Hydrogen Station Equipment Performance Device HyStEP

Summary of Failure Modes and Effects Analysis

Revision 0

TR00742-03-R00

January 2016

Prepared for:

Sandia National Laboratories

Powertech Project Number: PL-00742

Powertech Labs Inc.
12388 88th Avenue
Surrey, BC, V3W 7R7
www.powertechlabs.com

1 Executive Summary

The Failure Modes and Effects Analysis (FMEA) of the Hydrogen Station Equipment Performance Device (HyStEP) was carried out to examine the system for potential failure modes and their associated effects. The FMEA was facilitated by Intertek Consulting and was undertaken by Powertech Labs and the HyStEP Project Team. Results from this analysis were used to assist in finalizing and improving the system design and associated handling and testing procedures.

Assumptions made in the development of this FMEA include:

- No distinction was made for each item's maturity of design; each item was modeled based on its intended function.
- The system analyzed included the H2 receiving system, sequencing system, tank system, defuel system, purge system, control system, and data report.
- The FMEA followed the model defined by the Design FMEA section of SAE J1739:2009 as per the FMEA worksheet provided by Intertek Consulting
- The FMEA emphasized analysis at the functional level, based on the defined component functions.
- The failure modes were generally defined as the negative of the function.
- The FMEA focused on potential end effects only.

The FMEA results indicate the following:

- 7 functional blocks were analyzed
- 44 functions were defined
- 202 failure modes and effects were identified
- Each effect was assigned severity, occurrence, and detection/prevention ratings
- 47 failure mode effects had severity of 9 or 10 indicating a safety hazard
- 20 failure mode effects had a Risk Priority Number (RPN = severity*occurrence*detection) greater than 100

Table of Contents

2 Introduction

The Design Failure Modes and Effects Analysis (DFMEA) of the Hydrogen Station Equipment Performance Device (HyStEP Device) was carried out to examine the system for potential failure modes and their associated effects. Results from this analysis were used to assist in finalizing and improving the system design and associated handling and testing procedures.

3 Failure Modes and Effects Analysis

A Failure Modes and Effects Analysis (FMEA) is an analysis procedure that documents all potential failures of a system within specified ground rules. The FMEA is a procedure that determines what can fail and how it can fail (failure mode) and the effects of the failure on the system (effects).

The objectives and benefits of performing a FMEA include:

- Enhancing system safety by discovering potential failure modes that could result in hazardous conditions
- Analyzing the effects of severe, undetectable, and highly occurring failures
- Influencing the design to mitigate the impact of failures

Several cautions should be observed in the application and interpretation of a FMEA. First, a FMEA considers only non-simultaneous failure modes. Each failure mode is considered individually, assuming that all other components of the system function as designed. This provides limited insight into the effects of multiple component failures on system functions and into latent failures such as issues of timing or sequencing.

Secondly, the cause-effect relationship is not adequately represented in many FMEA models. In general, there is no representation for the likelihood that a cause will result in a particular effect. Some analysts address the issue by assuming that all potential effects will result, given that a cause of failure mode has occurred. This generally leads to an overestimation of risk.

A third weakness is the ambiguity of the Risk Priority Number (RPN), a primary output of the analysis. The RPN is calculated as the product of qualitative severity, occurrence, and detection values. This approach attempts to quantify risk, through the RPN, without adequately quantifying the factors that contribute to the RPN.

3.1 FMEA Overview

An effective and efficient FMEA requires some preliminary planning on how to approach the analysis. It also requires the establishment of various ground rules to guide the development and analysis of the failure modes and their effects. Details on the preliminary planning and the ground rules established for this FMEA are contained in the following sections.

3.1.1 System Model

An understanding of the system to be analyzed is essential prior to the development of a FMEA. Typically, system block diagrams and many other system-modeling techniques are used to understand system hierarchies. A FMEA cannot succeed without first having a complete and accurate system model.

The system model used for this FMEA was developed by Powertech Labs and the HyStEP Project Team using a template prepared by Intertek Consulting. For the purposes of this FMEA, the system analyzed was split into 7 different systems: the H2 receiving system, sequencing system, tank system, defuel system, purge system, control system, and data report. A block diagram is shown in Figure 1 below that shows how each system is interconnected. A P&ID drawing from the time the FMEA was conducted is shown in Figure 2 that identifies the components in each system. In this drawing, the green circled areas denote the safety system.

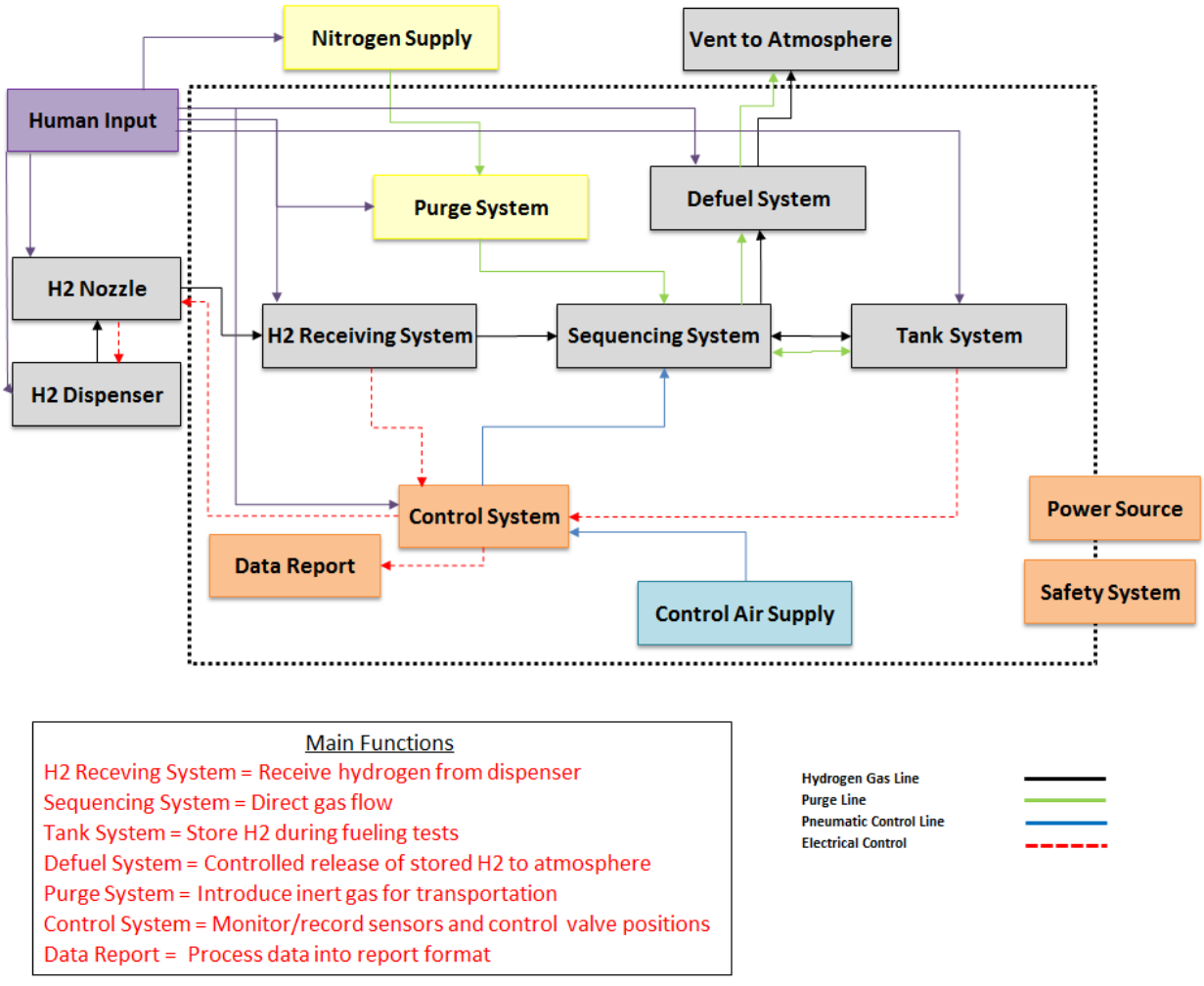

Figure 1: Block Diagram or Process Map

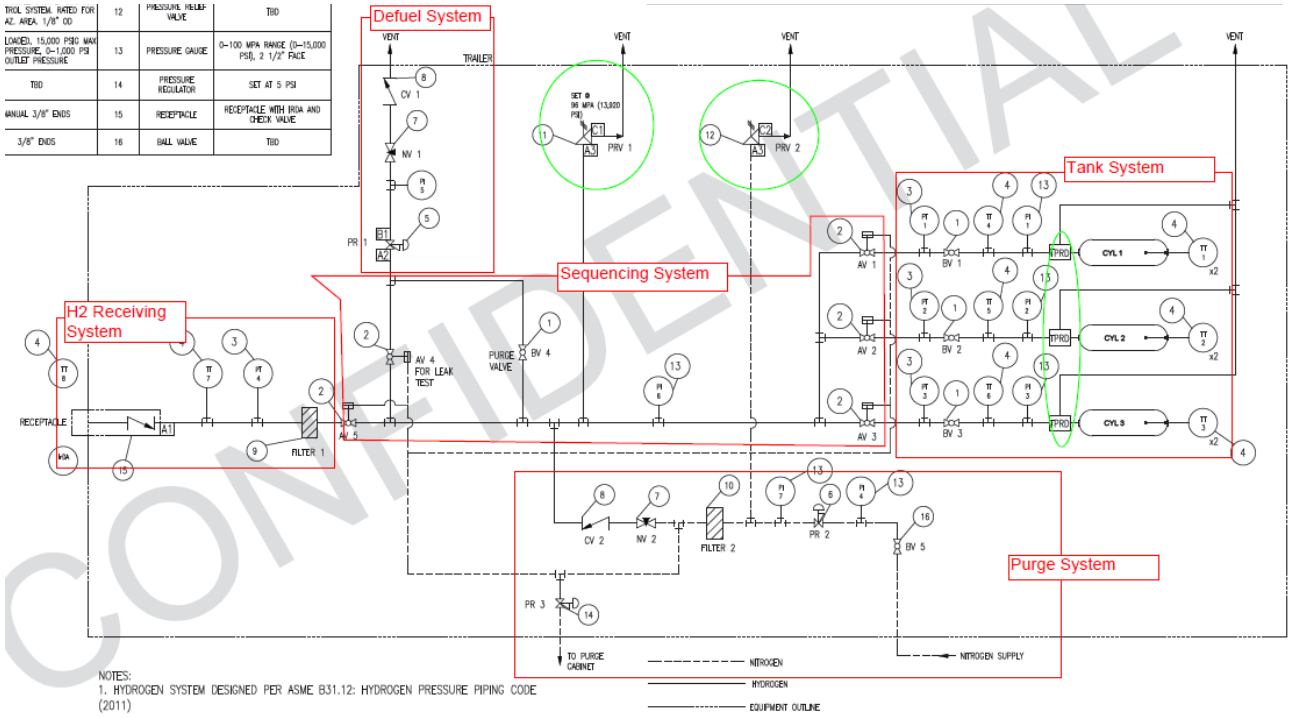

Figure 2: P&ID Drawing Showing FMEA Systems

Some design features were complete with specified hardware or software, while other design features were currently in conceptual or developmental stages. However, in the system model developed for this analysis, no distinction was made for each item's maturity of design; each item was modeled based on its intended function.

3.1.1.1 Boundary Conditions

All the systems contained within the dotted line of the block diagram (Figure 1) are contained within the HyStEP device. Blocks that are shown outside of this boundary are external to the device and are only included to represent external inputs. The FMEA was conducted only on the systems inside the dotted line, which represents the system boundary. There is one exception to this, which is the "Vent to Atmosphere" which was included as part of the defuel system.

3.1.2 FMEA Type

There are several different models on which to base a FMEA. Each model is based on a different recognized standard. The most common FMEA types (standards) are:

1. MIL-STD-1629A
2. SAE ARP 5580
3. SAE J1739

This FMEA followed the Design FMEA (DFMEA) section of SAE J1739:2009. The DFMEA was facilitated by Intertek Consulting and was undertaken by Powertech Labs and the HyStEP Project Team.

3.2 Analysis Definitions

The following sections define the ground rules for the specific analysis steps used to develop this FMEA.

3.2.1 Function Definition

Component functions were defined in the development of the functional model for the demonstration system and were used as defined. An important consideration is that failure to define all of the functions is likely to result in an incomplete list of the failure modes. A list of the output functions and control factors for each system is shown below.

Table 1: Functional Analysis

Component / Process	Output Function (y_i):		Control Factors (x_i)	
H2 Receiving System	1	Connection to H2 dispenser nozzle	1	Receptacle meets SAE J2600 (H70)
	2	Unidirectional Hydrogen Passage from Nozzle	1	Use of qualified components (ASME B31.12)
			2	H2 Receiving pressure < Nozzle pressure
			3	Check Valve in receptacle
	3	Temperature Measurement (+/- 1°C)	1	T-type thermocouple
	4	Pressure Measurement (0.1% FS)	1	Pressure Sensor (0-100 MPa range)
	5	Hydrogen particulate quality (<5 µm)	1	Particulate filter with 5 µm element
	6	Hydrogen passage to Sequencing System	1	Use of qualified components (ASME B31.12)
	7	Contain Hydrogen	1	Use of qualified components (ASME B31.12)
Sequencing System	1	Hydrogen passage from H2 Receiving System	1	Valve open from H2 Receiving System
			2	Use of qualified components (ASME B31.12)
			3	H2 Receiving pressure > Sequencing pressure
	2	Bi-direction gas flow to/from Tank System	1	Valve(s) open to/from Tank System
			2	Use of qualified components (ASME B31.12)
			3	Appropriate pressure differential between systems
	3	Gas passage to Defuel System	1	Valve open to Defuel System
			2	Use of qualified components (ASME B31.12)
	4	Pressure Indication to control panel	1	Pressure gauges for visual reference
	5	Prevent over pressurization	1	PRV
	6	Contain Hydrogen	1	Use of qualified components (ASME B31.12)
Tank System	1	Gas passage to/from Sequencing System	1	Use of qualified components (ASME B31.12)
			2	Appropriate pressure differential between systems
	2	Store gas (up to 70 MPa NWP, 87.5 MAWP)	1	Tanks meet testing requirements (eg. NGV 2, SAE 2759)
	3	Ability to test all SAE J2601 tank capacity ranges	1	3 tanks, ~3kg capacity each

	4	In-line Temperature Measurement (+/- 1°C)	1	T-type thermocouples
	5	In-tank Temperature Measurement (+/- 1°C)	1	T-type thermocouples (dual element probes)
	6	Pressure Measurement (0.1% FS)	1	Pressure Sensors (0-100 MPa range)
	7	Vent tanks in case of fire	1	TPRD
	8	Pressure Indication to control panel	1	Pressure gauges for visual reference
Defuel System	**1**	Unidirectional Controlled gas exhaust to atmosphere	1	Use of qualified components (ASME B31.12)
			2	Regulated gas pressure
			3	Flow rate controlled by operator
			4	Check Valve at vent
	2	Safe location for exhaust gas	1	Vent stack located away from device and dispenser
	3	Contain Hydrogen	1	Use of qualified components (ASME B31.12)
	4	Pressure Indication	1	Pressure gauge for visual reference
	5	Prevent over pressurization	1	PRV
Purge System	**1**	Connection to purge gas supply tank	1	Fitting connection for nitrogen T-cylinder
	2	Unidirectional purge gas passage to Sequencing System	1	Use of qualified components
			2	Purge gas pressure > Sequencing System pressure
			3	Check Valve
	3	Controlled flow of purge gas into the system	1	Flow rate controlled by operator
	4	Particulate filtration	1	Filter
	5	Pressure Indication	1	Pressure gauges for visual reference
	6	Contain Purge Gas	1	Use of qualified components (ASME B31.12)
	7	Prevent over pressurization	1	PRV
Control System	**1**	Operator Interface suitable for Class 1, Div 2	1	Touch Screen HMI (Class 1, Div 2)
			2	Control Panel (manually operated valves)
			3	Pressure gauges for visual reference
	2	Sensor Inputs (Class 1, Div 2)	1	DAQ - Thermocouple module
			2	DAQ - Analog Input module (pressure sensors, H2 sensors)
			3	DAQ - Digital Input module
	3	Valve control of Sequencing System	1	DAQ - Digital Output module
			2	Electric to Pneumatic Valves
	4	IRDA signals to Dispenser nozzle	1	IR transmitter at Receptacle
			2	DAQ communication interface
	5	Data collection, processing, logic control	1	DAQ controller
			2	Programmed Logic (DAQ Software)
			3	Mode of operation from operator
Data Report	**1**	Electronic File of relevant data in prescribed format	1	Processed data from DAQ system
			2	Electronic Data Storage

3.2.2 Failure Mode Identification Criteria

The failure mode describes how an item could fail to perform its previously defined function. It can be difficult at this stage to differentiate between a failure mode of the function, the effect of the failure mode of the function, or the cause of the failure mode. An effective strategy is to express the failure mode as the negative of the function.

Some failure mode criteria used included:

- Only single failure modes were considered.
  - No interactions between multiple valves or other system devices were assumed to occur.
- Interface failures, such as tubing, fittings, wiring, solder, etc., cause no new failure mode over and above those caused by the parts to which they interface.

3.2.3 Failure Effects

The failure mode effects describe the consequences of the failure mode. Effects can focus on local/immediate effects or global/system effects. Some FMEA standards divide effects into categories such as local effects, next effects, and end effects. For simplicity, this FMEA focused on potential end effects only.

3.2.4 Severity Classifications

The severity is a measure of the seriousness of the effect of the failure mode. Severity classifications are assigned to provide a qualitative measure of the worst possible consequences resulting from a failure. Typically, scales are assigned to predetermined loss criteria.

Severity classifications used for this analysis were included in a worksheet provided by Intertek Consulting and are shown below in Table 2 and 3. For this analysis, two different severity tables were provided to account for the variety of failure effects in this analysis.

Table 2: Severity Scale Option 1

Rating	Severity	Customer Description
10	**Hazardous Effect Without Warning**	Very hazardous effect. Effect occurs suddenly without warning to user and may pose a safety concern. Non-compliance with regulatory requirements is likely.
9	**Hazardous Effect With Warning**	Potentially hazardous effect with safety concerns. Able to halt product operation without mishap, i.e., gradual failure. Compliance with significant regulatory requirements is in jeopardy.
8	**Serious Effect**	Product is inoperable but safe, or a system is inoperable but safe. Customer dissatisfaction is very substantial and likely provokes anger.
7	**Major Effect**	Product performance is severely degraded but has some operational capability and remains safe. A subsystem may be inoperable, and customer is significantly dissatisfied and is likely angry.

6	**Significant Effect**	Customer experiences discomfort. Product performance is degraded but operable and safe, or a non-vital part is inoperable. Customer experiences frustration and perhaps anger.
5	**Moderate Effect**	Moderate degradation of product performance; Non-vital fault often requires repair and customer dissatisfaction is significant.
4	**Minor Effect**	Minor degradation of product performance that generally does not require repair. Non-vital fault noticed by 95% or more of customers resulting in minor irritation.
3	**Slight Effect**	Slight degradation of product performance. Non-vital fault noticed by median customer with inconsequential annoyance.
2	**Very Slight Effect**	Very slight degradation of product performance. Non-vital fault noticed by discriminating customer with negligible annoyance.
1	**No Effect**	No discernible effect.

Table 3: Severity Scale Option 2

Rating	Severity	Customer Description	Process Description	General Comments
9	**Hazardous**	The product may pose a Life Threatening, Grievous, Serious, or Minor Injury hazard during its entire life cycle (manufacture through disposal). Safety failure can occur with or without warning. (Severity '9' is to be used for Safety Failure Modes only)	The product may pose a Life Threatening, Grievous, Serious, or Minor Injury hazard during its entire life cycle (manufacture through disposal). Safety failure can occur with or without warning. (Severity '9' is to be used for Safety Failure Modes only)	Cannot begin production without completing risk assessment. May not be able to use or sell the product without completing risk assessment.
7	**Product Exchange**	Customers will be extremely dissatisfied. Product inoperable. Loss of primary function. Product unavailable because non-compliance with regulatory requirements. The risk of property damage may exist during use, handling or installation of the product.	100% of product may have to be scrapped. Product will have repair time of greater then 1 hour. The risk of property damage may exist during use, handling or installation of the product.	Major SIR machine repair (>45 minutes), may return the product, will not buy a product based on floor demonstration models
5	**Service Call**	Customers will be dissatisfied. Product operable but at reduced level of performance.	Portion may have to be scrapped with no sorting or repair time of less then 0 .5 to 1 hour.	May be a service call, will tell friends, may not buy another product, or would like a change to the product.
3	**Minimal**	Customers will see and may be slightly annoyed. (Fit, Finish, Squeak, Rattle) Noticed by 50% of customers.	Minor disruption to production line. Portion may have to be re-worked.	May tell friends, might suggest a change to the product
1	**None**	Has no effect on the customers.	No effect	Will not be noticed

3.2.5 Occurrence Classifications

Occurrence is often expressed as a qualitative or quantitative probability of failure mode occurrence. Typically, scales are assigned to predetermined probability criteria. Occurrence classifications reflect the probability that a failure mode will occur during the planned life expectancy of the system. These qualitative probabilities can be described in terms of potential occurrences per unit time, events, population, items, or activity. Severity classifications used for this analysis were included in a worksheet provided by Intertek Consulting. The classification option chosen for this analysis is shown below in Table 4.

Table 4: Occurrence Scale

Rating	Occurrence	History	PPM	Range	Percent
9	**Most certain to occur**	No prevention controls. New technology; very little knowledge about factors, effects, and noises.	> 50,000	1 of 20 or more	> 5
7	**Frequency**	No prevention controls. New technology, little knowledge of factors, effects and noises.	5,000 to 50,000	1 of 200 to 1 of 20	0.5 to 5.0
5	**Occasional**	Some prevention controls. New Technology proven in other industries, Some knowledge of factors, effects and noises.	500 to 5,000	1 of 2,000 to 1 of 200	0.05 to 0.50
3	**Rare**	Strong prevention controls. Existing Technology with new application. Knowledge of many factors, effects and noises.	10 to 500	1 of 100,000 to 1 of 2,000	0.001 to 0.050
1	**Improbable**	Significant, proven prevention controls. Implemented design previously and has proven predictability.	< 10	1 of 100,000 or less	< 0.001
0	**Reserved for Severity '9' Line Item Closure in the "Action Results" Section of the FMEA form.**	The hazard has been mitigated by application of the safety hierarchy (designed out, safeguarded or process change implemented, etc.). The PHM plots in the white area of the qualitative risk assessment or other approved closure applied (i.e. Hazard Communications). The product/component conforms to applicable standards. Only to be used for safety items (severity 9) in the action results area. Indicates that safety hierarchy thinking has been applied and appropriate action led to closure. Potential follow-up items (like a design change) need to be reassessed in a separate line item in this FMEA.			

3.2.6 Detection Classifications

Detection is a qualitative measure of the probability of observing the failure mode or indications of imminent failure before advancing to the next operation, activity, or delivering a product to a customer. Typically, scales are assigned to predetermined detection probability criteria. Detection classifications reflect an assessment of the ability of existing process controls to detect a potential failure mode or cause before the failure effect can be realized.

For this analysis, two different severity tables were provided to account for the variety of potential failure effects (Table 33 and 33 below).

Table 5: Detection Scale Option 1

Rating	Detection	Criteria
1	Almost Certain	Highest effectiveness of method; detection nearly certain in all known cases (proven design standard, best practice with near-total elimination of failure, etc.)
2	Very High	Effectiveness is very high but requires discretion i.e., test history of similar parts using proven test methods or validated simulation, computation, or modeling
3	High	High level of effectiveness, such as previously verified calculation or simulation based on similar designs; degradation testing prior to design release
4	Moderately High	Effective detection based on data-driven extrapolation and/or technical judgment from testing to failure or computation, simulation, or analysis with some correlation to expected operating conditions
5	Medium	Moderate detection from testing or computation, i.e., test results from moderately similar designs or order-of-magnitude computations; pass/fail testing prior to design release
6	Low	Detection methods reveal failure modes less than half the time; degradation testing in controlled conditions
7	Slight	Available methods reveal failure modes only under optimal conditions; testing to failure after design release
8	Very Slight	Available methods require extensive judgment or extrapolation and are known to have limited capability; pass/fail testing after design release
9	Remote	Speculative, unproved, or unreliable methods of detection; virtual analysis is not correlated with expected operating conditions
10	No detection	No known effective technique or method available, or no analysis planned

Table 6: Detection Scale Option 2

Detection	Rating	Criteria
Very Remote	9	Very remote chance that the control will PREVENT or DETECT the failure mode, effect or cause. *Process example: Control is achieved with indirect of random checks only.*
Low	7	Low chance that the control will PREVENT or DETECT the failure mode, effect or cause. *Process example: Control is achieved with visual or double visual inspection only.*
Moderate	5	Moderate chance that the control will PREVENT or DETECT the failure mode, effect or cause. *Process example: Control is achieved with control charting (SPC) or is based on gauging the parts after the parts have left the station (100% go/no go gauging, variables gauging).*
High	3	High chance that the control will PREVENT or DETECT the failure mode, effect or cause. *Process example: Error detection in subsequent operations (can not accept discrepant part), gauging of set up or first piece check (set up causes only), error detection in station.*

Almost Certain	**1**	Almost certain that the control will PREVENT the failure mode or cause. *Example: Discrepant parts cannot be made because item has been error proofed by progress/product design.*
Reserved for Severity '9' Line Item Closure in the "Action Results" Section of the FMEA form.	**0**	The hazard has been mitigated by application of the safety hierarchy (designed out, safeguarded or process change implemented, etc.). The PHM plots in the white area of the qualitative risk assessment or other approved closure applied (i.e. Hazard Communications). The product/component conforms to applicable standards. Only to be used for safety items (severity 9) in the action results area. Indicates that safety hierarchy thinking has been applied and appropriate action led to closure. Potential follow-up items (like a design change) need to be reassessed in a separate line item in this FMEA.

3.2.7 Causes

Causes indicate a reason for why or how a failure mode can occur. However, all causes do not contribute equally to a potential failure mode. Only "root causes" are likely to contribute to the majority of the failure mode. These root causes were emphasized in cause determination. However, causes were not developed for all potential failure modes in this analysis.

3.3.1 Risk Priority Number

Automotive FMEAs often use Risk Priority Number (RPN) values to assess criticality. Higher RPN values are an indication of more critical items. The product of the severity, occurrence, and detection values determines the RPN. The equation for RPN is: RPN = Severity × Occurrence × Detection

3.4 FMEA Assumptions

Many of the analysis assumptions are provided in the relevant preceding sections and are summarized here for convenience.

- No distinction was made for each item's maturity of design; each item was modeled based on its intended function.
- The system analyzed included the H2 receiving system, sequencing system, tank system, defuel system, purge system, control system, and data report.
- The FMEA followed the model defined by the Design FMEA section of SAE J1739:2009 as per the FMEA worksheet provided by Intertek Consulting (who were facilitating the process).
- The FMEA emphasized analysis at the functional level, based on the defined component functions.
- The failure modes were generally defined as the negative of the function.
- The FMEA focused on potential end effects only.

4 Results and Discussion

Detailed failure modes, and effect analysis results are contained in Appendix A of this report. This shows every potential failure mode, potential effect, cause, measures for prevention, and detection. Using the values determined for severity, occurrence, and detection a risk priority number (RPN) was calculated for each failure mode. Failure modes with a RPN greater than 100 were re-addressed and actions were taken in order to reduce the RPN to a value below 100. In summary, the FMEA resulted in the following:

- 7 functional blocks were analyzed
- 44 functions were defined
- 202 failure modes and effects were identified
- Each effect was assigned severity, occurrence, and detection/prevention ratings
- 47 failure mode effects had severity of 9 or 10 indicating a safety hazard
- 20 failure mode effects had a Risk Priority Number (RPN = severity*occurrence*detection) greater than 100

4.1 Risk Priority Number Results

Components with failure modes having the highest risk priority numbers (RPN) (100 or greater) are summarized in Table 7. This table lists the RPN along with the system, function, potential failure mode, and potential effects of the failure. It also shows the RPN value after actions were taken to improve safety in that area. Note, that for the details of the severity, occurrence, and detection of each failure mode, Appendix A must be referred to.

Table 7: Table of Highest Initial RPN's

System	Function	Potential Failure Mode	Potential Effects of Failure	Initial RPN	Actions Taken	Final RPN
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	**180**	Included Heat/Fire Detection	**100**
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	**180**	Included Heat/Fire Detection. Check list item for vent stack cap for every station	**90**
H2 Receiving System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	**144**	Passive ventilation included in trailer, testing to occur with doors open (interlock)	**72**
Sequencing System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	**144**	Passive ventilation included in trailer, testing to occur with doors open (interlock)	**72**
Tank System	Contain gas (up to 70 MPa NWP, 87.5 MAWP)	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	**144**	Passive ventilation included in trailer, testing to occur with doors open (interlock)	**72**
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	**144**	Passive ventilation included in trailer, testing to occur with doors open (interlock)	**72**
Control System	Hydrogen Sensors	Incorrect H2 sensor reading	Higher level of H2 in trailer than measured	**144**	Passive ventilation included in trailer, testing to occur with doors open (interlock), redundant sensors	**72**
Control System	Proper sensor inputs (Class 1, Div 2)	Failure of explosion proof cabinet	Non rated electronics in classified area	**135**	Explosion proof panel has many bolts, very unlikely to open panel except for maintenance.	**54**
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	**135**	Several triggers to operator when targets out of bounds (APRR, SOC, IRDA signals etc.)	**81**
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	**135**	Several triggers to operator when targets out of bounds (APRR, SOC, IRDA signals etc.)	**81**
H2 Receiving System	Hydrogen particulate quality (<5 µm)	Allows >5um particles into system	Damage to downstream components (valves)	**126**	Filter installation procedure/schedule to be included. Include tamper sticker.	**72**
H2 Receiving System	Hydrogen particulate quality (<5 µm)	Allows >5um particles into system	Damage to downstream components (valves)	**126**	Filter installation procedure/schedule to be included. Include tamper sticker.	**72**
Purge System	Particulate filtration	Allows >5um particles into system	Damage to downstream components (valves)	**126**	Filter installation procedure/schedule to be included. Include tamper sticker.	**72**
Purge System	Particulate filtration	Allows >5um particles into system	Damage to downstream components (valves)	**126**	Filter installation procedure/schedule to be included. Include tamper sticker.	**72**
Control System	Valve control of Sequencing System	Valves fail open	Undesired gas transfer between systems	**120**	Limit switches added to valves	**96**
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen flow back through receptacle	Leak to atmosphere	**108**	AV5 automatic open/closed during fueling events and remains closed while not fueling	**72**

Control System	Hydrogen Sensors	Incorrect H2 sensor reading	Higher level of H2 in trailer than measured	**108**	Passive ventilation included in trailer, testing to occur with doors open (interlock). Calibration procedure to be included with operator/maintenance manual.	**54**
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Hydrogen Leakage external to trailer under dispenser canopy	**105**	Considered a low risk item - no further action. (Based on severity value, see Appendix A)	**105**
Control System	Valve control of Sequencing System	Unable to open valve(s) (Note: valves are normally closed)	Unable to transfer gas between systems	**105**	Limit switches added to valves	**84**

4.4 Summary

Overall, 202 failure mode effects were identified for the 7 functional blocks that were analyzed. Out of those, 155 were identified as being negligible in terms of severity.

Of the other 47 failure mode effects, only 20 were identified as catastrophic, based on the Risk Priority Number. For these, design changes were implemented to either decrease the severity, occurrence, or to improve the detection of the failure.

There are a number of severe failure modes which were considered, but most have a remote or improbable chance of occurring. In all cases, procedures and controls will prevent or mitigate any real risks.

5 Recommendations

Operation of the system will include a number of hazards including high pressure hydrogen, hydrogen gas leak potential, and failure of components. Procedures and both passive and active controls and safeguards will be important to insure safe operations of the system. A list of procedures and safeguards has been developed based on this analysis. Procedures are documented in the device manual. All trained operators will be required to read, understand, and follow these procedures. Safeguards will be fully tested prior to operating the system.

In response to the analysis presented above, items with high RPN values were further investigated. In all of these cases, preventive or mitigating controls or procedures were identified and implemented to insure safe operation. The second column from the right of Table 7 shows the procedure or control that will mitigate or prevent the failure mode effects.

6 Appendix A: FMEA Worksheet

See next page.

FMEA Worksheet

Intertek
Consulting

Component/ System/ Process/ Operations/ Index	Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) / Mechanism(s) of Failure	Occurrence	Current Design/ Process Control PREVENTION	Current Design/ Process Control DETECTION	Detection	RPN	Recommended Action(s)	Responsibility	Target Completion Date	Actions Taken	Severity	Occurrence	Detection	RPN
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	10	Localized fire does not activate TPRD	2	Short tank design, TPRD location	Operator inspection	9	180	Sandia's quantitative risk assesment. Consider fire/heat detection in device, if added, and depending on QRA results, revisit numbers. Comparable or less than vehicle risk. Tech val data shows zero occuurances of this in over 10 years			Included Heat/Fire Detection	10	2	5	100
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	10	Blocked vent line prevents gas from escaping after TPRD activation	2	Plastic cap on vent to prevent water/contamination ingress	Operator inspection	9	180	Sandia's quantitative risk assesment. Consider fire/heat detection in device, if added, and depending on QRA results, revisit numbers. Comparable or less than vehicle risk. Tech val data shows zero occuurances of this in over 10 years. Critical maintenance item.			Included Heat/Fire Detection. Check list item for vent stack cap for every station	10	1	9	90
H2 Receiving System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	144	Consider positive/passive ventilation of the trailer. Vent should prevent reaching LFL in a minor leak scenario. Update based on vent design.			Passive ventilation included in trailer, testing to occur with doors open (interlock)	9	2	4	72
Sequencing System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	144	Consider positive/passive ventilation of the trailer. Vent should prevent reaching LFL in a minor leak scenario. Update based on vent design.			Passive ventilation included in trailer, testing to occur with doors open (interlock)	9	2	4	72
Tank System	Contain gas (up to 70 MPa NWP, 87.5 MAWP)	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	144	Consider positive/passive ventilation of the trailer. Vent should prevent reaching LFL in a minor leak scenario. Update based on vent design.			Passive ventilation included in trailer, testing to occur with doors open (interlock)	9	2	4	72
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	144	Consider positive/passive ventilation of the trailer. Vent should prevent reaching LFL in a minor leak scenario. Update based on vent design.			Passive ventilation included in trailer, testing to occur with doors open (interlock)	9	2	4	72
Control System	Hydrogen Sensors	Incorrect H2 sensor reading	Higher level of H2 in trailer than measured	9	Sensor calibration	4	Operating, maintenance plan	Operator inspection, feedback from controls	4	144	Scheduled maintenance, take credit for ventilation			Passive ventilation included in trailer, testing to occur with doors open (interlock), redundant sensors	9	2	4	72
Control System	Proper sensor inputs (Class 1, Div 2)	Failure of explosion proof cabinent	Non rated electronics in classified area	9	Door left open	3	Operating/maintenance instructions	Operator inspection	5	135	Door open switch? Difficult to leave door open accidentally. Gathering more info that may affect rating. Physical interlock with the main disconnect is possible			Explosion proof panel has many bolts, very unlikely to open panel except for maintenance.	9	2	3	54
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	9	Failure of IR signal generator	3	IR Signal Generator credentials, robust commissioning, Device shut-downs	Feedback from dispenser, operator, in tank temp /pressure measurements, positive tank shutoff. Calculate SoC.	5	135	Site owner/operator on site? DAQ shutdown for fast pressure ramp, etc. Reduce detection numbers when SoC calculation cutoff and T/P limits are reached.			Several triggers to operator when targets out of bounds (APRR, SOC, IRDA signals etc.)	9	3	3	81
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	9	Failure of communication from DAQ control to signal generator	3	DAQ credentials, robust commissioning, device shut-downs	Feedback from dispenser, operator, in tank temp measurements, positive tank shutoff.	5	135	Site owner/operator on site? DAQ shutdown for fast pressure ramp, etc. Reduce detection numbers when SoC calculation cutoff and T/P limits are reached.			Several triggers to operator when targets out of bounds (APRR, SOC, IRDA signals etc.)	9	3	3	81
H2 Receiving System	Hydrogen particulate quality (<5 µm)	Allows >5um particles into system	Damage to downstream components (valves)	6	Filter element not installed	3	Operating instructions/procedures	Operator inspection	7	126	Filter installation procedure, detection will be improved if included. If filter is installed once, and checked at annual manitenance, then detection goes down, consider tamper evident sticker/wire			Filter installation procedure/schedule to be included. Include tamper sticker.	6	3	4	72
H2 Receiving System	Hydrogen particulate quality (<5 µm)	Allows >5um particles into system	Damage to downstream components (valves)	6	Damged filter element	3	Operating instructions/procedures	Operator inspection	7	126	Filter installation procedure, detection will be improved if included. If filter is installed once, and checked at annual manitenance, then detection goes down, consider tamper evident sticker/wire			Filter installation procedure/schedule to be included. Include tamper sticker.	6	3	4	72

Purge System	Particulate filtration	Allows >5um particles into system	Damage to downstream components (valves)	6	Filter element not installed	3	Operating instructions/procedures	Operator inspection	7	126	Filter installation procedure, detection will be improved if included, may include tamper evident/resistant housing, annual maintenance check			Filter installation procedure/schedule to be included. Include tamper sticker.	6	3	4	72
Purge System	Particulate filtration	Allows >5um particles into system	Damage to downstream components (valves)	6	Damged filter element	3	Operating instructions/procedures	Operator inspection	7	126	Filter installation procedure, detection will be improved if included, may include tamper evident/resistant housing, annual maintenance check			Filter installation procedure/schedule to be included. Include tamper sticker.	6	3	4	72
Control System	Valve control of Sequencing System	Valves fail open	Undesired gas transfer between systems	8	Control signal to solenoid failure	3	Robust commissioning	Operator inspection, Valve command displayed on screen	5	120	Consider limit switches on valves	Powertech to source limit switches for Avs		Limit switches added to valves	8	3	4	96
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen flow back through receptacle	Leak to atmosphere	9	Check valve failure	3	SAE J2600 H70 receptacle	Operator inspection	4	108	Evaluate addition of redundant check valve also note that AV5 is NC unless filling.			AV5 automatic open/closed during fueling events and remains closed while not fueling	9	2	4	72
Control System	Hydrogen Sensors	Incorrect H2 sensor reading	Higher level of H2 in trailer than measured	9	Sensor failure	3	H2 Sensor credentials	Operator inspection, feedback from controls	4	108	Scheduled maintenance, credit for ventilation can reduce numbers, also consider additional sensors			Passive ventilation included in trailer, testing to occur with doors open (interlock). Calibration procedure to be included with operator/maintenance manual.	9	2	3	54
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Hydrogen Leakage external to trailer under dispenser canopy	7	Hose or connection Failure (trailer to vent stack)	3	Hose/connection creditials, operator instructions/procedures	Operator inspection	5	105	Pressure at this point in the system is very low, and unlikely to cause a significant leak. Any leak that does happen will rapidly dissipate			Considered a low risk item - no further action.	7	3	5	105
Control System	Valve control of Sequencing System	Unable to open valve(s) (Note: valves are normally closed)	Unable to transfer gas between systems	7	Solenoid Failure	3	Solenoid credentials	Operator inspection, Valve command displayed on screen	5	105	Consider limit switches on valves	Powertech to source limit switches for Avs		Limit switches added to valves	7	3	4	84
H2 Receiving System	Temperature Measurement (+/- 1°C)	Temperature fail high	Fail to detect gas temperature that is too low causes component damage	9	Faulty thermocouple	2	Thermocouple, dispenser credentials	Operator inspection	5	90	Consider redundant thermocouples (TT 4-6), control system comparison, calibration plan			TT4-6 give redundant feedback to operator. Pre-test Inspection checklist	9	2	4	72
Control System	Proper sensor inputs (Class 1, Div 2)	Failure of explosion proof cabinent	Non rated electronics in classified area	9	Damaged door seal	2	Panel credentials, operating/maintenance instructions	Operator inspection	5	90	Door open switch?			Explosion proof panel has many bolts, very unlikely to open panel except for maintenance.	9	2	3	54
Control System	Proper sensor inputs (Class 1, Div 2)	Failure of explosion proof cabinent	Non rated electronics in classified area	9	Damaged connection seals	2	Seal credentials, installation	Operator inspection	5	90	Door open switch?			Explosion proof panel has many bolts, very unlikely to open panel except for maintenance.	9	2	3	54
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	10	TPRD Fails to activate when subjected to fire	1	TPRD credentials	Operator inspection	9	90	Sandia's quantitative risk assesment. Consider fire/heat detection in device							
H2 Receiving System	Temperature Measurement (+/- 1°C)	Temperature fail low	System Shutdown	6	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	90	Consider redundant thermocouples, control system comparison, calibration plan							
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail low	Fail to detect gas pressure that is too high - exceeds MAWP of components	7	Faulty pressure transducer	3	PT credentials	Operator inspection	4	84	Consider pressure relief valve							
H2 Receiving System	Hydrogen particulate quality (<5 µm)	Allows >5um particles into system	Damage to downstream components (valves)	6	Wrong filter element installed	2	Operating instructions/procedures	Operator inspection	7	84	Filter installation procedure, detection will be improved if included							
Purge System	Particulate filtration	Allows >5um particles into system	Damage to downstream components (valves)	6	Wrong filter element installed	2	Operating instructions/procedures	Operator inspection	7	84	Filter installation procedure, detection will be improved if included							
Defuel System	Safe location for exhaust gas	Exhaust gas in unsafe location	Explosive atmosphere in unsafe area	9	Operator placement of vent stack, improper training	3	Operating instructions/procedures	Operator inspection	3	81	Determine safe location (i.e. distance from dispenser and trailer, height, vent hose path), consultation with site owner, feedback from DMS							
Defuel System	Contain Hydrogen	Loss of containment (major leakage)	Hydrogen Leakage external to trailer under dispenser canopy	9	PRV Failure or activation	3	PRV credentials	Operator inspection	3	81	Review if PRV is required			PRV removed - determined to be required by Project Team				
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	Hydrogen flow back through check valve	Hydrogen Leakage external to trailer under dispenser canopy	9	PRV activation	3	Check valve credentials	Operator inspection	3	81				Note: PRV replaced with burst disk for improved reliability with vibration	9	3	3	81
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Noise from fast venting	8	Flow control valve open too much	5	Operating instructions/procedures	Operating Inspections, Procedures, Audible	2	80	Muffler considered on vent stack							0
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Maximum allowable defuel rates exceeded, tank liner damage	8	Flow control valve open too much	5	Operating instructions/procedures	Operating Inspections, Procedures, Audible	2	80	Solution for defueling below maximum allowable defuel rate (find out from Quantum)							
Control System	Valve control of Sequencing System	Valves fail open	Undesired gas transfer between systems	8	Solenoid Failure	2	Solenoid credentials	Operator inspection, Valve command displayed on screen	5	80	Consider limit switches on valves							0
Control System	Data collection, processing, logic control	Data processed incorrectly	Bad data	8	DAQ hardware/software failure, programmer error	2	DAQ credentials, robust commissioning, data handling system	Data report	5	80	Consider if bad data then potentially certifying station not meeting J2601							
H2 Receiving System	Contain Hydrogen	Loss of containment (minor leakage)	Bad test results	5	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	80								
Sequencing System	Contain Hydrogen	Loss of containment (minor leakage)	Bad test results	5	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	80								
Tank System	Contain gas (up to 70 MPa NWP, 87.5 MAWP)	Loss of containment (minor leakage)	Bad test results	5	Component Leak	4	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	80								

H2 Receiving System	Temperature Measurement (+/- 1°C)	Temperature fail high	Bad data	5	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	75	Consider redundant thermocouples, control system comparison, calibration plan							0
H2 Receiving System	Temperature Measurement (+/- 1°C)	Temperature fail low	Bad data	5	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	75	Consider redundant thermocouples, control system comparison, calibration plan							
Tank System	In-tank Temperature Measurement (+/- 1°C)	Temperature fail high	Bad data	5	Faulty thermocouple	3	Thermocouple credentials, redundant thermocouple element in tank	Operator inspection, control comparison	5	75								0
Tank System	In-tank Temperature Measurement (+/- 1°C)	Temperature fail low	Bad data	5	Faulty thermocouple	3	Thermocouple credentials, redundant thermocouple element in tank	Operator inspection, control comparison	5	75								
Tank System	Contain gas (up to 70 MPa NWP, 87.5 MAWP)	Loss of containment (major leakage)	Hydrogen Leakage external to trailer under dispenser canopy	9	TPRD false trip	2	TPRD credentials	Audible	4	72								
Defuel System	Safe location for exhaust gas	Exhaust gas in unsafe location	Explosive atmosphere in unsafe area	9	Operator securement of vent stack, improper training	4	Operating instructions/procedures	Operator inspection	2	72	Determine proper securing method, stability analysis report.							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	Hydrogen flow back through check valve	Overpressurize purge system causing component failure	9	Check valve fails open	2	Check valve credentials, PRV in purge system, filtration of purge gas	Operator inspection, pressure gauge, audible if PRV activates	4	72				Note: PRV replaced with burst disk for improved reliability with vibration	9	2	4	72
Purge System	Prevent overpressurization	Overpressurization	Exceed pressure rating of purge system causing component failure	9	Check-valve failure	2	Rated components, acceptance testing, checks. All components rated for maximum T-cylinder pressure (PRV is considered for check valve failure only)	Operator inspection, pressure gauge, audible if PRV activates	4	72	Label for max inlet pressure for purge gas connection, see above for check valve failure mode			Note: PRV replaced with burst disk for improved reliability with vibration	9	2	4	72
Control System	Proper sensor inputs (Class 1, Div 2)	Sensors not suitable for Class 1, Div 2	Non rated electronics in classified area	9	Non-rated sensors installed	2	Sensor credentials, sensor connections in explosion proof panel, intrinsically safe wiring	Operator inspection , equipment list, maintenance and calibration procedures	4	72								
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Noise from fast venting	8	Failed regulator increases pressure	3	Operating instructions/procedures, secondary flow control with flow control valve downstream	Operating Inspections, Procedures, pressure indicator for operator, Audible	3	72	Muffler considered on vent stack, PRV on vent line? Analysis required for pressure drop, component rating, etc. Assumption: operator cannot set pressure too high, considerer natural pressure changes to regulator output. Review manual bypass. Is "Purge" valve required. Back-up "NV1 closed?" on HMI during activation of AV4							
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Maximum allowable defuel rates exceeded, tank liner damage	8	Failed regulator increases pressure	3	Operating instructions/procedures, secondary flow control with flow control valve downstream	Operating Inspections, Procedures, pressure indicator for operator, Audible	3	72	Solution for defueling below maximum allowable defuel rate (find out from Quantum)							
Defuel System	Controlled unidirectional gas exhaust to atmosphere	No Flow	Cannot defuel tanks, cannot transport trailer	8	Flow control valve (NV1) failed closed	3	Needle valve credentials, pre-test inspection (operating procedures), maintenance plan	Operating Inspections, Procedures	3	72								
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail high	System Shutdown	6	Faulty pressure transducer	3	PT credentials	Operator inspection	4	72	Consider redundant PTs, control system comparison, calibration plan							
H2 Receiving System	Hydrogen passage to Sequencing System	Low gas flow to sequencing system	Bad test outcome	6	Clogged Filter	4	Operating instructions/procedures	Operator inspection	3	72	Filter installation procedure, detection will be improved if included							
H2 Receiving System	Hydrogen passage to Sequencing System	Low gas flow to sequencing system	Bad test outcome	6	Obstruction in gas line	4	Operating instructions/procedures	Operator inspection	3	72								
Tank System	Pressure Measurement (0.1% FS)	Pressure fail high	System Shutdown prematurly (87.5 MPa)	6	Faulty pressure transducer	3	PT credentials	Operator inspection	4	72	Consider redundant PTs, control system comparison, calibration plan							
Control System	Supplying power to the system	No main power to control system	Device inoperable	6	Accidental disconnection of 120VAC	4	Operating procedures	Feedback from control system on display	3	72	Assumption: battery back-up for DAQ, follow-up on what battery back-up covers							0
Control System	Supplying power to the system	No main power to control system	Power loss shutdown occurs	6	Accidental disconnection of 120VAC	4	Operating procedures	Feedback from control system on display	3	72	Assumption: battery back-up for DAQ, controlled shutdown sequence							
Tank System	Pressure Measurement (0.1% FS)	Pressure fail low	Fail to detect gas pressure that is too high - exceeds MAWP of components	8	Faulty pressure transducer, pressure too high	2	PT credentials	Operator inspection	4	64	Consider redundant PTs, control system comparison (receiving PT, other tanks), calibration plan							
Defuel System	Controlled unidirectional gas exhaust to atmosphere	No Flow	Cannot defuel tanks, cannot transport trailer	8	Obstruction in gas line	2	Filtration in H2 Receiving System and Purging System	Operating Inspections, Procedures	4	64								
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown during fueling when inlet gas is <-40C	Fail to detect gas temperature that is too low causes component damage	8	Incorrect Lower Temperautre Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device shut-downs	Operator inspection	4	64	Link back to individual sensors in other systems, maintenance captured in device manual							0
Control System	System shutdown when pressure limits exceeded	System does not shutdown when pressure is >87.5 MPa	Gas pressure that is too high - exceeds MAWP of components	8	Incorrect upper pressure Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning shut-downs, PRV	Operator inspection	4	64	Link back to individual sensors in other systems, maintenance captured in device manual							0

Control System	IRDA signals to Dispenser nozzle	Loss of IRDA signal	Non-comm fueling testing only	7	Failure of IR transmitter	3	IR Transmitter credentials, robust commissioning	Feedback from dispenser, operator	3	63	Test sequence planning (ABORT command as first test)							0
Control System	IRDA signals to Dispenser nozzle	Loss of IRDA signal	Non-comm fueling testing only	7	Failure of IR signal generator	3	IR Signal Generator credentials, robust commissioning	Feedback from dispenser, operator	3	63	Test sequence planning (ABORT command as first test)							
Control System	IRDA signals to Dispenser nozzle	Loss of IRDA signal	Non-comm fueling testing only	7	Failure of communication from DAQ controls to signal generator	3	DAQ credentials, robust commissioning	Feedback from dispenser, operator	3	63	Test sequence planning (ABORT command as first test)							
Control System	System shutdown during ESD event	No shutdown when ESD button pressed	Overpressure, temperatures too high/low, H2 leaks	10	ESD button sticking	2	ESD button credentials, maintenance plan	ESD check as part of operating procedures	3	60	ESD shutdown procedure							
Control System	System shutdown during ESD event	No shutdown when ESD button pressed	Overpressure, temperatures too high/low, H2 leaks	10	Water infiltration bridging ESD contacts	2	ESD button credentials/enclosure/installation, maintenance plan	ESD check as part of operating procedures	3	60								
Control System	System shutdown during ESD event	No shutdown when ESD command from DAQ system	Overpressure, temperatures too high/low, H2 leaks	10	DAQ failure	2	DAQ credentials, robust commissioning	Feedback from control system on display	3	60	Watchdog timer, heartbeat (control health status), communcation loss shutdowns?			cDAQ Health Check included in Alarm Matrix	10	2	3	60
Control System	System shutdown during ESD event	No shutdown when H2 sensors alarm	Overpressure, temperatures too high/low, H2 leaks	10	H2 Sensor failure	2	H2 Sensor credentials, robust commisioning	Feedback from control system on display	3	60								
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail high	Bad data	5	Faulty pressure transducer	3	PT credentials	Operator inspection	4	60	Consider redundant PTs, control system comparison, calibration plan							0
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail low	Bad data	5	Faulty pressure transducer	3	PT credentials	Operator inspection	4	60	Consider redundant PTs, control system comparison, calibration plan							
Tank System	Pressure Measurement (0.1% FS)	Pressure fail high	Bad data	5	Faulty pressure transducer	3	PT credentials	Operator inspection	4	60	Consider redundant PTs, control system comparison, calibration plan							0
Tank System	Pressure Measurement (0.1% FS)	Pressure fail low	Bad data	5	Faulty pressure transducer	3	PT credentials	Operator inspection	4	60	Consider redundant PTs, control system comparison (receiving PT, other tanks), calibration plan							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	Low gas flow to sequencing system	Slow purging	5	Clogged Filter	4	Operating instructions/procedures	Operator inspection	3	60	Filter installation procedure, detection will be improved if included							
Control System	Proper sensor inputs (Class 1, Div 2)	Sensors not properly installed	Inaccurate measurements or no measurements, bad data	5	Installation/maintenance error, incorrect wiring	3	Sensor credentials, robust comissioning	Operator inspection, control comparison	4	60	Link back to individual sensors in other systems, maintenance captured in device manual							0
Control System	Proper sensor inputs (Class 1, Div 2)	Sensor inputs wrong scale	Inaccurate measurements or no measurements, bad data	5	Installation/maintenance error	3	Sensor credentials, robust comissioning	Operator inspection, control comparison	4	60	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	Proper sensor inputs (Class 1, Div 2)	Sensors not calibrated	Inaccurate measurements or no measurements, bad data	5	Installation/maintenance error, incorrect wiring	3	Sensor credentials, robust comissioning	Operator inspection, control comparison	4	60	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	Proper sensor inputs (Class 1, Div 2)	Sensors do not meet electrical specifications (24VDC, 4-20 mA)	Inaccurate measurements or no measurements, bad data	5	Installation/maintenance error	3	Sensor credentials, robust comissioning	Operator inspection, control comparison	4	60	Link back to individual sensors in other systems, maintenance captured in device manual							
Tank System	In-line Temperature Measurement (+/- 1°C)	Temperature fail high	Bad data	4	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	60	Control system comparison, calibration plan, Determine how warning/alarm processed by controls. Assumption is these sensors not used for control.							0
Tank System	In-line Temperature Measurement (+/- 1°C)	Temperature fail low	Bad data	4	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	60	Control system comparison, calibration plan, Determine how warning/alarm processed by controls. Assumption is these sensors not used for control.							
Tank System	Gas passage to/from Sequencing System	No hydrogen flow to sequencing system	Not able to defuel tanks	7	Obstruction in gas line	2	Filtration in H2 Receiving System and Purging System	Operating Inspections, Procedures	4	56								
Tank System	Gas passage to/from Sequencing System	No hydrogen flow from sequencing system	Not able to test	7	Obstruction in gas line	2	Filtration in H2 Receiving System and Purging System	Operating Inspections, Procedures	4	56								
Tank System	Gas passage to/from Sequencing System	No nitrogen flow to/from sequencing system	Not able to purge tanks	7	Obstruction in gas line	2	Filtration in H2 Receiving System and Purging System	Operating Inspections, Procedures	4	56								
Purge System	Contain purge gas	Loss of containment (major leakage)	Purge gas leakage external to trailer under dispenser canopy	7	Hose or connection Failure	4	Hose/connection creditials, operator instructions/procedures	Operator inspection, Audible	2	56	Review N2 source and installed locatation							
H2 Receiving System	Connection to H2 dispenser nozzle	Loose Connection	Hydrogen Leakage	9	Damage,defect or obstruction to nozzle/receptacle	2	SAE J2600 H70, protected during transport, plastic cap	Operator detects audible leak or dispenser leak detection	3	54								
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank damage	9	Localized fire does not activate TPRD	2	Short tank design, TPRD location	Operator inspection	3	54	Sandia's quantitative risk assesment. Consider fire/heat detection in device							
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank damage	9	Blocked vent line prevents gas from escaping after TPRD activation	2	Plastic cap on vent to prevent water/contamination ingress	Operator inspection	3	54	Sandia's quantitative risk assesment. Consider fire/heat detection in device							

Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Ignition of hydrogen at vent stack	9	Flow control valve open too much plus ignition event	3	Operating instructions/procedures, vent stack design, placement, stability	Operating Inspections, Procedures, Audible	2	54				CGA Vent stack considerations				
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Ignition of hydrogen at vent stack	9	Failed regulator increases pressure plus ignition event	2	Operating instructions/procedures, secondary flow control with flow control valve downstream, vent stack design, placement, stability	Operating Inspections, Procedures, pressure indicator for operator, Audible	3	54				CGA Vent stack considerations				
Defuel System	Contain Hydrogen	Loss of containment (major leakage)	Hydrogen Leakage external to trailer under dispenser canopy	9	Hose or connection Failure (trailer to vent stack)	2	Hose/connection creditials, operator instructions/procedures	Operator inspection, Audible	3	54								
Control System	System shutdown during ESD event	ESD circuit shuts down when not required	Prevent testing	6	Operator error (ESD button pushed)	3	Operator training	Feedback from control system on display	3	54	Software acknoledgment							
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Reverse flow	Allows air into defuel system causing gas mixure	3	Failed check valve	2	Check valve credentials	None	9	54	Is check valve required? Check valve included in quick-connect? Assumption: pressure downstream when mixed with 1 atm air reduces level below explosion limit and pushed out of vent stack.							
Defuel System	Controlled unidirectional gas exhaust to atmosphere	No Flow	Cannot defuel tanks, cannot transport trailer	8	Regulator fails, no regulated pressure	2	Regulator credentials, operating instructions/procedures	Operating Inspections, Procedures, pressure gauge	3	48								
Control System	Valve control of Sequencing System	Valves fail open	Undesired gas transfer between systems	8	Wrong connection of air supply to valves	2	Robust commissioning, valve/hose identification	Operator inspection, Valve command displayed on screen	3	48	Maintenance manual							
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown during defueling when tank gas is <-40 C	Fail to detect gas temperature that is too low causes component damage	8	Incorrect Lower Temperautre Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device warning and shut-downs	Operator inspection, feedback from controls	3	48	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown during defueling when tank gas is <-40 C	Fail to detect gas temperature that is too low, tank liner damage	8	Incorrect Lower Temperautre Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device warning and shut-downs	Operator inspection, feedback from controls	3	48	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown when tank gas is >85 C	Fail to detect gas temperature that is too high, tank liner damage	8	Incorrect upper Temperautre Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device warning and shut-downs	Operator inspection, feedback from controls	3	48	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	Prevent uncontrollable flow between tanks	Uncontrolled gas transfer between tanks	Excced allowable defuel rate, temperature swings in tanks	8	Incorrect tank pressure differential Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device alarms, tank temperature alarms	Operator inspection, audible	3	48	Link back to individual sensors in other systems, maintenance captured in device manual							
Control System	Supplying power to the system	Loss of 24 VDC power	ESD Shutdown mode, system inoperable	8	24VDC Power supply fails	2	Power supply credentials	Blank screen	3	48								
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail low	False indication of leak	4	Faulty pressure transducer	3	PT credentials	Operator inspection	4	48	Consider redundant PTs, control system comparison, calibration plan							
Tank System	Pressure Measurement (0.1% FS)	Pressure fail low	False indication of leak	4	Faulty pressure transducer	3	PT credentials	Operator inspection	4	48	Consider redundant PTs, control system comparison, calibration plan							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Filter clogged	3	Filter credentials, operating instructions/procedures	Operator inspection	2	42	Filter installation procedure, detection will be improved if included							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Check valve fails closed	2	Check valve credentials, operating instructions/procedures	Operator inspection	3	42								
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Obstruction in gas line	2	Operating instructions/procedures	Operator inspection	3	42								
Purge System	Contain purge gas	Loss of containment (major leakage)	Purge gas leakage external to trailer under dispenser canopy	7	PRV Failure or activation	3	PRV credentials	Operator inspection, audible	2	42								
Control System	Data collection, processing, logic control	No data collection	Loss of test results	7	DAQ hardware/software failure	2	DAQ credentials, robust commissioning, data handling system	Control feedback, data report	3	42	Determine feedback loop to operator							0
Data Report	Provide Electronic File of relevant data in prescribed format	No electronic file	No data report available	7	File not saved properly	2	DAQ credentials, robust commissioning, data handling system	Control feedback, data report checks	3	42	Note: hardcopy/printer to be discussed in Design review (rated area, etc)							
Data Report	Provide Electronic File of relevant data in prescribed format	No electronic file	No data report available	7	File corrupted	2	DAQ credentials, robust commissioning, data handling system	Control feedback, data report checks	3	42								
Data Report	Provide Electronic File of relevant data in prescribed format	No electronic file	No data report available	7	Insufficient storage space	2	DAQ credentials, robust commissioning, data handling system, size of storage and operator downloading instructions	Control feedback, data report checks	3	42								
Purge System	Contain purge gas	Loss of containment (minor leakage)	Waste of purge gas	2	Component Leak	3	Rated components, acceptance testing, checks	Operator inspection,	7	42								0

H2 Receiving System	Contain Hydrogen	Loss of containment (major leakage)	Explosive atmosphere inside trailer	10	Component Rupture	2	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	2	40	Assume that leak is detected after occurance in time for safe shutdown, consider appropriate sensor placement and flow path							
Sequencing System	Contain Hydrogen	Loss of containment (major leakage)	Explosive atmosphere inside trailer	10	Component Rupture	2	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	2	40								
Tank System	Contain gas (up to 70 MPa NWP, 87.5 MAWP)	Loss of containment (major leakage)	Explosive atmosphere inside trailer	10	Component Rupture	2	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	2	40								
Defuel System	Pressure Indication	Pressure fail low	Regulated defuel pressure set higher than expected	5	Damaged/defective gauge	2	Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction	Operator inspection	4	40								
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	Hydrogen flow back through check valve	Hydrogen mixing with purge gas	5	Check valve fails open	2	Check valve credentials, Purge system components rated for hydrogen use	Operator inspection, pressure gauge, audible if PRV activates	4	40								
Defuel System	Contain Hydrogen	Loss of containment (major leakage)	Explosive atmosphere inside trailer	10	Component Rupture	2	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	2	40								
Control System	System shutdown during ESD event	ESD circuit shuts down when not required	Prevent testing	6	ESD circuit failure	2	ESD circuit credentials, robust comissioning	Feedback from control system on display	3	36								
Control System	Supplying power to the system	No main power to control system	Device inoperable	6	Fuse blown	2	Fuse sized appropriately, fuse credentials	Feedback from control system on display	3	36	Assumption: battery back-up for DAQ, follow-up on what battery back-up covers							
Control System	Supplying power to the system	No main power to control system	Device inoperable	6	Facility power outage	2	None	Feedback from control system on display	3	36	Assumption: battery back-up for DAQ, follow-up on what battery back-up covers							
Control System	Supplying power to the system	No main power to control system	Power loss shutdown occurs	6	Fuse blown	2	Fuse sized appropriately, fuse credentials	Feedback from control system on display	3	36	Assumption: battery back-up for DAQ, controlled shutdown sequence							
Control System	Supplying power to the system	No main power to control system	Power loss shutdown occurs	6	Facility power outage	2	None	Feedback from control system on display	3	36	Assumption: battery back-up for DAQ, controlled shutdown sequence							
Control System	Supplying power to the system	Loss of 24 VDC power	ESD Shutdown mode, system inoperable	6	Fuse blown	2	Fuse sized appropriately, fuse credentials	Blank screen	3	36								
Data Report	Provide Electronic File of relevant data in prescribed format	File in wrong format	Loss of productivity - operator tries to sort out data	6	Programming error	2	DAQ credentials, robust commissioning, data handling system	Control feedback, data report checks	3	36								
Data Report	Provide Electronic File of relevant data in prescribed format	File in wrong format	Loss of productivity - operator tries to sort out data	6	File corrupted	2	DAQ credentials, robust commissioning, data handling system	Control feedback, data report checks	3	36								
Defuel System	Prevent overpressurization	Overpressurization of defuel/vent components	Exceed rating of defuel/vent components causing component damage	9	Failure of pressure regulator with defuel valve open and blockage in vent line	1	PRV downstream of regulator	Operator inspection, pressure gauge, audible if PRV activates	4	36	Review if PRV is required (see above). Assumption: operator cannot exceed recommended regulated pressure.			Note: PRV removed from Defuel System (rated components up to vent stack)				
Purge System	Contain purge gas	Loss of containment (major leakage)	Waste of purge gas, oxygen displacement in trailer	9	Component Rupture	2	Rated components, acceptance testing, checks, trailer ventilation	Operator inspection, Audible	2	36								
Control System	Touch screen to provide operator Interface suitable for Class 1, Div 2	Touch screen not suitable for Class 1, Div 2	Non rated electronics in classified area	9	Non-rated display installed	1	Touch Screen credentials	Design, equipment list	4	36	Include Touch Screen classification in device manual							
Control System	Valve control of Sequencing System	Unable to open valve(s) (Note: valves are normally closed)	Unable to transfer gas between systems	7	Loss of air supply	5	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	35								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen from Tank System	Not able to test or defuel tanks	8	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	32								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen from Tank System	Not able to test or defuel tanks	8	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	32								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen from Tank System	Not able to test or defuel tanks	8	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	32								
Tank System	In-tank Temperature Measurement (+/- 1°C)	Temperature fail high	Fail to detect gas temperature that is too low causes component damage	8	Faulty thermocouple, cold gas	2	Thermocouple credentials, redundant thermocouple element in tank	Control comparison, alarm/shutdown sequence	2	32	Alarm/shutdown sequence TBD							
Tank System	In-tank Temperature Measurement (+/- 1°C)	Temperature fail low	Fail to detect gas temperature that is too high causes component damage	8	Faulty thermocouple, hot gas	2	Thermocouple credentials, redundant thermocouple element in tank	Control comparison, alarm/shutdown sequence	2	32	Alarm/shutdown sequence TBD							
Purge System	Pressure Indication	Pressure fail low	Regulated purge pressure set higher than expected	4	Damaged/defective gauge	2	Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction	Operator inspection	4	32								
Purge System	Pressure Indication	Pressure fail null	Lack of confidence in pressure reading	4	Damaged/defective gauge	2	Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction	Operator inspection	4	32								
H2 Receiving System	Temperature Measurement (+/- 1°C)	Temperature fail null	Bad data	5	Faulty thermocouple	3	Thermocouple credentials	Control System flag	2	30	Determine how this this processed by controls.							
H2 Receiving System	Pressure Measurement (0.1% FS)	Pressure fail null	Bad data	5	Faulty pressure transducer	3	PT credentials	Control System flag	2	30	Determine how this this processed by controls.							
Tank System	In-tank Temperature Measurement (+/- 1°C)	Temperature fail null	Bad data	5	Faulty thermocouple	3	Thermocouple credentials, redundant thermocouple element in tank	Control System flag	2	30								

Tank System	Pressure Measurement (0.1% FS)	Pressure fail null	Bad data	5	Faulty pressure transducer	3	PT credentials	Control System flag	2	30	Determine how this this processed by controls.							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	Low gas flow to sequencing system	Slow purging	5	Obstruction in gas line	2	Operating instructions/procedures	Operator inspection	3	30								
Control System	System alarms when Temperature Limits exceeded	System does not alarm when any sensor <-40C or >85C	Operator not alerted to potential temperature sensor problem	5	Incorrect upper/lower Temperautre Limit Setpoints, signal output fails (Digital output module)	2	DAQ credentials, robust commissioning, device alarms	Operator inspection	3	30	Link back to individual sensors in other systems, maintenance captured in device manual							
H2 Receiving System	Connection to H2 dispenser nozzle	Stuck Connection (frozen)	Cannot remove nozzle	7	High ambient moisture, back to back fills	4	SAE J2600 H70, protected during transport, plastic cap	Operator inspection	1	28								
Sequencing System	Hydrogen passage from H2 Receiving System	No flow of gas from Receiving system	Not able to test	7	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	28								0
Sequencing System	Hydrogen passage from H2 Receiving System	No flow of gas from Receiving system	Not able to test	7	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	28								
Sequencing System	Hydrogen passage from H2 Receiving System	No flow of gas from Receiving system	Not able to test	7	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	28								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen to Tank System	Not able to test	7	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	28								0
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen to Tank System	Not able to test	7	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	28								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen to Tank System	Not able to test	7	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	28								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of nitrogen to/from Tank System	Not able to purge tanks	7	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	28								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of nitrogen to/from Tank System	Not able to purge tanks	7	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	28								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of nitrogen to/from Tank System	Not able to purge tanks	7	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	28								
Purge System	Connection to purge gas supply tank	No connection	No purging	7	No nitrogen supply on site or delivered	4	Operator training, test planning	Operator inspection	1	28	Check TDG requirements, etc. Nitrogen on-board v. delivered.							
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Ball valve fails closed	2	Ball valve credentials, operating instructions/procedures	Operator inspection	2	28								0
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Regulator fails	2	Regulator credentials, operating instructions/procedures	Operator inspection	2	28								
Purge System	Controlled unidirectional Purge gas passage to Sequencing System	No gas flow to sequencing system	No purging possible	7	Needle Valve fail closed	2	Needle valve credentials, operating instructions/procedures	Operator inspection	2	28								
H2 Receiving System	Connection to H2 dispenser nozzle	Loose Connection	Nozzle pop-off	9	Operator Error	3	Operator training	Operator inspection	1	27								
Sequencing System	Contain Hydrogen	Loss of containment (major leakage)	Hydrogen Leakage external to trailer under dispenser canopy	9	PRV Failure	1	PRV credentials	None	3	27	System conrols shutdown below PRV set pressure				Note: PRV removed from Sequencing system as determined by Project Team			
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank damage	9	TPRD Fails to activate when subjected to fire	1	TPRD credentials	Operator inspection	3	27	Sandia's quantitative risk assesment. Consider fire/heat detection in device							
Control System	Hydrogen Sensors	No H2 sensor reading	Explosive concentration in trailer with no hydrogen detection	9	H2 Sensor loose connection	3	Monitored by dection panel causing alarm condition, trailer vent	Supervised Input	1	27	Sensor shutdown plan				Shutdown plan included in Alarm Matrix			
H2 Receiving System	Connection to H2 dispenser nozzle	No connection	No fueling	8	Operator Error	3	Operator training	Operator inspection	1	24								
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen not able to pass through receptacle	No hydrogen flow	8	Pressure too high in Receiving System	3	Operator training	Operator inspection	1	24								
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen from Tank System	Not able to test or defuel tanks	8	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	24	Add to main P&ID							
Control System	Touch screen to provide operator Interface suitable for Class 1, Div 4	Touch screen inoperable	Operator unable to interact with control system, no further testing	8	DAQ hardware/software failure	3	DAQ hardware credentials, robust commissioning	Operator inspection	1	24								
Tank System	In-line Temperature Measurement (+/- 1°C)	Temperature fail null	Bad data	4	Faulty thermocouple	3	Thermocouple credentials	Control System flag	2	24	Determine how warning/alarm processed by controls.							
Sequencing System	Pressure Indication to control panel	Pressure fail high	Lack of confidence in digital pressure	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								0
Sequencing System	Pressure Indication to control panel	Pressure fail low	Lack of confidence in digital pressure	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								
Sequencing System	Pressure Indication to control panel	Pressure fail null	Lack of confidence in digital pressure, operator to replace gauge	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								
Tank System	Pressure Indication to control panel	Pressure fail high	Lack of confidence in digital pressure	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								0
Tank System	Pressure Indication to control panel	Pressure fail low	Lack of confidence in digital pressure	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								
Tank System	Pressure Indication to control panel	Pressure fail null	Lack of confidence in digital pressure, operator to replace gauge	3	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	24								

H2 Receiving System	Hydrogen passage to Sequencing System	No gas flow to sequencing system	No testing possible	7	Clogged Filter	3	Operating instructions/procedures	Operator inspection	1	21	Filter installation procedure, detection will be improved if included							0
H2 Receiving System	Hydrogen passage to Sequencing System	No gas flow to sequencing system	No testing possible	7	Obstruction in gas line	3	Operating instructions/procedures	Operator inspection	1	21								
Sequencing System	Hydrogen passage from H2 Receiving System	No flow of gas from Receiving system	Not able to test	7	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	21	Add to main P&ID							
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of hydrogen to Tank System	Not able to test	7	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	21	Add to main P&ID							
Sequencing System	Bi-direction gas flow to/from Tank System	No flow of nitrogen to/from Tank System	Not able to purge tanks	7	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	21	Add to main P&ID							
Purge System	Connection to purge gas supply tank	No connection	No purging	7	Operator Error	3	Operator training	Operator inspection	1	21								
Defuel System	Pressure Indication	Pressure fail null	Lack of confidence, no readout	5	Damaged/defective gauge	2	Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction	Operator inspection	2	20								
H2 Receiving System	Connection to H2 dispenser nozzle	Loose Connection	Nozzle pop-off	9	Damage,defect or obstruction to nozzle/receptacle	2	Dispenser Leak Check	Operator inspection	1	18								
Purge System	Connection to purge gas supply tank	Connection to wrong supply gas	Improper gas entering device	9	Connected to non-nitrogen gas supply	1	Connector designed for N2 (inert gas) T-cylinder	Operator inspection	2	18								
Control System	Hydrogen Sensors	No H2 sensor reading	Explosive concentration in trailer with no hydrogen detection	9	H2 Sensor power failure	2	Monitored by dection panel causing alarm condition, trailer vent	Supervised Input	1	18	Sensor shutdown plan			Shutdown plan included in Alarm Matrix				
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Tank temperature to cold, liner damage	8	Flow control valve open too much	2	Controlled stop/shutdown if any in-tank sensors <-40 C	Operating Inspections, Procedures, Audible, Control system detection	1	16								
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Tank temperature to cold, liner damage	8	Failed regulator increases pressure	2	Controlled stop/shutdown if any in-tank sensors <-40 C	Operating Inspections, Procedures, pressure indicator for operator, Audible, control system detection	1	16								
Control System	Touch screen to provide operator Interface suitable for Class 1, Div 2	Touch screen inoperable	Operator unable to interact with control system, no further testing	8	Faulty/damaged display	2	Touch Screen credentials, laptop backup	Operator inspection	1	16	Review using laptop in classified area							0
Control System	Touch screen to provide operator Interface suitable for Class 1, Div 3	Touch screen inoperable	Operator unable to interact with control system, no further testing	8	Connection to DAQ system failed	2	Connection cable credentials, laptop backup	Operator inspection	1	16								
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel	4	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	16								0
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel	4	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	16								
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel	4	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	16								
Defuel System	Pressure Indication	Pressure fail high	Regulated defuel pressure set lower than expected	2	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	16								0
Purge System	Pressure Indication	Pressure fail high	Regulated purge pressure set lower than expected	2	Damaged/defective gauge	2	Gauge credentials, calibration check plan	Operator inspection	4	16								0
Purge System	Connection to purge gas supply tank	No connection	No purging	7	Damage or defect to connector	2	Connector assembly stored during transport	Operator inspection	1	14								0
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel	4	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	12								
Tank System	Gas passage to/from Sequencing System	No hydrogen flow to sequencing system	Not able to defuel tanks	4	Manual ball valves closed	3	Operating instructions/procedures	Operating Inspections, Procedures	1	12					1	1	1	1
Tank System	Gas passage to/from Sequencing System	No hydrogen flow from sequencing system	Not able to test	4	Manual ball valves closed	3	Operating instructions/procedures	Operating Inspections, Procedures	1	12								
Tank System	Gas passage to/from Sequencing System	No nitrogen flow to/from sequencing system	Not able to purge tanks	4	Manual ball valves closed	3	Operating instructions/procedures	Operating Inspections, Procedures	1	12								
Sequencing System	Gas passage to Defuel System	No flow of nitrogen to Defuel System	Not able to automatically purge tanks, need to manually defuel	3	Valve fails closed (mechanical)	2	Valve credentials	Operator inspection	2	12								

Sequencing System	Gas passage to Defuel System	No flow of nitrogen to Defuel System	Not able to automatically purge tanks, need to manually defuel	3	Valve fails closed (air supply - solenoid failure)	2	Solenoid credentials	Operator inspection	2	12								
Sequencing System	Gas passage to Defuel System	No flow of nitrogen to Defuel System	Not able to automatically purge tanks, need to manually defuel	3	Valve fails closed (control signal)	2	DAQ credentials	Operator inspection	2	12								
Sequencing System	Gas passage to Defuel System	No flow of nitrogen to Defuel System	Not able to automatically purge tanks, need to manually defuel	3	Valve fails closed (air supply source failure)	3	Rated components, acceptance testing, checks, pressure switch, operating procedure	Operator inspection, Low air supply pressure alarm	1	9								
H2 Receiving System	Connection to H2 dispenser nozzle	No connection	No fueling	8	Damage,defect or obstruction to nozzle/receptacle	1	SAE J2600 H70, protected during transport, plastic cap	Operator inspection	1	8						1	1	1	1
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen not able to pass through receptacle	No hydrogen flow	8	Damage,defect or obstruction to nozzle/receptacle	1	SAE J2600 H70, protected during transport, plastic cap	Operator inspection	1	8								0
H2 Receiving System	Connection to H2 dispenser nozzle	Stuck Connection (mechanical)	Cannot remove nozzle	7	Nozzle pressure not vented	1	SAE J2600 H70, protected during transport, plastic cap	Operator inspection	1	7								
H2 Receiving System	Connection to H2 dispenser nozzle	Stuck Connection (mechanical)	Cannot remove nozzle	7	Damage,defect or obstruction to nozzle/receptacle	1	SAE J2600 H70, protected during transport, plastic cap	Operator inspection	1	7								
Sequencing System	Prevent overpressurization	Overpressurization	Exceed MAWP of receptacle, tanks, TPRD	7	Overpressure from dispenser: failure of triple redundant systems of dispenser (including PRV at 1.38x NWP)	1	Station dispenser limits, controls, PRV control system (station and device), device control (IRDA abort command, receiving valve closure)	Control System flag at upper pressure limit, device control/alarm, PRV activation (audible)	1	7	Review if PRV is required (assumptions - station side limit to pressure that can be applied to device							0