake
		2. fail partially open	1. loss of reactant	3	1. internal failure	1	1. check rate of pressure decay on PT1	2	6	1. Discuss H2 vent location—aft of engine intake
		3. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
2. O2 storage tank relief valve RV2	RV2	1. fail fully open	1. loss of reactant	4	1. internal failure	1	1. check rate of pressure decay on PT2	1	4	
		2. fail partially open	1. loss of reactant	2	1. internal failure	1	1. check rate of pressure decay on PT2	2	4	
		3. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4	2. Periodic RV check is only means to detect failed closed condition
3. H2 delivery relief valve RV3	RV3	1. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
		3. fail partially open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
4. O2 delivery relief valve RV4	RV4	1. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		2. fail fully open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
		3. fail partially open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
5. H2 delivery inlet solenoid valve, NC SV1	SV1	1. fail closed	1. no shutdown	4	1. electrical control failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
		2. fail fully open	1. no shutdown	4	1. electrical control failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
		3. fail partially open	1. no shutdown	4	1. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
6. O2 delivery inlet solenoid valve, NC SV2	SV2	1. fail closed	1. none on shutdown	1	1. electrical control failure	1	1. alarm dP PT3/PT4	1	1	
					2. internal failure	1	1. alarm dP PT3/PT4	1	1	
		2. fail fully open	1. no shutdown	4	1. electrical control failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
		3. fail partially open	1. none on shutdown	1	1. internal failure	1	1. alarm dP PT3/PT4	1	1	
	SV3	1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm dP PT3/PT4	1	4	
			2. high dP on stack	3	2. internal failure	1	1. alarm dP PT3/PT4	1	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations	
7. H2 water trap drain solenoid valve, NC SV3		2. fail partially open	3. no shutdown	4	1. blockage	2	1. alarm dP PT3/PT4	1	8	11. Consider a timeout for not completing shutdown	
			1. decrease in pressure	4							
			2. high dP on stack	3							
		3. fail closed—closed drain	3. no shutdown	4							
			1. residual water after shutdown	2	1. electrical control failure	1	1. none	1	2		
			2. internal failure	1	1. electrical control failure	1	1. none	1	2		
	SV4	1. fail fully open—open drain	1. loss of pressure	4	1. electrical control failure	1	1. alarm dP PT3/PT4	1	4	11. Consider a timeout for not completing shutdown	
			2. high dP on stack	3	2. internal failure	1	1. alarm dP PT3/PT4	1	4		
			3. no shutdown	4	1. blockage	2	1. alarm dP PT3/PT4	1	8		
		2. fail partially open	1. decrease in pressure	4							
			2. high dP on stack	3							
			3. no shutdown	4							
		3. fail closed—closed drain	1. residual water after shutdown	2	1. electrical control failure	1	1. none	1	2		
			2. internal failure	1	1. electrical control failure	1	1. none	1	2		
			SV5	1. fail fully open—open vent	1. loss of pressure	4	1. electrical control failure	1	4	11. Consider a timeout for not completing shutdown	
		2. fail partially open	2. high dP on stack	3	2. internal failure	2	1. alarm dP PT3/PT4	1	8		
			3. no shutdown	4	1. blockage	2	1. alarm dP PT3/PT4	1	8		
		3. fail closed—closed vent	1. decrease in pressure	2							
			2. high dP on stack	2							
			3. no shutdown	4							
		SV6	1. fail fully open—open vent	1. none on shutdown	1	1. electrical control failure	1	4	4	11. Consider a timeout for not completing shutdown	
			2. internal failure	2	2. internal failure	2	1. alarm dP PT3/PT4	1	8		
			3. no shutdown	4	1. blockage	2	1. alarm dP PT3/PT4	1	8		
		2. fail partially open	1. decrease in pressure	2							
			2. high dP on stack	2							
			3. no shutdown	4							
		3. fail closed—closed vent	1. none on shutdown	1	1. electrical control failure	1	1. none	4	4		
			2. internal failure	1	1. electrical control failure	1	1. none	4	4		
			MV1	1. fail closed	1. no shutdown	4	1. internal failure	1	none	11. Consider a timeout for not completing shutdown	
		2. fail partially open	1. no shutdown	1	1. internal failure	1	1. none	4	4		
			1. none on shutdown	1	1. internal failure	1	1. none	4	4		
	MV2	1. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4		

H-2

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
12. O2 storage manual fill valve MV2		2. fail partially open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
		3. fail fully open	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
13. H2 delivery pressure regulator FPR1	FPR1	1. fail closed	1. no shutdown	4	1. electrical control failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
		2. fail partial closed, low outlet press	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		3. fail partially open, high outlet press	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		4. fail fully open, high outlet press	1. loss of reactant, RV opens	4	1. internal failure	1	1. none	4	16	1. Discuss H2 vent location—aft of engine intake 10. Describe how to size RV3/RV4 for full high-pressure storage flow
14. O2 delivery pressure regulator FPR2	FPR2	1. fail closed, no outlet press	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		2. fail partial closed, low outlet press	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		3. fail partially open, high outlet press	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		4. fail fully open, high outlet press	1. loss of reactant, RV opens	4	1. internal failure	1		4	16	6. Discuss high-pressure O2 release through luggage compartment hatch 10. Describe how to size RV3/RV4 for full high-pressure storage flow
15. H2 storage pressure transmitter PT1	PT1	1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range 2. check PG1	1	1	
					2. internal failure	1	1. signal out of range 2. check PG1	1	1	
		2. fail low—low electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range 2. check PG1	1	1	
					2. internal failure	1	1. signal out of range 2. check PG1	1	1	
		3. drift high or low	1. loss of leak detection	1	1. internal failure	1	1. check PG1 2. amp-hr check on reactant consumption vs pressure	3	3	3. Check accuracy of PGs at 200-hr maintenance interval
16. O2 storage pressure transmitter PT2	PT2	1. fail high—high electrical output	1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range 2. check PG2	1	1	
					2. internal failure	1	1. signal out of range 2. check PG2	1	1	
			1. loss of leak detection	1	1. electrical control failure	1	1. signal out of range	1	1	

H-3

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
H-4	PT3	2. fail low—low electrical output			2. internal failure	1	2. check PG2	1	1	
							1. signal out of range			
							2. check PG2			
		3. drift high or low	1. loss of leak detection	1	1. internal failure	1	1. check PG2	3	3	3. Check accuracy of PGs at 200 hr maintenance interval
							2. amp-hr check on reactant consumption vs pressure			
		17. H2 stack pressure transmitter PT3	1. fail high—high electrical output	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown
					2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown.
					1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown
		3. drift high or low	1. no shutdown	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown
					1. internal failure	1	1. none	4	12	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown
18.	PT4	O2 stack pressure transmitter PT4	1. fail high—high electrical output	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown
			2. false alarm high pressure	4	2. electrical control failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
										11. Consider a timeout for not completing shutdown

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
S-H		2. fail low—low electrical output	1. false alarm high dP	4	1. internal failure	1	1. none	4	16	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
			2. false alarm low pressure	4	2. electrical control failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
			3. drift high or low	1	1. internal failure	1	1. none	4	12	5. Need redundant pressure indicator for reactant. Consider second PT at reactant FC outlet.
			1. high dP on stack	3	1. internal failure	1	1. none			11. Consider a timeout for not completing shutdown
			1. false alarm high temperature	1	1. internal failure	1	1. check T4 for redundant alarm	1	1	
			2. none on shutdown	1	2. electrical control failure	1	1. check T4 for redundant alarm	1	1	
20. Coolant outlet temperature transmitter T2	T2	2. fail low—low electrical output	1. none on shutdown	3	1. internal failure	1	1. check T4 for redundant alarm	1	3	
			2. electrical control failure		1. electrical control failure	1	1. check T4 for redundant alarm	1	3	
			3. drift high or low	1	1. internal failure	1	1. T4 redundant	1	1	
			1. none on shutdown	1	1. internal failure	1	1. none	1	1	
			2. electrical control failure		1. electrical control failure	1	1. none	1	1	
			3. drift high or low	1	1. internal failure	1	1. none	1	1	
21. H2 water trap level switch LS1	LS1	1. fail set—SV3 remains open after amp-hr count	1. none on shutdown	1	1. electrical control failure	1	1. alarm PT3	1	1	
			2. internal failure		2. internal failure	2	1. alarm PT3	1	2	
		2. fail open -SV3 remains closed	1. none on shutdown	1	1. electrical control failure	1	1. amp-hr check on water accumulation	1	1	
			2. internal failure		2. internal failure	2	1. amp-hr check on water accumulation	1	2	
22. O2 water trap level switch LS2	LS2	1. fail set—SV4 remains open after amp-hr count	1. none on shutdown	1	1. electrical control failure	1	1. alarm PT4	1	1	
			2. internal failure		2. internal failure	2	1. alarm PT4	1	2	
		2. fail open -SV4 remains closed	1. none on shutdown	1	1. electrical control failure	1	1. amp-hr check on water accumulation	1	1	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
					2. internal failure	2	1. amp-hr check on water accumulation	1	2	
23. Coolant tank level switch LS3	LS3	1. fail set—electrically set filled	1. none on shutdown	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	9. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp
		2. fail open—electrically open empty	1. false low level indication	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	2	1. none	4	8	9. Develop an algorithm to indicate adequate coolant volume based on coolant flow and stack temp
		24. Coolant flow switch FS1	1. failed closed—indicates flow	1	1. internal failure	1	1. none	4	4	
			2. failed open—indicates no flow	1	1. internal failure	1	1. none	4	4	
25. H2 recirculation pump M1	M1	1. external gas leak	1. external H2 reaction	4	1. mechanical failure	1	1. alarm dP PT3/PT4	1	4	
			2. loss of pressure	4						
			3. no shutdown	4						
		2. fails to turn off	1. damage pump	3	1. electrical control failure	1	1. none	4	12	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	12	11. Consider a timeout for not completing shutdown
26. O2 recirculation pump M2	M2	1. external gas leak	1. external O2 reaction	4	1. mechanical failure	1	1. alarm dP PT3/PT4	1	4	
			2. loss of reactant	4						
			3. no shutdown	4						
		2. fails to turn off	1. damage pump	3	1. electrical control failure	1	1. none	4	12	11. Consider a timeout for not completing shutdown
					2. internal failure	1	1. none	4	12	11. Consider a timeout for not completing shutdown
27. Coolant circulation pump M3	M3	1. pumping stops	1. none on shutdown	1	1. electrical control failure	1	1. none	4	4	
					2. internal failure	1	1. none	4	4	
		2. pumping reduced	1. none on shutdown	1	1. blockage partial	1	1. alarm low flow FS1	3	3	
					2. electrical control failure	1	1. alarm low flow FS1	3	3	
					3. internal failure	1	1. alarm low flow FS1	3	3	
		3. external coolant leak	1. none on shutdown	1	1. mechanical failure	1	1. alarm low level LS3	1	1	
28. H2 water trap WT1	WT1	1. external gas leak	1. high dP on stack	4	1. mechanical failure	1	1. alarm dP PT3/PT4	1	4	
			2. residual water after shutdown	2						
29. O2 water trap WT2	WT2	1. external gas leak	1. high dP on stack	4	1. mechanical failure	1	1. alarm dP PT3/PT4	1	4	

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
			2. residual water after shutdown							
30. H2 Leak Detector A1	A1	1. fails off—no signal	1. reaction with H2	4	1. internal failure	1	1. interlocked with FC system	1	4	
					2. electrical control failure	1	1. interlocked with FC system	1	4	
		2. fails out of calibration—low	1. reaction with H2	3	1. internal failure	2	1. none	4	24	12. H2 leak detector calibration must be constantly checked
		3. fails out of calibration—high	1. false alarm high ambient H2	2	1. internal failure	2	1. interlocked with FC system	1	4	13. Consider redundant H2 leak detector
31. O2 delivery manual isolation valve MV4	MV4	1. fail closed	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		2. fail partially open	1. none on shutdown	1	1. internal failure	1	1. none	1	1	
		3. fail fully open	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
32. H2 delivery manual isolation valve MV3	MV3	1. fail closed	1. no shutdown	4	1. internal failure	1	1. none	4	16	11. Consider a timeout for not completing shutdown
		2. fail partially open	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
		3. fail fully open	1. none on shutdown	1	1. internal failure	1	1. none	4	4	
33. H2 storage tank V1	V1	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. amp-hr check on reactant consumption vs pressure	1	4	7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump.
			2. external H2 reaction	4						
		2. tank rupture	1. loss of reactant	4	1. mechanical failure	1	1. check rate of pressure decay on PT1	1	4	4. Appropriate procedures for handling high-pressure reactant tanks must be in place
			2. external H2 reaction	4						7. Develop a response to a detectable H2 tank gas leak. Consider an emergency storage tank dump.
34. O2 storage tank V2	V2	1. external gas leak	1. loss of reactant	3	1. mechanical failure	1	1. amp-hr check on reactant consumption vs pressure	1	3	8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump.
		2. tank rupture	1. loss of reactant	4	1. mechanical failure	1	1. check rate of pressure decay on PT2	1	4	4. Appropriate procedures for handling high-pressure reactant tanks must be in place
										8. Develop a response to a detectable O2 tank gas leak. Consider an emergency storage tank dump.
35. Coolant reservoir V3	V3	1. external coolant leak	1. flood system	1	1. mechanical failure	1	1. alarm low level LS3	1	1	
		2. blocked coolant outlet/inlet	1. none on shutdown	1	1. internal failure	1	1. alarm low flow FS1	1	1	
36. Product water tank	V4	1. external leak	1. none on shutdown	1	1. mechanical failure	1	1. none	4	4	

L-H

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Se v	Potential Cause/Mechanism of Failure	Oc c	Current Design Controls (Detection)	De t	RPN	Recommendations
		2. blocked inlet	1. residual water after shutdown	2	1. mechanical failure	1	1. none	4	8	14. Include a visual level indicator
37. System heat exchanger HTX1	HTX1	1. external coolant leak	1. none on shutdown	1	1. mechanical failure	1	1. alarm low level LS3	1	1	
		2. blocked coolant outlet	1. none on shutdown	1	1. internal failure	1	1. alarm low flow FS1	1	1	
		3. blocked coolant inlet	1. none on shutdown	1	1. internal failure	1	1. alarm low flow FS1	1	1	
		4. no air flow	1. none on shutdown	1	1. mechanical failure	1	1. none	4	4	
					2. electrical control failure	1	1. none	4	4	
		5. reduced air flow	1. none on shutdown	1	1. mechanical failure	1	1. none	4	4	
38. Fuel cell stack anode FC1-H2	FC1-H2	1. external H2 gas leak	1. none on shutdown	1	1. internal failure at cell	1	1. alarm low cell voltage	3	3	
		2. cross leak H2 to coolant	1. none on shutdown	1	1. internal failure at cell	1	1. none	4	4	
		3. cross leak H2 to cathode	1. none on shutdown	1	1. internal failure at cell	1	1. alarm low cell voltage	1	1	
		4. water blocking anode reactant path	1. none on shutdown	1	1. excess condensation in cell	1	1. alarm low cell voltage	1	1	
					2. loss of hydrophobicity in cell	1	1. alarm low cell voltage	1	1	
		5. dehydrated cell— anode	1. none on shutdown	1	1. over effective product water removal	1	1. alarm low cell voltage	1	1	
39. Fuel cell stack cathode FC1-O2	FC1-O2	6. inert gas buildup— anode	1. none on shutdown	1	1. reactant purity	3	1. monitor cell voltage and amp-hr for purge	1	3	
		1. external O2 gas leak	1. none on shutdown	1	1. internal failure at cell	1	1. alarm low cell voltage	3	3	
		2. cross leak O2 to coolant	1. none on shutdown	1	1. internal failure at cell	1	1. none	4	4	
		3. cross leak O2 to cathode	1. none on shutdown	1	1. internal failure at cell	1	1. alarm low cell voltage	1	1	
		4. water blocking anode reactant path	1. none on shutdown	1	1. excess condensation in cell	1	1. alarm low cell voltage	1	1	
					2. loss of hydrophobicity in cell	1	1. alarm low cell voltage	1	1	
40. Fuel cell stack coolant FC1-C	FC1-C	5. dehydrated cell— anode	1. none on shutdown	1	1. over effective product water removal	1	1. alarm low cell voltage	1	1	
		6. inert gas buildup— anode	1. none on shutdown	1	1. reactant purity	3	1. monitor cell voltage and amp-hr for purge	1	3	
		1. cross leak coolant to anode	1. decaying voltage	3	1. internal failure	1	1. alarm low cell voltage	1	3	
			2. flood stack	3						
		2. cross leak coolant to cathode	1. decaying voltage	3	1. internal failure	1	1. alarm low cell voltage	1	3	
			2. flood stack	3						

Items	P&ID No.	Potential Failure Modes	Potential Effect(s) of Failure	Sev	Potential Cause/Mechanism of Failure	Oc	Current Design Controls (Detection)	Det	RPN	Recommendations
		3. external coolant leak	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
		4. blocked coolant inlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
		5. blocked coolant outlet	1. high-temperature stack FC1	3	1. internal failure	1	1. alarm high temp TC4	1	3	
41. Coolant tank heater HT1	HT1	1. fail on—continuous heat	1. high-temperature stack FC1	3	1. electrical control failure	1	1. alarm high delta temp TC4/TC3	1	3	
		2. fail off—no heat	1. none on shutdown	1	1. electrical control failure	1	1. none	4	4	
					2. mechanical failure	1	1. none	4	4	
42. H2 storage pressure gauge PG1	PG1	1. fail out of range—high or low	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		2. out of calibration—low	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		3. out of calibration—high	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
43. O2 storage pressure gauge PG2	PG2	1. fail out of range—high or low	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		2. out of calibration—low	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval
		3. out of calibration—high	1. none on shutdown	1	1. internal failure	1	1. none	4	4	3. Check accuracy of PGs at 200 hr maintenance interval

APPENDIX I—TEST RESULTS

EPS Test #2—Pressure Difference EPS Test #6—Pressure Difference MPS Test #4—Pressure Difference

1. Scope
 - Purpose—This test simulates a pressure difference between anode and cathode caused by loss of reactant upstream or one reactant continually venting through an open downstream vent valve.
 - Shutdown/failure criteria—A pressure difference shutdown will be ignored and the pressure allowed to drop until an individual cell voltage drops below a 0.6 Vdc level.
2. Test conditions
 - Test article—4-cell stack 2.8x4.2-081
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load
 - Temp/pressure—70°C, 30 psig with H₂ or O₂ dropping to 0 psig
 - Reactants—fully humidified, 100% H₂ and O₂
 - Reactant flows
 - H₂ = 2.0 SLM (0.0112 SLM/Amp/cell no.)
 - O₂ = 1.68 SLM (0.0093 SLM/Amp/cell no.)
 - Load—constant 145W
3. Baseline test
 - 70°C, 30 psig, 100% H₂ and O₂
 - 1-hour test followed by polarization curve
4. Testing sequence
 - 2 separate 1-hour tests with one reactant dropping in 1 psid increments with a 2-minute hold at each increment
 - A. O₂ held at 30 psig, H₂ dropping from 30 psig to 0 psig
 - B. H₂ held at 30 psig, O₂ dropping from 30 psig to 0 psig
 - Each test followed by a baseline test
5. Data requirements
 - Standard output available from the Medusa test station

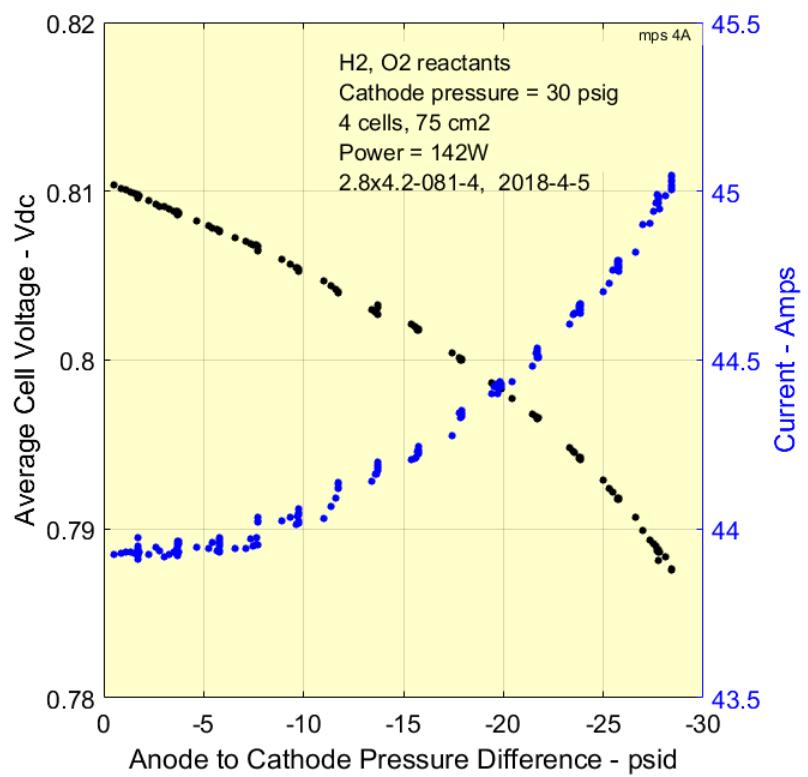


Figure I-1—Pressure Difference Test A

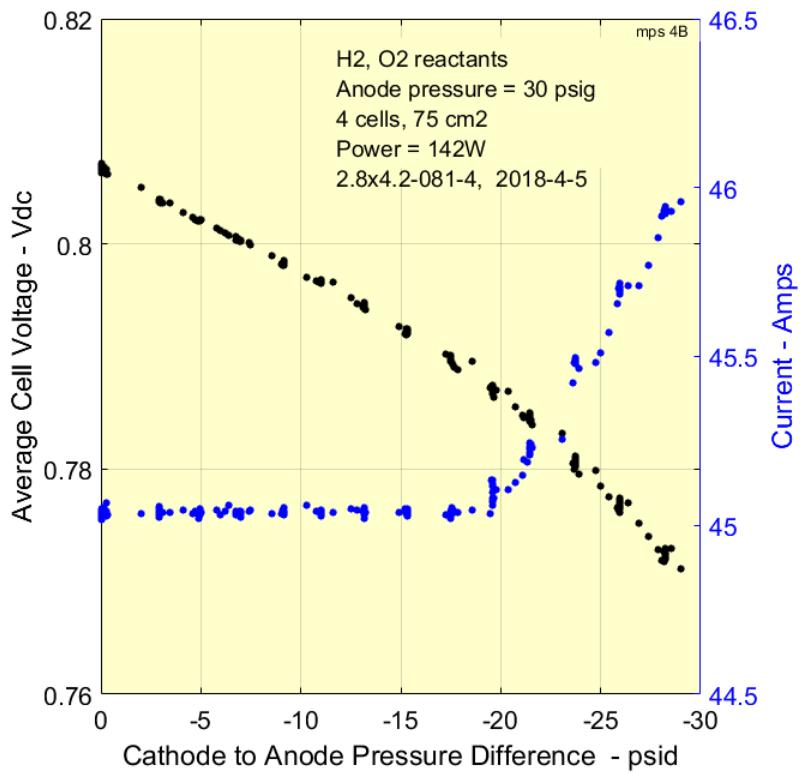


Figure I-2—Pressure Difference Test B

Remarks

The system pressure difference signal is typically set to alarm at 5 psid. These data show that the stack will continue to run long after the pressure difference alarm is activated, regardless of lower anode (H_2) or cathode (O_2) pressure.

Note that in Test B, the test station has some difficulty controlling current to maintain constant power as the cell voltage drops. This is believed to be due to the accuracy and tolerance level in the current control and oxygen mass flow controller.

Polarization data recorded at baseline conditions after each test did not show any degradation in stack performance.

EPS Test #1—Reactant Recirculation
MPS Test #1—Reactant Recirculation

1. Scope
 - Purpose—A series of tests will be run to simulate a reactant flow rate decay in either the anode or cathode recirculating circuit. Separate tests will be run with reduced recirculation for the anode and the cathode.
 - Shutdown/failure criteria—An individual test will be run for 1 hour or until individual cell voltage drops below a 0.6 Vdc level.
2. Test conditions
 - Test article—cell stack 2.8x4.2-081
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load
 - Temp/pressure—70°C, 30 psig with H₂ and O₂.
 - Reactants—fully humidified, 100% H₂ and O₂
 - Reactant flows
 - H₂ = 2.0 SLM, stoic = 1.5 (0.0112 SLM/Amp/cell no.) dropping to 1.35 SLM, stoic = 1 (0.00748 SLM/Amp/cell)
 - O₂ = 1.68 SLM, stoic = 2.5 (0.00935 SLM/Amp/cell no.) dropping to near 0.673 SLM, stoic = 1 (0.00374 SLM/Amp/cell)
 - Load—constant 45A (600mA/cm²)
3. Baseline test
 - 70°C, 30 psig, H₂ stoic = 1.5, and O₂ stoic = 2.5
 - 1-hour test followed by polarization curve
4. Testing sequence
 - 2 separate groups of tests. One group with variable H₂ flows for the anode and constant cathode flow. The other group with variable O₂ flows for the cathode and constant anode flow. Each test will be run at the given flows for 1 hour or until an individual cell voltage drops below 0.6 Vdc.
 - Following each test, the stack will be run at baseline conditions until the performance recorded during the initial baseline test returns.
 - Variable H₂ flow tests
 - A. H₂ = 1.62 SLM, stoic = 1.20, O₂ = 1.68 SLM, stoic = 2.50
 - B. H₂ = 1.49 SLM, stoic = 1.10, O₂ = 1.68 SLM, stoic = 2.50
 - C. H₂ = 1.42 SLM, stoic = 1.05, O₂ = 1.68 SLM, stoic = 2.50
 - Variable O₂ flow tests
 - D. H₂ = 2.03 SLM, stoic = 1.50, O₂ = 1.08 SLM, stoic = 1.60
 - E. H₂ = 2.03 SLM, stoic = 1.50, O₂ = 0.94 SLM, stoic = 1.40
 - F. H₂ = 2.03 SLM, stoic = 1.50, O₂ = 0.81 SLM, stoic = 1.20

5. Data requirements

- Standard output available from the Medusa test station

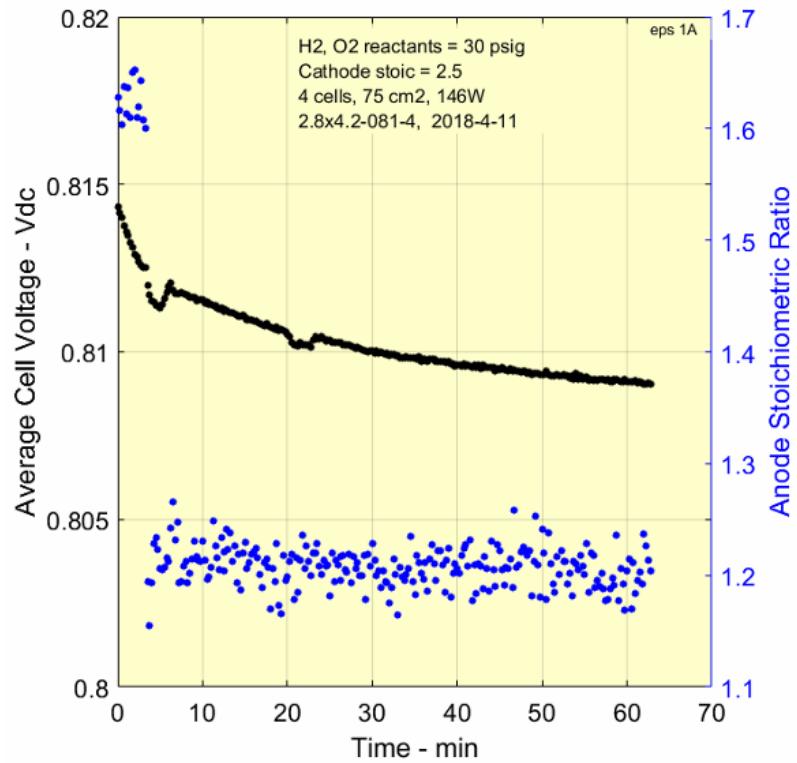


Figure I-3—Reactant Recirculation Test A

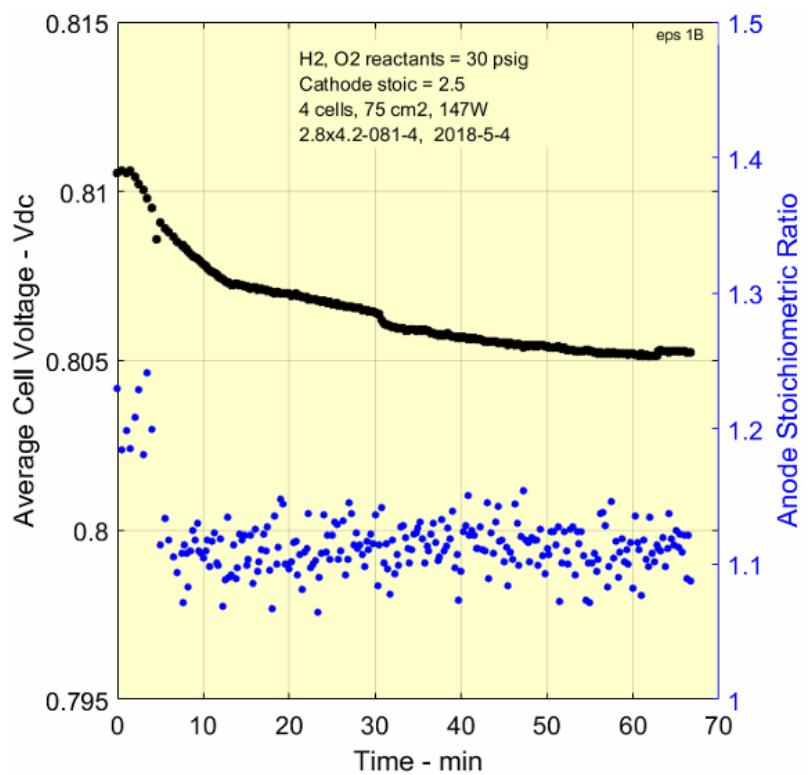


Figure I-4—Reactant Recirculation Test B

Test C—Could not be run successfully because of the low stoichiometric ratio on the anode.

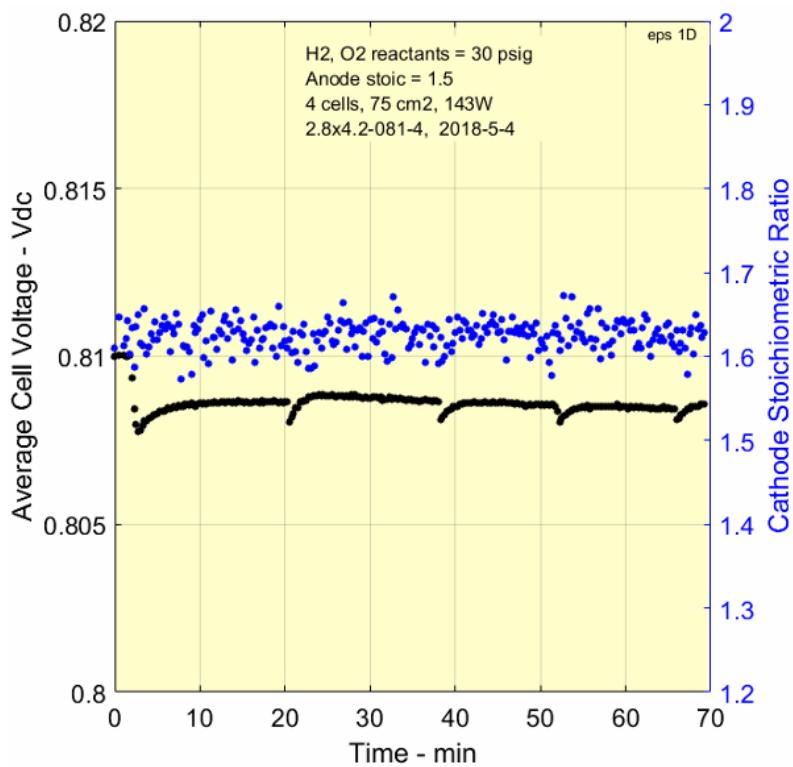


Figure I-5—Reactant Recirculation Test D

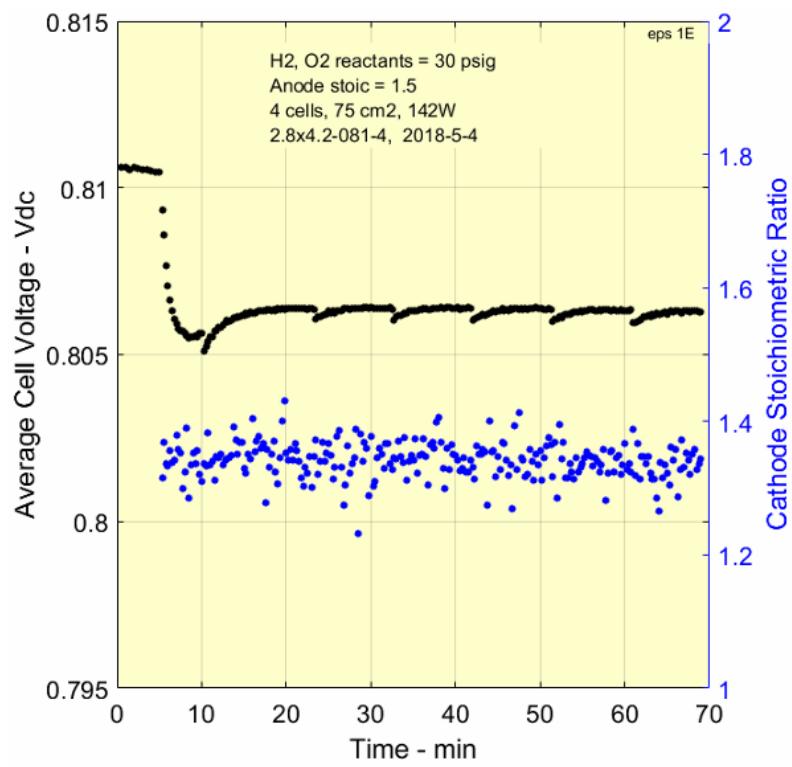


Figure I-6—Reactant Recirculation Test E

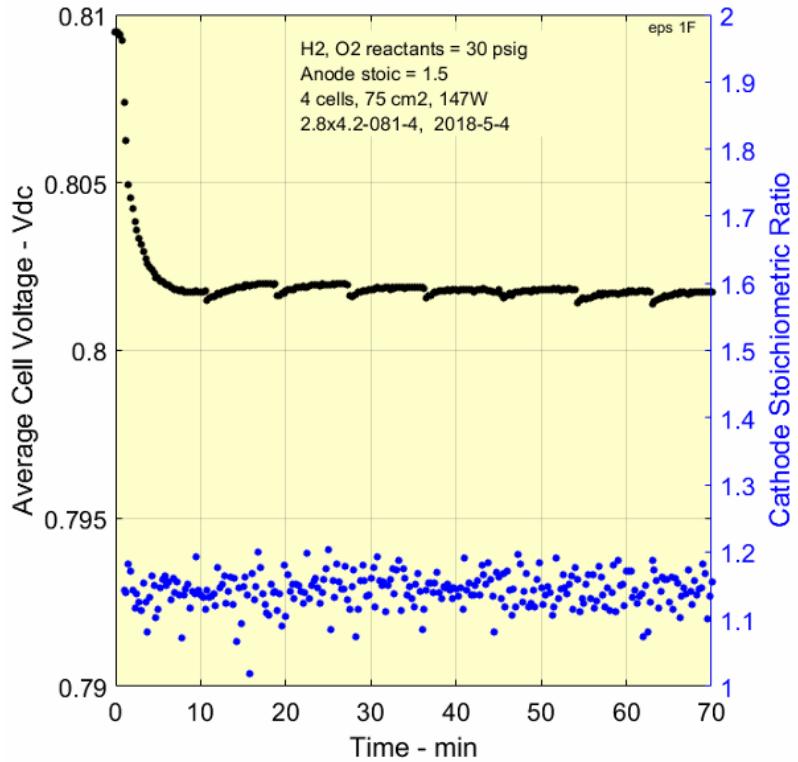


Figure I-7—Reactant Recirculation Test F

Remarks

Although the magnitude of the cell voltage drop is similar for both the anode (H₂) and cathode (O₂), the rate of the drop is the opposite of what is expected. Also, it was expected that the anode would be able to run with a stoichiometric ratio lower than 1.1. These results are probably due to the anode catalyst being a lightly loaded carbon-supported material that does not perform as well as the cathode, which is a pure platinum black material. The question now becomes how would the stack perform under similar conditions with a platinum black catalyst on both electrodes.

Note that in Tests D, E, and F, the periodic drop in cell voltage is due to a periodic drop in cathode pressure when a water trap on the oxygen side of the system is momentarily opened to vent product water.

Polarization data recorded at baseline conditions after each test did not show any degradation in stack performance.

EPS Test #7—Reactant Impurity
MPS Test #6—Reactant Impurity

1. Scope

- Purpose—The goal is to verify the reactant purge algorithm developed for maintaining fuel cell stack performance. The test will look at the decline of individual cell voltages as inert gases build up in the reactants.
- Shutdown/test criteria—Testing the stack on an open system does not allow the inerts to naturally build up. Several reactant mixes with increasing inert gas concentrations will be tested to provide data for predicting cell voltage degradation versus inert gas concentration. Reactant stoics will be held constant, and the total fuel flow will be increased to compensate for the increase in inert N2.

2. Test conditions

- Test article—4-cell stack 2.8x4.2-081
- Test station—4-cell capable Medusa for 150A, 4 Vdc load
- Temp/pressure—70°C, 45 psia
- Reactants—fully humidified
 - 100% H2 and O2 for baseline
 - 10%, 30% and 50% N2 in H2 for anode degradation
 - 10%, 30% and 50% N2 in O2 for cathode degradation
- Reactant flows—up 2.0 SLM H2 & 1.68 O2 for baseline, greater with inert contaminated reactants
- Load—constant 145W

3. Baseline test

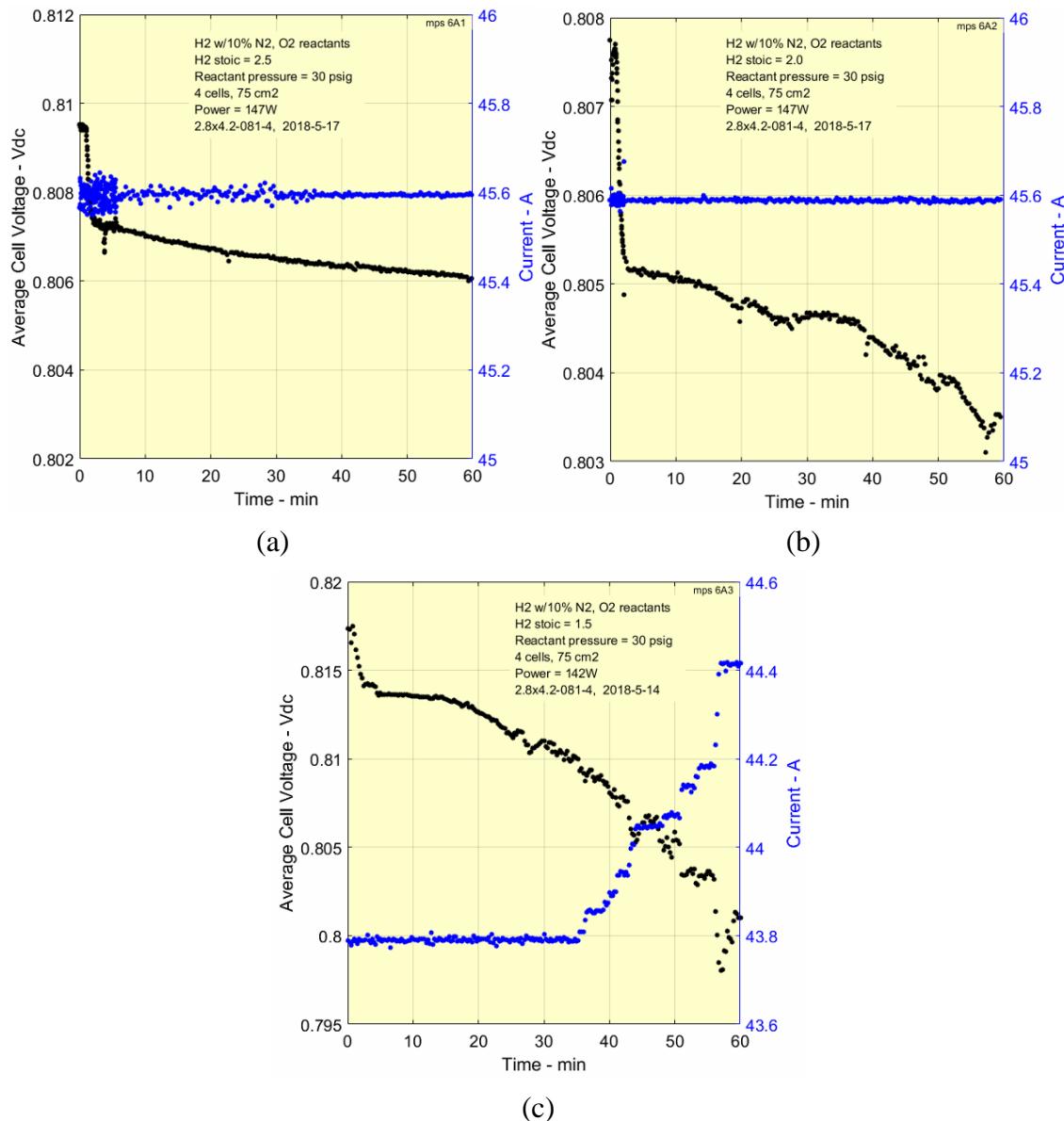
- 70°C, 45 psia, 100% H2 and O2
- 1-hour test followed by polarization curve data

4. Testing sequence

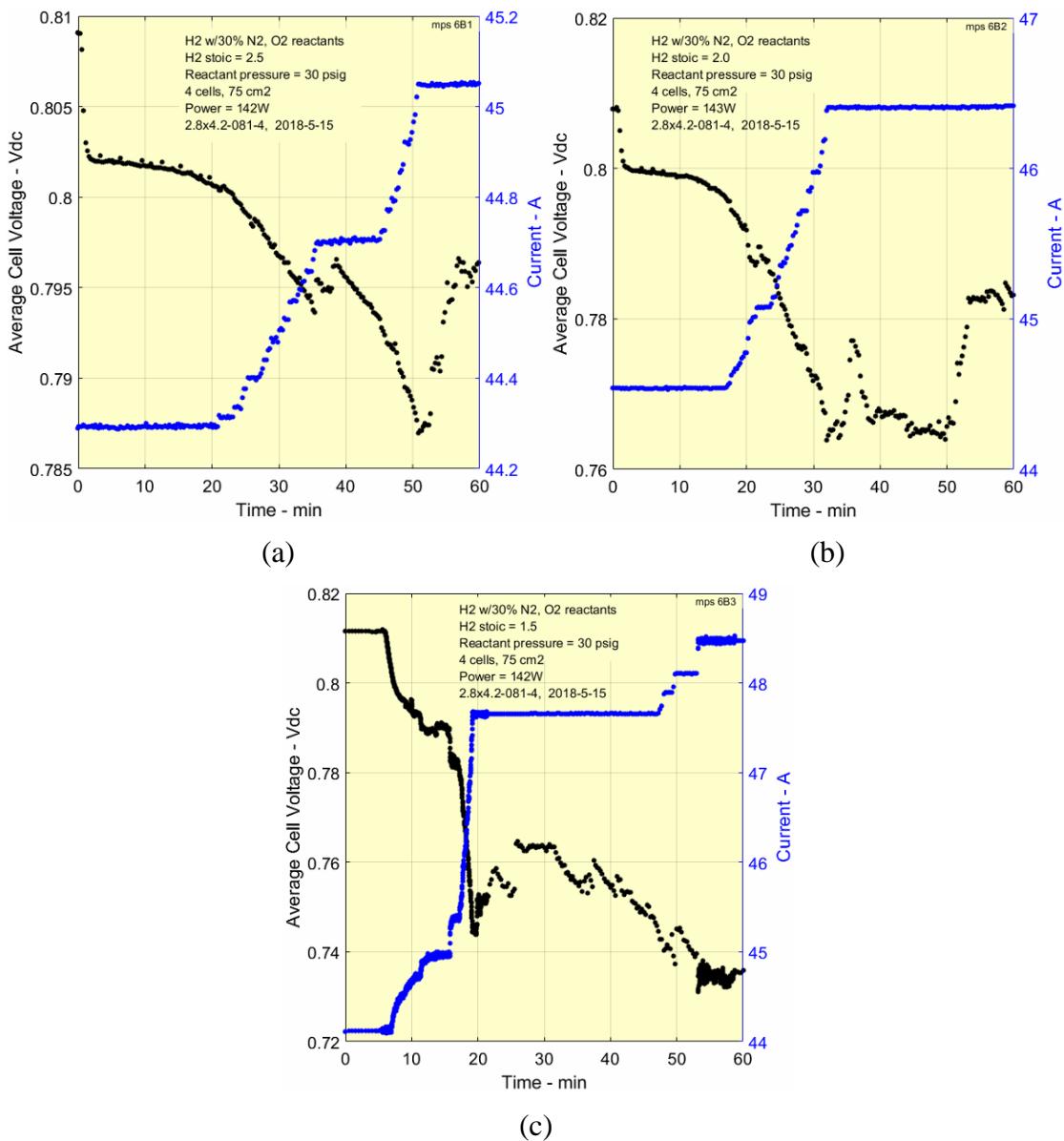
- 9 separate tests with H2—70°C, 45 psia, reactant stoics of 2.5, 2.0 & 1.5
 - A. 10% N2 in H2, 100% O2—anode flow (SLM) = 3.7 3.0 2.2
 - B. 30% N2 in H2, 100% O2—anode flow (SLM) = 4.4 3.5 2.6
 - C. 50% N2 in H2, 100% O2—node flow (SLM) = 5.0 4.0 3.0
- 9 separate tests with O2—70°C, 45 psia, reactant stoics of 1.5, 1.2, & 1.1
 - D. 10% N2 in O2, 100% H2—cathode flow (SLM) = 1.1 0.89 0.81
 - E. 30% N2 in O2, 100% H2—cathode flow (SLM) = 1.3 1.05 0.96
 - F. 50% N2 in O2, 100% H2—cathode flow (SLM) = 1.5 1.21 1.11
- 1-hour test followed by polarization curve data

5. Data requirements

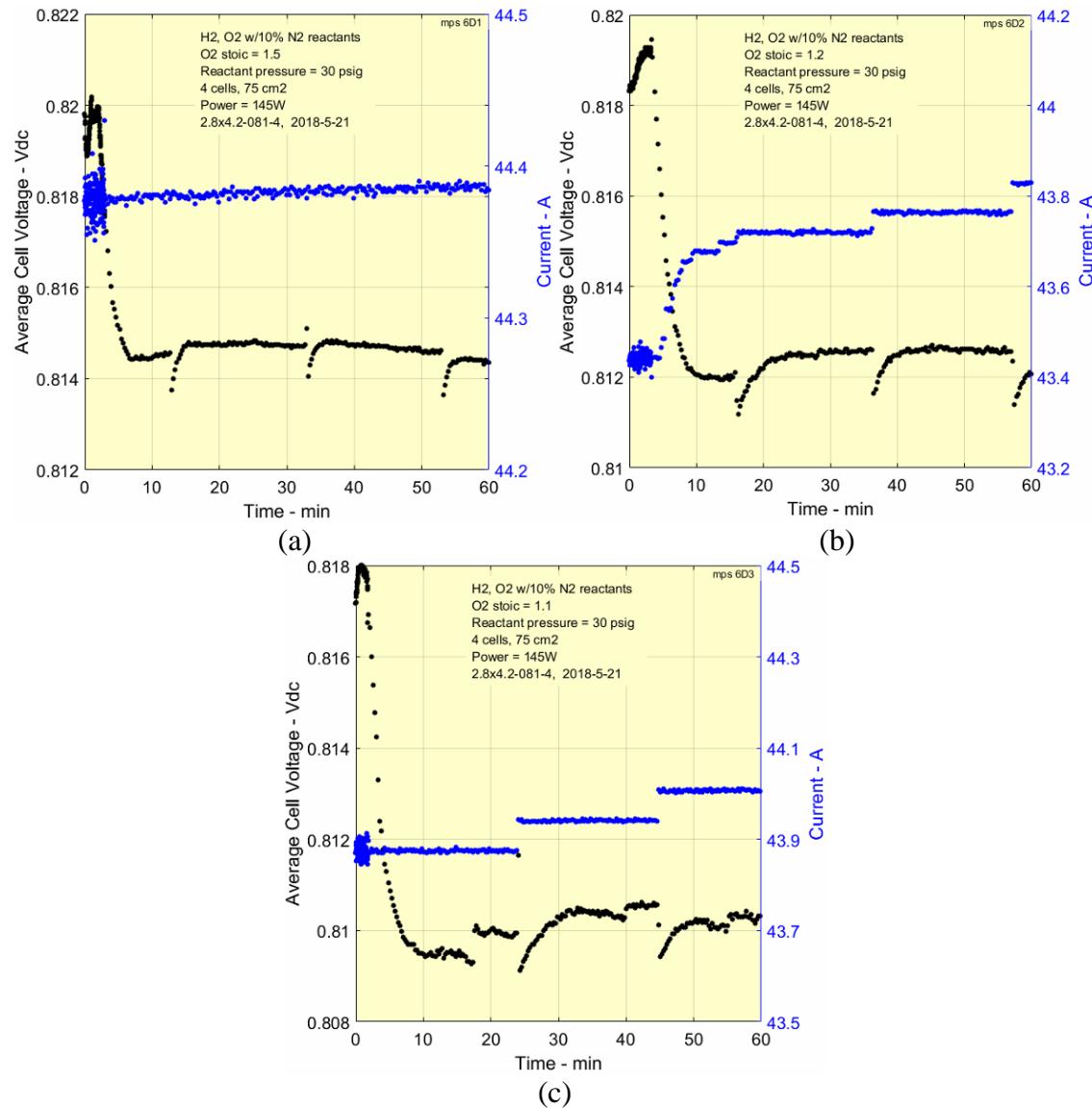
- Standard output available from the Medusa test station



Figures I-8—Reactant Impurity Test: (a) A1, (b) A2, and (c) A3



Figures I-9—Reactant Impurity Test: (a) B1, (b) B2, and (3) B3



Figures I-10—Reactant Impurity Test: (a) D1, (b) D2, and (c) D3

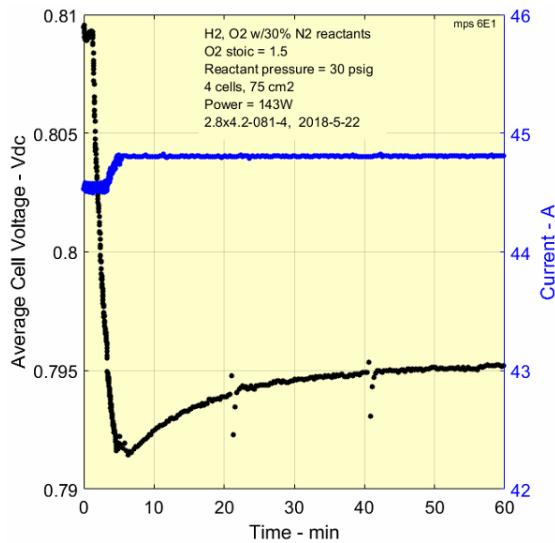


Figure I-11—Reactant Impurity Test E1

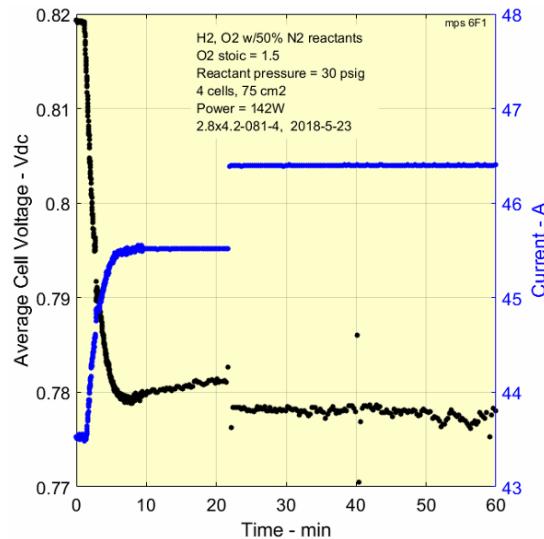


Figure I-12—Reactant Impurity Test F1

Tests C1, C2, C3, E2, E3, F2, F3—Could not be run successfully because of excessively high inert concentration or low stoichiometric flow.

Remarks

The inert nitrogen content in the reactants was deliberately chosen to be much higher than even the worst-case scenarios. The effect on performance from increased inert concentration and reduced stoichiometric content can be seen when comparing one chart to the next.

The test station had difficulty controlling current to maintain constant power as the cell voltage dropped. Also the periodic drop in cell voltage due to a periodic drop in cathode pressure is

present in some of the data. The periodic drop in cathode pressure occurs when the water trap on the oxygen side of the system is momentarily opened to vent product water.

Polarization data recorded at baseline conditions after each test did not show any degradation in stack performance.

MPS Test #3 – Excess Product Water

1. Scope
 - Purpose—The objective of this test will be to validate the amp-hour method for determining liquid water levels in the water-management system.
2. Test conditions
 - Test article—4-cell stack 2.8x4.2-081
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load
 - Temp/pressure—70°C, 30 psig with H₂ and O₂.
 - Reactants—100% H₂ and O₂, fully humidified
 - Reactant flows
 - H₂ stoic = 1.5
 - O₂ stoic = 2.5
 - Load—constant 600mA/cm²
3. Baseline test
 - 70°C, 30 psig, H₂ stoic = 1.5, and O₂ stoic = 2.5
 - 1-hour test followed by polarization curve
4. Testing sequence
 - Run at baseline conditions for 5 hours, collecting and measuring anode and cathode product water volume every hour.
5. Data requirements
 - Standard output available from the Medusa test station

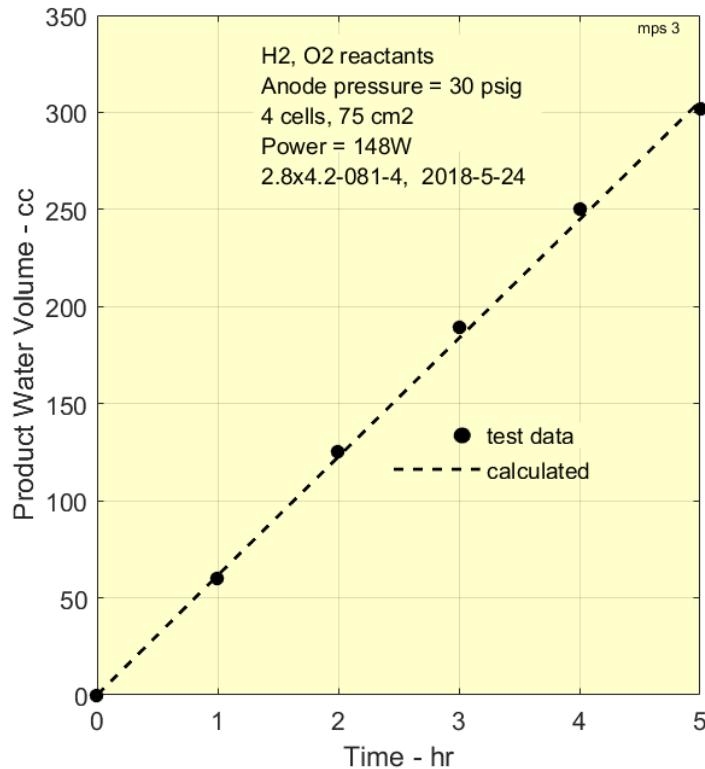


Figure I-13—Excess Product Water Test MPS

Remarks

The calculated value for the total accumulated amount of water produced by the fuel cell reaction is represented by the dash line. The water volumes collected during the 5-hour test closely match the computed values.

Note that the calculated volume is for the total product water volume. The accumulation of product water occurs largely on the cathode side of the cell. The sizing, drain sequence, and alarm conditions for both traps are all based on total accumulation in the cathode trap.

Polarization data recorded at baseline conditions before and after each test did not show any degradation in stack performance.

MPS Test #8—Cold Startup

1. Scope
 - Purpose—The MPS uses a coolant heater (HT1) as a bootstrap load for accelerating the warmup period when starting the system. The purpose of this test is to determine the warmup temperature rise rate in the absence of the bootstrap heater.
 - Test criteria—The test will be run until an operating temperature of 60°C is reached but no longer than 2 hours.
2. Test conditions
 - Test article—64-cell stack 2.8x4.2-082 with integrated BOP on TESI test cart
 - Temp/pressure—room temperature, ambient pressure
 - Reactants—100% H₂ and O₂ at 15 psig
 - Load—constant 1 kW
3. Testing sequence
 - System starts at test conditions and operates until operating temperature is achieved
4. Data requirements
 - a. Standard pressure outputs available from the TESI test cart

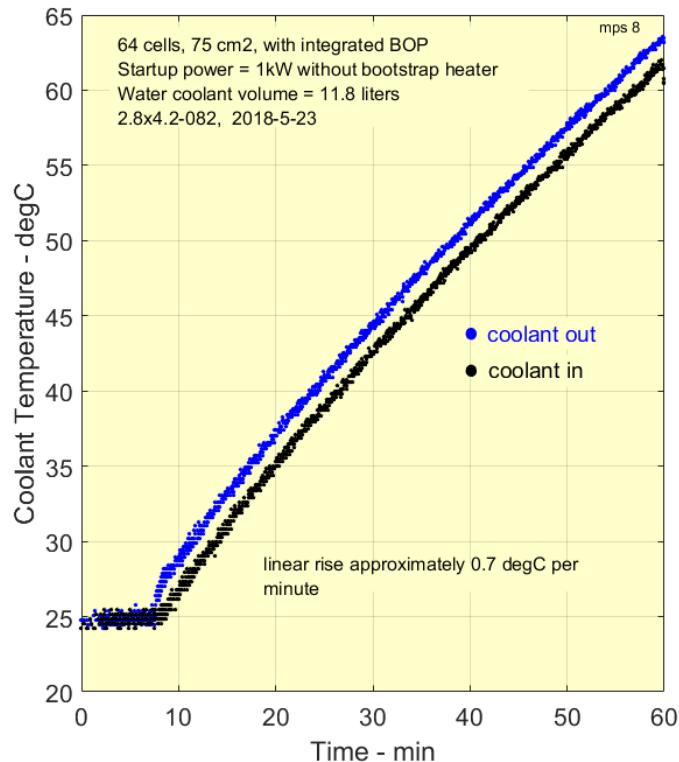


Figure I-14—Cold Startup Test

Remarks

The test was run on a full-size fuel cell system. This included a 64-cell stack with an integrated balance of plant and a coolant system designed for the appropriate thermal control. The total thermal capacitance includes all of the components plus the coolant.

Running with constant 1 kW load, the system took 50 minutes to reach a 63°C coolant outlet, using only the inefficiency of the stack. This test shows the need and benefit of using the output power to input additional heat through a bootstrap heater to accelerate system warmup.

Polarization data recorded at baseline conditions before and after each test did not show any degradation in stack performance.

EPS Test #9—Fuel Cell Stack Evacuation

1. Scope

- Purpose—The EPS fuel cell stack is evacuated as part of the pre-flight check and remains at low vacuum while in the standby condition, which ideally (unless an emergency would occur) would be until the next scheduled pre-flight check. This will determine the length of time the EPS stack can maintain the evacuated state.
- Test criteria—The test will be run for a maximum of 24 hours or until the stack pressure reaches ambient pressure.

2. Test conditions

- Test article—64-cell stack 2.8x4.2-082 with integrated BOP on TESI test cart
- Temp/pressure—room temperature, ambient pressure

3. Testing sequence

- System is run and then shutdown with the residual reactants consumed to create a vacuum. The system is then isolated and the system's pressure is monitored for the stack pressure versus time response.

4. Data requirements

- Standard pressure outputs available from the TESI test cart

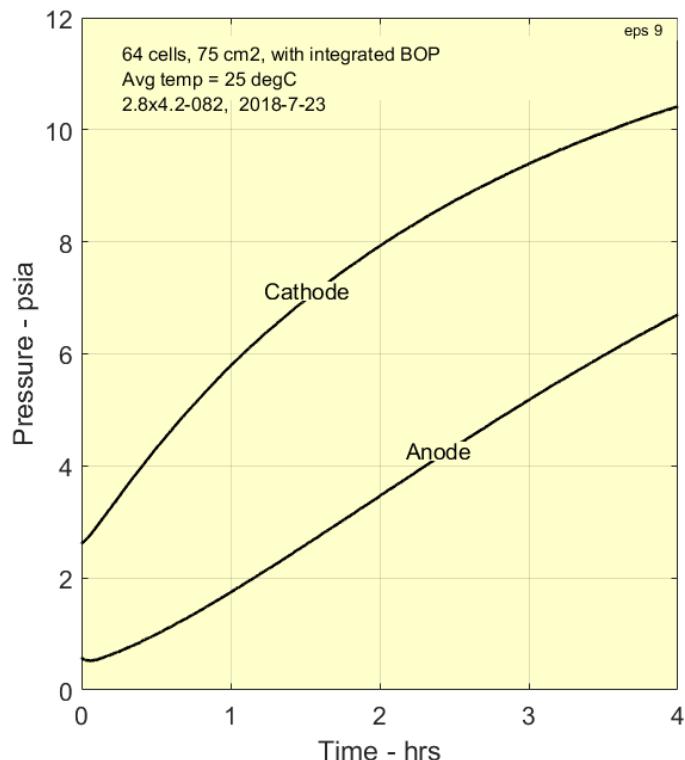


Figure I-15—Fuel Cell Stack Evacuation Test

Remarks

The test was run on a 64-cell stack with an integrated balance of plant (BOP). After the evacuation process is completed, the stack and BOP are isolated from the reactant supply by upstream solenoid valves. The total volume evacuated includes the water-management portion of the stack assembly and the BOP volume.

The test data indicate that a sufficient vacuum can be held for several hours. If the system downtime is any longer, an inert gas purge should be considered before a system restart.

Polarization data recorded at baseline conditions before and after each test did not show any degradation in stack performance.

EPS Test #5—Frozen Startup

1. Scope
 - Purpose—The intent of this test is to determine what effect sub-freezing temperature exposure has on the fuel cell stack ability to start and operate, and to uncover any detrimental effects to the fuel cell stack composition.
 - Shutdown/test criteria—Tests will be run until the baseline temperature of 70°C is reached but for no longer than 2 hours.
2. Test conditions
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load
 - Temp/pressure—70°C, 30 psig with H₂ and O₂
 - Reactants—100% H₂ and O₂, humidified to 5°C below the rising stack temperature beginning at room temperature
 - Reactant flows
 - H₂ stoic = 1.5
 - O₂ stoic = 2.5
 - Load—constant current at 15A (200mA/cm²)
3. Baseline test
 - 70°C, 30 psig, H₂ stoic = 1.5, and O₂ stoic = 2.5
 - 1-hour test followed by polarization curve
4. Testing sequence
 - 2 separate tests based on stack preparation prior to freezing
 - Prepped with purge—The stack will be dried using a dry, low-pressure N₂ purge of both the anode and cathode for a minimum of 30 minutes. Following the purge, the anode and cathode ports will be isolated, and N₂ will remain at pressure in the stack during the freezing process.
 - Prepped with vacuum—The stack will be evacuated by the process of dead-end consumption of all remaining reactants. H₂ will be added during the process to maintain the required stoichiometric mix. The anode and cathode ports will be isolated, and the stack will remain in a vacuum state during the freezing process.
 - Freeze—Prior to each startup test, the stack will be saturated to -20°C by a minimum 6-hr soak in the LabRepCo freezer set at -20°C.
 - First Leak Test—Prepped with purge
 - Following a “prepped with purge” and freeze, perform standard leak check to verify membrane integrity.
 - Startup Test—Prepped with purge.
 - Following “prepped with purge” and freeze, run startup at 15A (200mA/ cm²) to 70°C or 2 hrs.
 - Second Leak Test—Prepped with vacuum.

- Following a “prepped with vacuum” and freeze, perform standard leak check to verify membrane integrity.
- Startup Tests—Prepped with vacuum.
- Following “prepped with vacuum” and freeze, run startup at 15A (200mA/ cm²) to 70°C or 2 hrs.
- Following each test, the stack will be run at baseline conditions until the performance recorded during the initial baseline test returns.

5. Data requirements

- Standard output available from the Medusa test station.

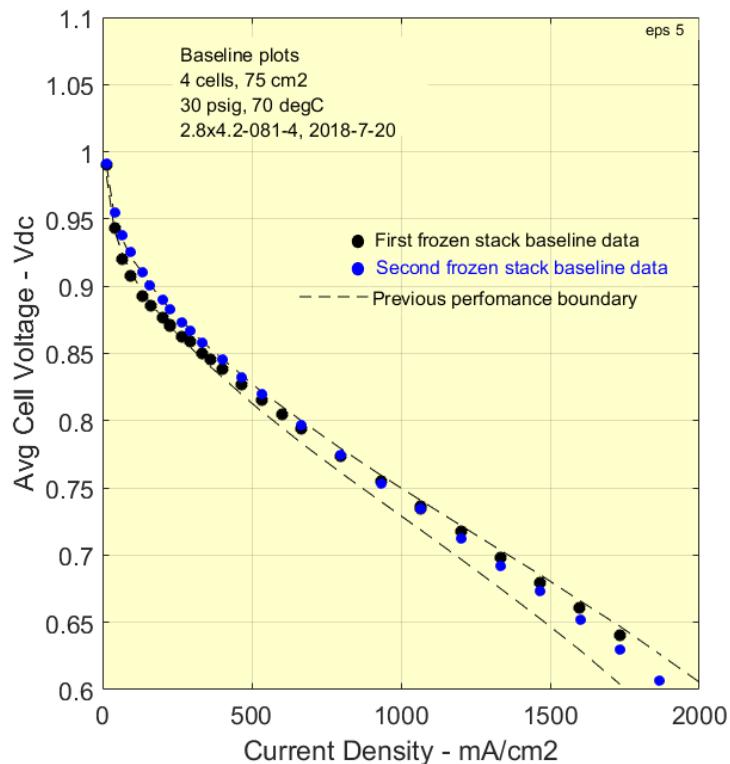


Figure I-16—Frozen Startup Test

Remarks

The PEM fuel cell operation depends on a well-hydrated membrane. Damage to a hydrated membrane as a result of freezing is a concern for the PEM fuel cell when not in operation.

The testing prepared a 4-cell stack for exposure to freezing conditions using two different methods. One method used a nitrogen purge to expel as much liquid water as possible. The second method used the evacuation by reactant consumption process, making no attempt to remove excess liquid water.

Polarization data recorded at baseline conditions after each test did not show any degradation in stack performance.

EPS Test #4—Excess Product Water

1. Scope
 - Purpose—The purpose of this test is to determine the effect of excess product water building up within the fuel cell stack. The test will track the decline in performance as the water buildup progresses and will check for any permanent effect.
 - Shutdown/test criteria—Tests will be run until a decline in performance becomes evident.
2. Test conditions
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load.
 - Temp/pressure—50°C, 5 psig with H₂ and O₂.
 - Reactants—100% H₂ and O₂, over humidified to 90°C.
 - Reactant flows
 - H₂ stoic = 1.5
 - O₂ stoic = 2.5
 - Load—constant current at 15A (200mA/cm²).
3. Baseline test
 - 70°C, 30 psig, H₂ stoic = 1.5, and O₂ stoic = 2.5
 - 1-hour test followed by polarization curve.
4. Testing sequence
 - Run the stack at the over-humidified condition until the average cell voltage begins to drop.
 - Follow with a baseline test.
5. Data requirements
 - Standard output available from the Medusa test station.

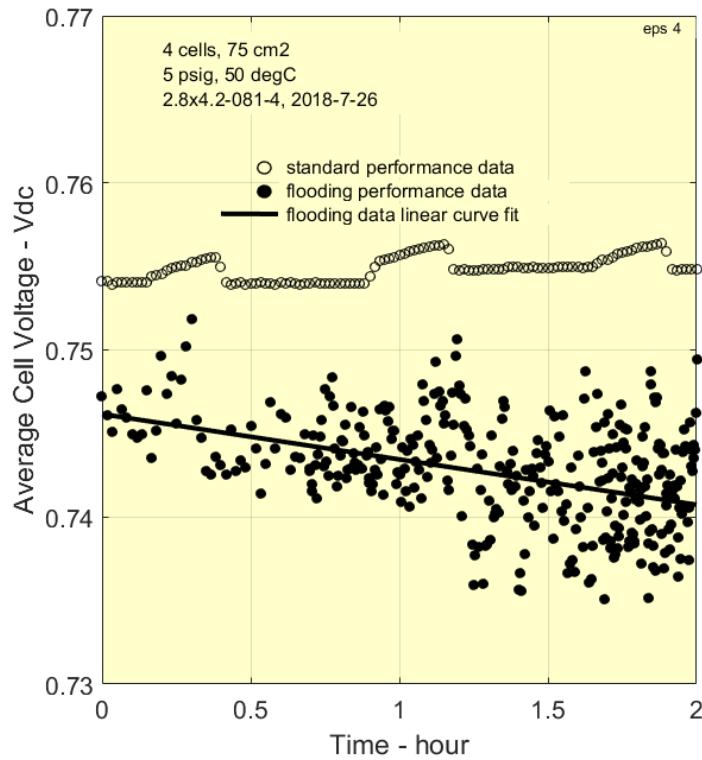


Figure I-17—Excess Product Water Test EPS

Remarks

Conditions for this test were set up to gradually cause the fuel cell stack to flood while monitoring performance. The stack was run at a lower pressure to allow a higher moisture content or humidity ratio (mass of water to unit mass of reactant gas). A higher humidification temperature also contributed to a higher humidity ratio. The stack was operated at a lower temperature to promote condensation of the highly humidified reactants.

The chart shows the standard performance at the temperature and pressure conditions before the onset of flooding. Note the periodic increase in cell voltage is due to an increase in coolant temperature as the controller fluctuates the temperature to maintain the thermal load. The lower voltage data in the chart show considerable scatter as flooding of the stack progresses. The solid line is a linear fit of the scattered data showing a decreasing performance trend due to the flooding.

Polarization data recorded at baseline conditions after each test did not show any degradation in stack performance.

MPS Test #2—High-Temperature Operation
EPS Test #3—High-Temperature Operation

1. Scope
 - Purpose—The purpose of this test is to determine the effect of operating the stack at an excessively high temperature. The test will track performance as the stack climbs above the nominal alarm-shutdown temperature. A baseline polarization test run will determine any cell damage.
 - Shutdown/test criteria—The test will run until the estimated maximum cell temperature is considered too extreme or cell failure is evident.
2. Test conditions
 - Test station—4-cell capable Medusa for 150A, 4 Vdc load.
 - Temp/pressure—No coolant, no temperature control, 30 psig with H₂ and O₂.
 - Reactants—100% H₂ and O₂, fully humidified to 90°C.
 - Reactant flows
 - H₂ stoic = 1.5
 - O₂ stoic = 2.5
 - Load—constant current at 45A (600mA/cm²)
3. Baseline test
 - 70°C, 30 psig, H₂ stoic = 1.5, and O₂ stoic = 2.5
 - 1-hour test followed by polarization curve.
4. Testing sequence
 - Run the stack without coolant and temperature control. Monitor the exterior temperature of the graphite bipolar plates using an IR thermometer. Run until estimated maximum interior cell temperature exceeds 120°C.
 - Follow with a baseline test.
5. Data requirements
 - Standard output available from the Medusa test station.
 - Graphite bipolar, exterior temperature, recorded concurrent with test station data.

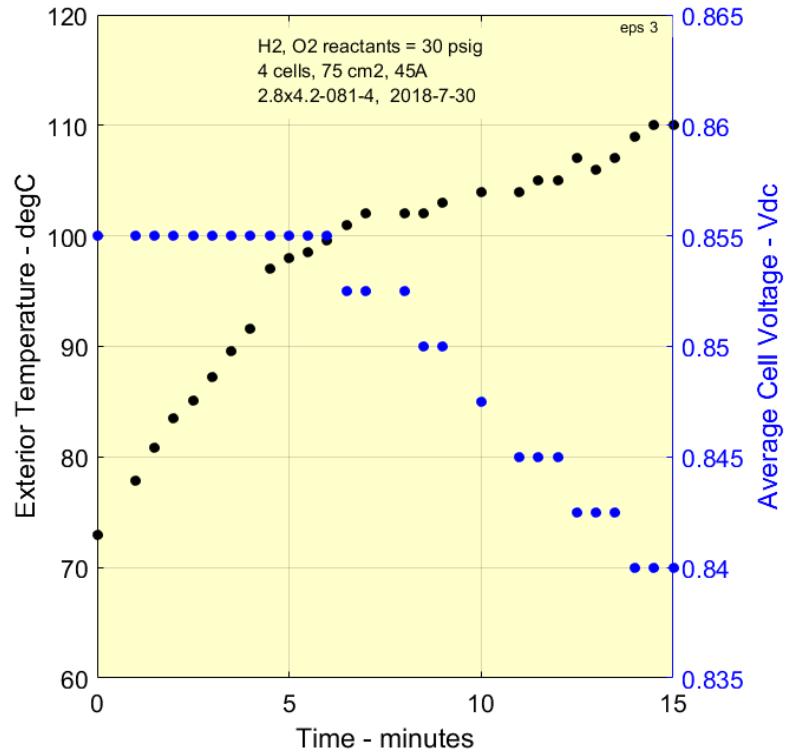


Figure I-18—Post High Temperature Operation Baseline

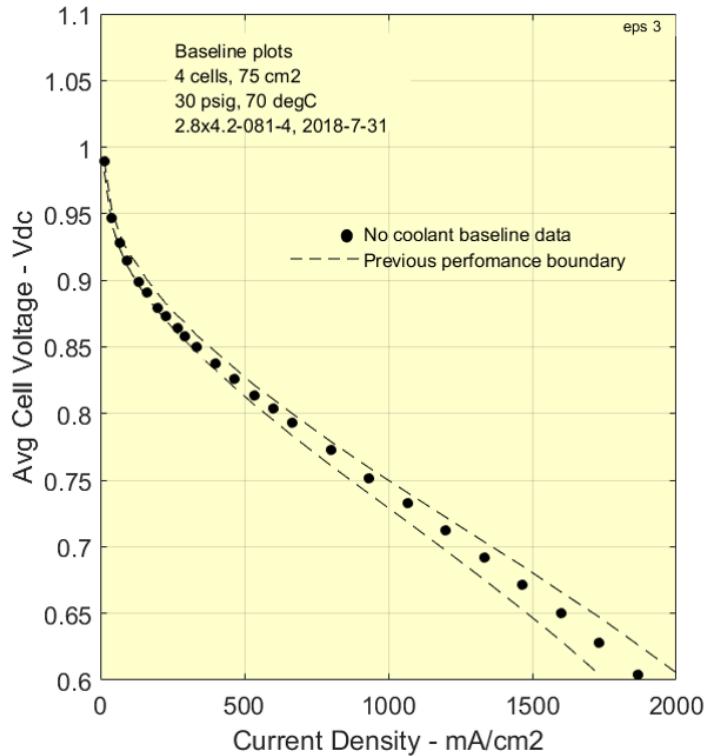


Figure I-19—High-Temperature Operation Test

Remarks

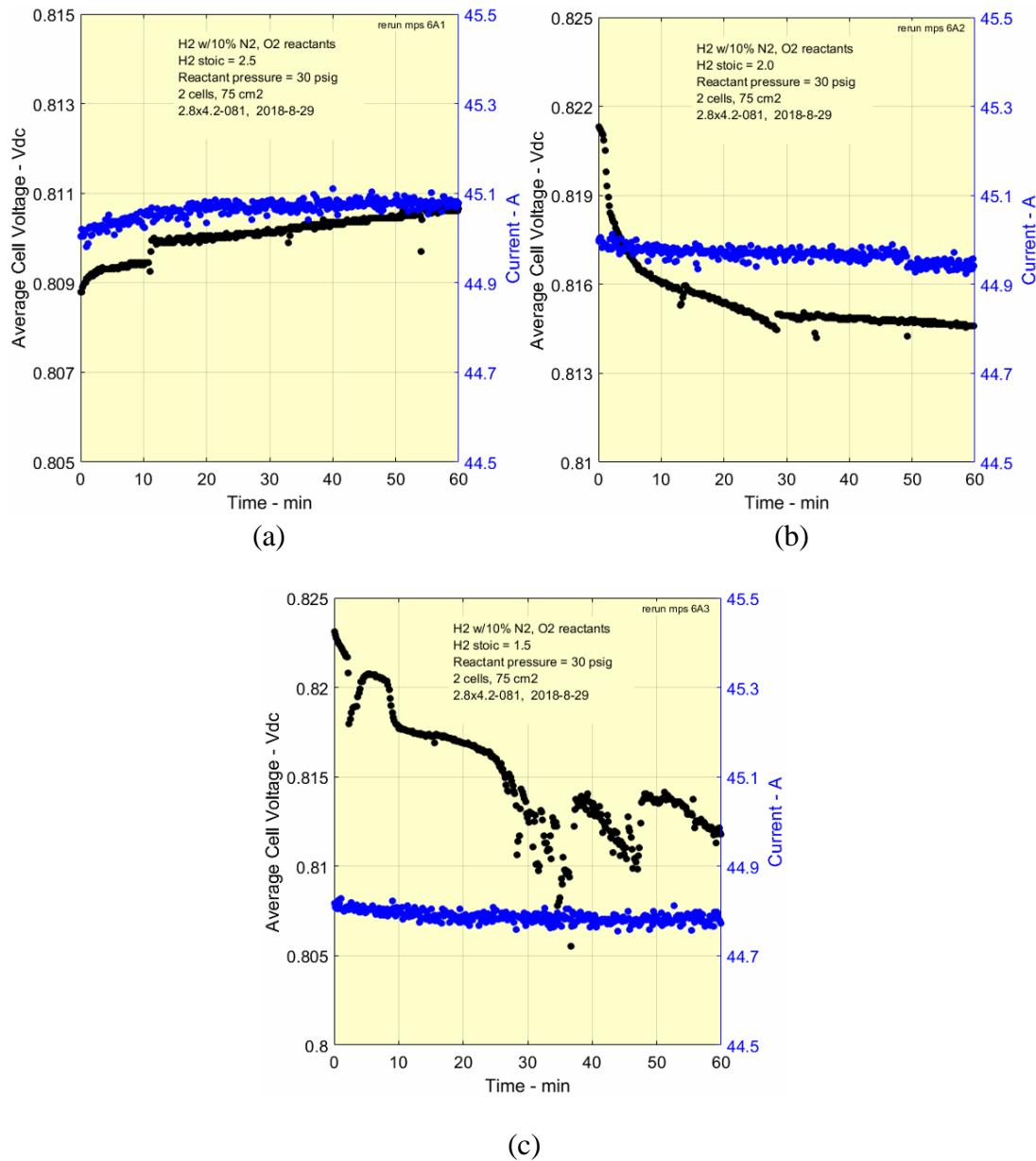
The coolant was removed for this test. Without a coolant, the internal temperature of the stack cannot be measured or controlled. The stack was run at constant current, and the stack temperature was allowed to increase. The external temperature of the graphite bipolar plates was monitored using an infrared thermometer. At an external temperature of 110°C, the test was terminated.

The data collected during the test show a decrease in the average cell voltage. This is evidence that the stack was drying out at the elevated temperatures. The test-station humidifiers are limited to 90°C. The internal cell temperatures exceeded the humidifier limit enough to begin to dry out the cells.

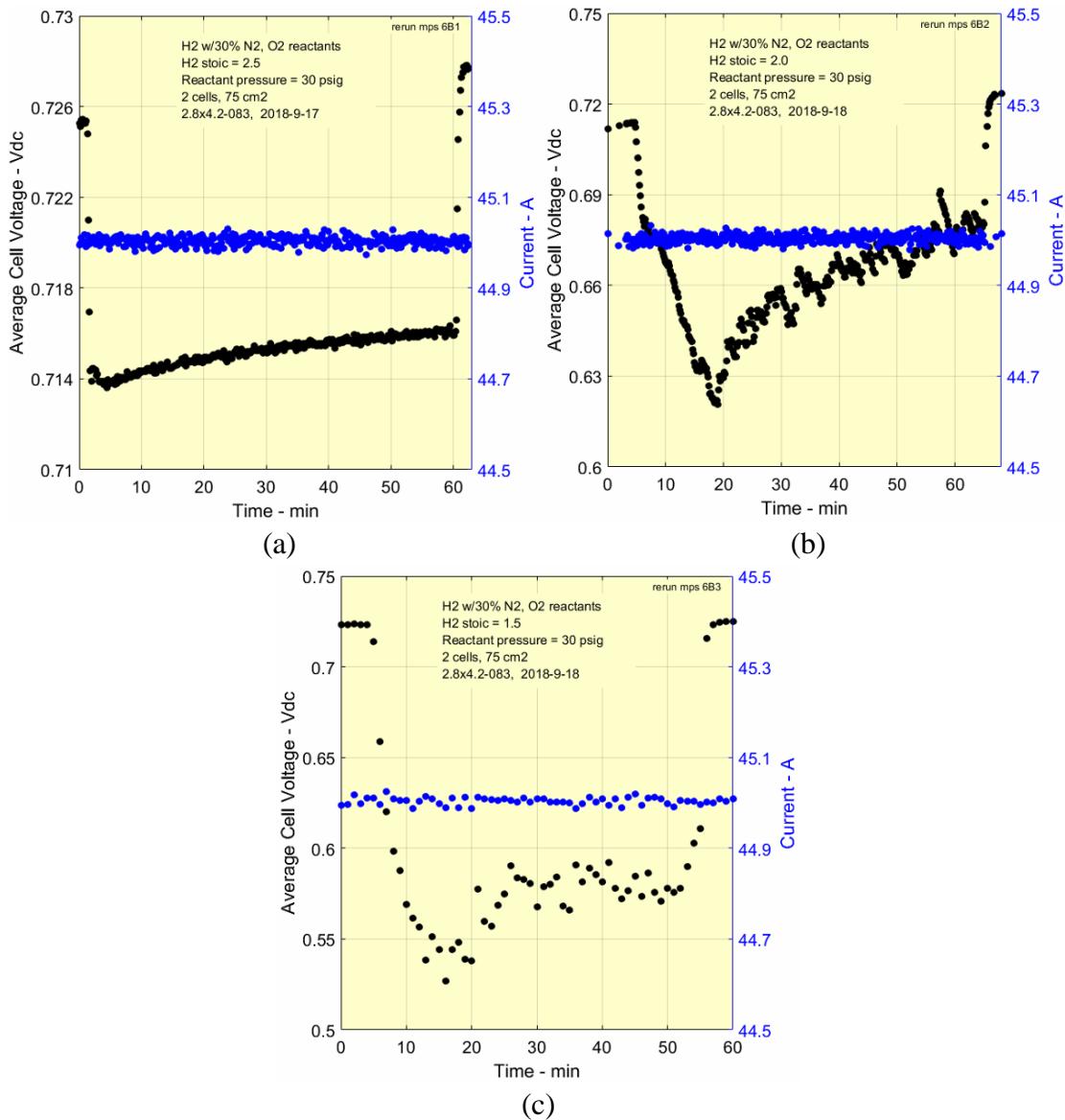
Polarization data recorded at baseline conditions after the test are shown in figure I-18. After operating to a maximum internal temperature estimated to exceed 120 °C, the polarization data does indicate any degradation in stack performance when compared with previous performance data.

Rerun EPS Test #7 and MPS Test #6 – Reactant Impurity

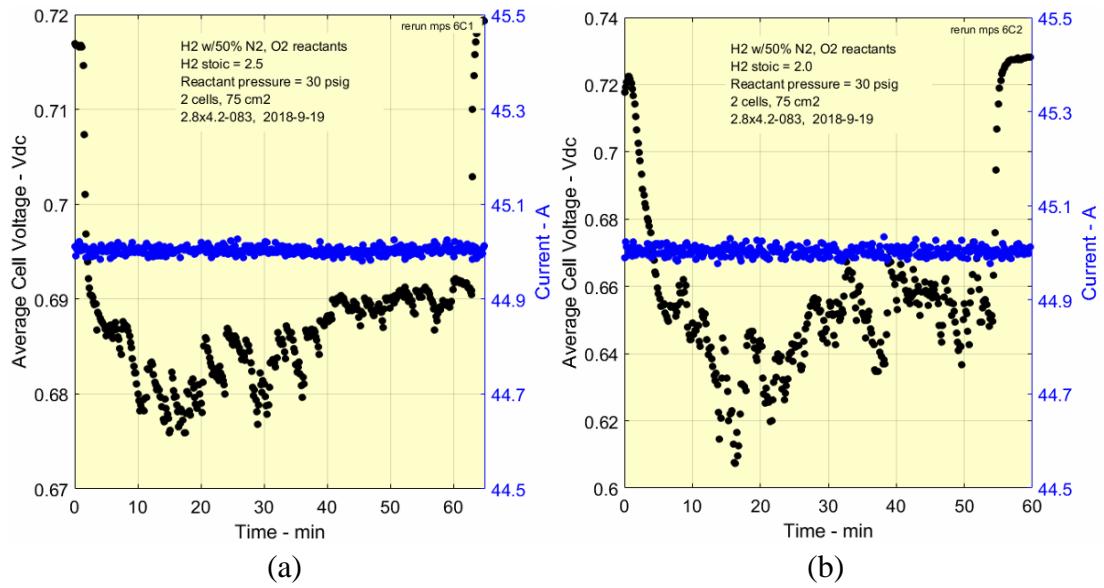
1. Scope
 - Purpose—Rerun the reactant impurity test with platinum black catalyst on the anodes. The test will look at the decline of individual cell voltages as inert gases build up in the reactants and compare with previous tests using a carbon-supported catalyst on the anodes.
 - Shutdown/test criteria—Testing the stack on an open system does not allow the inert gases to naturally build up. Several reactant mixes with increasing inert gas concentrations will be tested to provide data for predicting cell-voltage degradation versus inert gas concentration. Reactant stoics will be held constant, and the total fuel flow will be increased to compensate for the increase in inert N2.
2. Test conditions
 - Test station—2-cell capable Medusa for 100A, 4 Vdc load
 - Temp/pressure—70°C, 45 psia
 - Reactants—fully humidified
 - 100% H2 and O2 for baseline
 - 10%, 30% and 50% N2 in H2 for anode degradation
 - Reactant flows—up 2.0 SLM H2 & 1.68 O2 for baseline, greater with inert contaminated reactants
 - Load—constant 145W
3. Baseline test
 - 70°C, 45 psia, 100% H2 and O2
 - 1-hour test followed by polarization curve data
4. Testing sequence
 - 9 separate tests with H2—70°C, 45 psia, reactant stoics of 2.5, 2.0 & 1.5
 - D. 10% N2 in H2, 100% O2—anode flow (SLM) = 1.9 1.5 1.1
 - E. 30% N2 in H2, 100% O2—anode flow (SLM) = 2.2 1.8 1.3
 - F. 50% N2 in H2, 100% O2—anode flow (SLM) = 2.5 2.0 1.5
5. Data requirements
 - Standard output available from the Medusa test station



Figures I-20—Rerun Reactant Impurity Test: (a) A1, (b) A2, and (c) A3



Figures I-21—Rerun Reactant Impurity Test: (a) B1, (2) B2, (3) B3



Figures I-22—Rerun Reactant Impurity Test: (a) C1 and (b) C2

Test C3—Could not be run successfully because of excessively high inert concentration or low stoichiometric flow

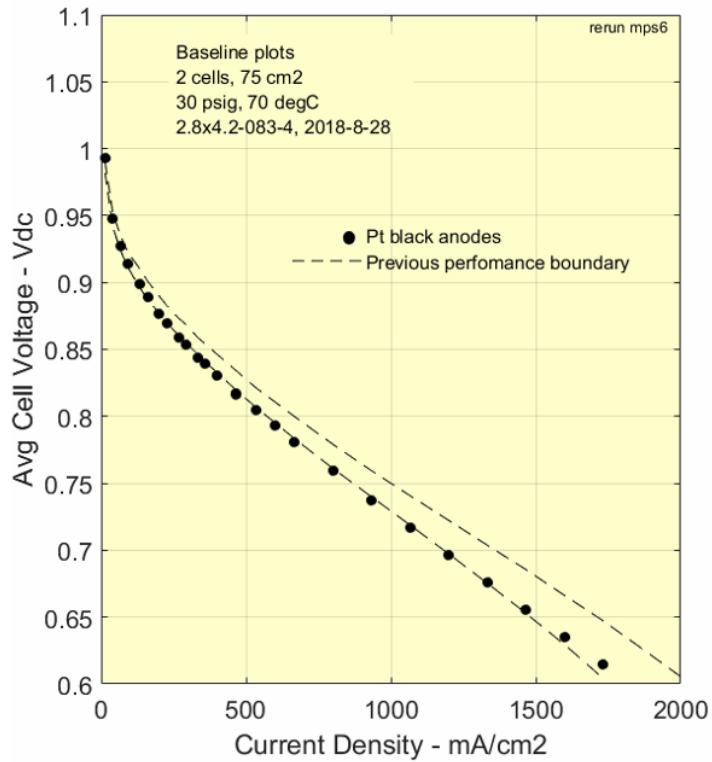


Figure I-23—Post Rerun Reactant Impurity Baseline

Remarks

The inert nitrogen content in the reactants was deliberately chosen to be much higher than even the worst-case scenarios. The effect on performance from the increased inert concentration and reduced stoichiometric content can be seen in figure I-24. Performance degradation is shown as maximum average cell voltage drop. The results using a Pt black anode catalyst show a tolerance to the reactant with the 50% inert content not seen with the carbon supported Pt catalyst.

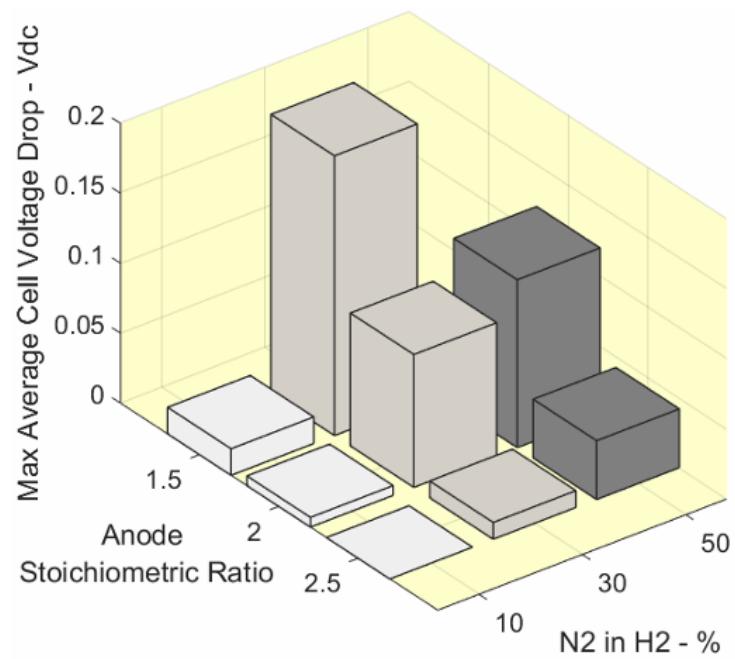


Figure I-24—Rerun Reactant Impurity Performance Comparison