Revision: 0 Pages: 18

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

HyStEP Design Failure Modes and Effects Analysis

Revision: 0 Pages: 18

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



Report: 1 KUU / 42-U3-KUU HyStEP Design Failure Modes and Effects Analysis

Table of Contents

1 EXECUTIVE SUMMARY	2
2 INTRODUCTION	4
3 FAILURE MODES AND EFFECTS ANALYSIS	4
3.1 FMEA OVERVIEW	4
3.1.1 System Model	
3.1.1.1 Boundary Conditions	
3.1.2 FMEA Type	
3.2 ANALYSIS DEFINITIONS	
3.2.1 Function Definition	
3.2.2 Failure Mode Identification Criteria	9
3.2.3 Failure Effects	
3.2.4 Severity Classifications	
3.2.5 Occurrence Classifications	
3.2.6 Detection Classifications	
3.2.7 Causes	
3.3.1 Risk Priority Number	
3.4 FMEA ASSUMPTIONS	13
4 RESULTS AND DISCUSSION	14
4.1 RISK PRIORITY NUMBER RESULTS	15
4.4 SUMMARY	
5 RECOMMENDATIONS	17
6 APPENDIX A: FMEA WORKSHEET	18

HyStEP Design Failure Modes and Effects Analysis

Revision: 0 Pages: 18

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.

HyStEP Design Failure Modes and Effects Analysis

Revision: 0 Pages: 18

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.

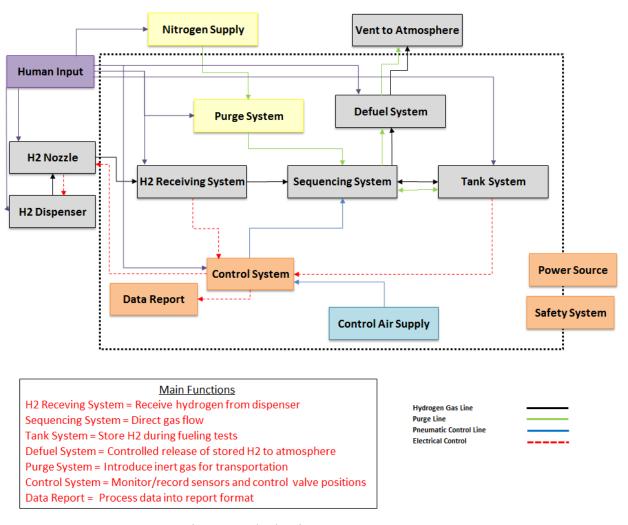


Figure 1: Block Diagram or Process Map

Revision: 0 HyStEP Design Failure Modes and Effects Analysis Pages: 18

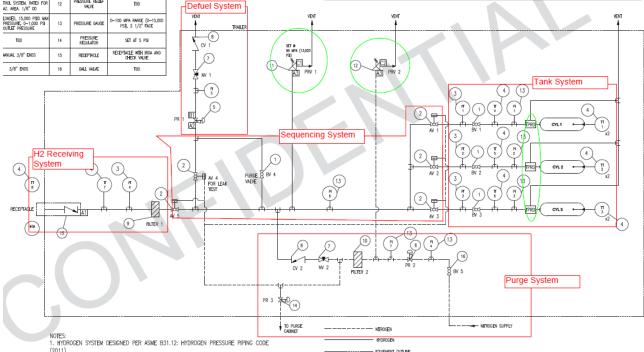


Figure 2: P&ID Drawing Showing FMEA Systems

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

Report: TR00742-03-R00 Revision: 0

Pages: 18

HyStEP Design Failure Modes and Effects Analysis

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	



Pages: 18

Revision: 0

	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

HyStEP Design Failure Modes and Effects Analysis Pages: 18

Revision: 0

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.				



Powertech HyStEP Design Failure Modes and Effects Analysis Revision: 0 Pages: 18

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 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

HyStEP Design Failure Modes and Effects Analysis Pages: 18

Revision: 0

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	No prevention controls. Frequency 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.			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 (design implemented, etc.). The PHM plots in the white area of the qualitative risk as 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. Indicate applied and appropriate action led to closure. Potential follow-up items (like a separate line item in this FMEA.	esessment or contact of the second of the se	other approved clo	g has been

HyStEP Design Failure Modes and Effects Analysis Pages: 18

Revision: 0

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 chance that the control will PREVENT or DETECT the failure mode, effect or cause.				
Low	7	Process example: Control is achieved with visual or double visual inspection only.				
		Moderate chance that the control will PREVENT or DETECT the failure mode, effect or cause.				
Moderate	5	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 chance that the control will PREVENT or DETECT the failure mode, effect or cause.				
High	3	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.				



Report: TR00742-03-R00 Revision: 0

HyStEP Design Failure Modes and Effects Analysis Pages: 18

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.

HyStEP Design Failure Modes and Effects Analysis Pages: 18

Revision: 0

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



Revision: 0

HyStEP Design Failure Modes and Effects Analysis Pages: 18

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
	Vent tanks in case of					
Tank System	fire	Tanks not vented when subjected to fire	Tank rupture	180	Included Heat/Fire Detection	100
	Vent tanks in case of				Included Heat/Fire Detection. Check list item	
Tank System	fire	Tanks not vented when subjected to fire	Tank rupture	180	for vent stack cap for every station	90
H2 Receiving					Passive ventilation included in trailer, testing	
System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	144	to occur with doors open (interlock)	72
Sequencing					Passive ventilation included in trailer, testing	
System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	144	to occur with doors open (interlock)	72
	Contain gas (up to 70				Passive ventilation included in trailer, testing	
Tank System	MPa NWP, 87.5 MAWP)	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	144	to occur with doors open (interlock)	72
					Passive ventilation included in trailer, testing	
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	144	to occur with doors open (interlock)	72
Control States	Hadasaa Canaan	la compatible de la companya di companya d	Higher level of H2 in trailer than	144	Passive ventilation included in trailer, testing to occur with doors open (interlock),	72
Control System	Hydrogen Sensors	Incorrect H2 sensor reading	measured	144	redundant sensors	/2
					Explosion proof panel has many bolts, very	
	Proper sensor inputs				unlikely to open panel except for	
Control System	(Class 1, Div 2)	Failure of explosion proof cabinet	Non rated electronics in classified area	135	maintenance.	54
	IRDA signals to				Several triggers to operator when targets out	
Control System	Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	135	of bounds (APRR, SOC, IRDA signals etc.)	81
	IRDA signals to				Several triggers to operator when targets out	
Control System	Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	135	of bounds (APRR, SOC, IRDA signals etc.)	81
H2 Receiving	Hydrogen particulate		Damage to downstream components		Filter installation procedure/schedule to be	
System	quality (<5 μm)	Allows >5um particles into system	(valves)	126	included. Include tamper sticker.	72
H2 Receiving	Hydrogen particulate		Damage to downstream components		Filter installation procedure/schedule to be	
System	quality (<5 μm)	Allows >5um particles into system	(valves)	126	included. Include tamper sticker.	72
			Damage to downstream components		Filter installation procedure/schedule to be	
Purge System	Particulate filtration	Allows >5um particles into system	(valves)	126	included. Include tamper sticker.	72
	D .: 1 . Cl:		Damage to downstream components	425	Filter installation procedure/schedule to be	
Purge System	Particulate filtration	Allows >5um particles into system	(valves)	126	included. Include tamper sticker.	72
	Valve control of	V. 1. 6.11		100		0.5
Control System	Sequencing System	Valves fail open	Undesired gas transfer between systems	120	Limit switches added to valves	96
H2 Receiving	Unidirectional Hydrogen				AV5 automatic open/closed during fueling	
System	Passage from Nozzle	Hydrogen flow back through receptacle	Leak to atmosphere	108	events and remains closed while not fueling	72



Revision: 0 Pages: 18

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



HyStEP Design Failure Modes and Effects Analysis

Revision: 0 Pages: 18

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.



Pages: 18

Revision: 0

6 Appendix A: FMEA Worksheet

See next page.

FMEA Worksheet



						Consultin	9								
Component/ System/ Process/ Operations/ Index	Function	Potential Failure Mode	Potential Effect(s) of Failure	Potential Cause(s) / Mechanism(s) of Failure	Current Design/ Process Control PREVENTION	Current Design/ Process Control DETECTION	Detection	RPN	Recommended Action(s)	Responsibility	Target Completion Date	Actions Taken	Severity	Occurrence	RPN
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	Localized fire does not activate TPRD	2 Short tank design, TPRD location	Operator inspection	9		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	5 100
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank rupture	Blocked vent line prevents gas from escaping after 10 TPRD activation	Plastic cap on vent to prevent water/contamination ingress	Operator inspection	9		Sandia's quantitative risk assesment. Consider fire/heat detection in device, if added, and depending on QRA results, revisit numbers. Comparable or less than wehicle 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	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	1	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	4 72
Sequencing System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9 Component Leak	Rated components, acceptance testing, checks	. Operator inspection, hydrogen sensors	4	1	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	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	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	i	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	4 72
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Explosive atmosphere inside trailer	9 Component Leak	Rated components, acceptance testing, checks	Operator inspection, hydrogen sensors	4	i	Consider positive/passive ventilation of the trailer. Vent should prevent reaching LFL n a minor leak scenario. Update based on vent design.			Passive ventilation included in trailer, testing to occur with doors open (interlock)	9	2 4	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		Scheduled maintenance, take credit for ventilation			Passive ventilation included in trailer, testing to occur with doors open (interlock), redundant sensors	9	2 4	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	1	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, ver unlikely to open panel except for maintenance.	у 9	2 3	3 54
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	Failure of IR signal 9 generator	IR Signal Generator credentials, robust commissioning, Device shut-downs	Feedback from dispenser, operator, in tank temp /pressure measurements, positive tank shutoff. Calculate SoC.	5		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	3 81
Control System	IRDA signals to Dispenser nozzle	Incorrect IRDA signals	Dispenser receives improper feedback	Failure of communication from DAQ control to signal generator	DAQ credentials, robust commissioning device shut-downs	Feedback from dispenser, operator, in tank temp i, measurements, positive tank shutoff.	5		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	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	!	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.		3 4	4 72
H2 Receiving System	Hydrogen particulate quality (<5 μm)	Allows >5um particles into system	Damage to downstream	6 Damged filter element	3 Operating instructions/procedures	Operator inspection	7		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.	oe 6	3	4 72

											Filter installation procedure, detection will					/ 7	
											be improved if included, may include					/ 7	
			Damage to downstream								tamper evident/resistant housing, annual		ı	ilter installation procedure/schedule to be		/ 7	
Purge System	Particulate filtration	Allows >5um particles into system	components (valves)	6	Filter element not installed	3	Operating instructions/procedures	Operator inspection	7	126	maintenance check			ncluded. Include tamper sticker.	6	3	4 72
											Filter installation procedure, detection will					/ 7	
											be improved if included, may include					/ 7	
			Damage to downstream								tamper evident/resistant housing, annual			ilter installation procedure/schedule to be		/ 7	
Purge System	Particulate filtration	Allows >5um particles into system	components (valves)	6	Damged filter element	3	Operating instructions/procedures	Operator inspection Operator inspection,	7	126	maintenance check			ncluded. Include tamper sticker.	6	3	4 72
	Valve control of Sequencing		Undesired gas transfer		Control signal to solenoid			Valve command displayed								/ 7	
Control System	System	Valves fail open	between systems		failure	3	Robust commissioning	on screen	5	120	Consider limit switches on valves	Powertech to source limit switches for Avs	1	imit switches added to valves	8	3	4 96
														AV5 automatic open/closed during fueling		7	
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen flow back through receptacle	Leak to atmosphere	۰	Check valve failure	,	SAE J2600 H70 receptacle	Operator inspection	4	100	Evaluate addition of redundant check valve also note that AV5 is NC unless filling.			events and remains closed while not ueling	9	2	4 72
nz keceiving system	rassage Holli Nozzie	receptacie	Leak to atmosphere	9	Clieck valve failure	3	SAE 12000 H70 receptacie	Operator inspection	-	108	also note that AV3 is NC unless miling.			Passive ventilation included in trailer,	9	_	4 /2
														esting to occur with doors open		/ 7	
			High and and of H2 in the line					0			Scheduled maintenance, credit for			interlock). Calibration procedure to be		/ 7	
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	ventilation can reduce numbers, also consider additional sensors			ncluded with operator/maintenance manual.	9	2	3 54
	.,,,										Pressure at this point in the system is very						
											low, and unlikely to cause a significant					/ 7	
Defuel System	Contain Hydrogen	Loss of containment (minor leakage)	Hydrogen Leakage external to trailer under dispenser canopy		Hose or connection Failure		Hose/connection creditials, operator instructions/procedures	Operator inspection	_	105	leak. Any leak that does happen will rapidly dissipate			Considered a low risk item - no further action.	,	3	5 105
Deluei System	Contain Hydrogen	leakage)	trailer under dispenser carlopy		(trailer to verit stack)	3	instructions/procedures	Operator inspection,	3	103	rapidiy dissipate		•	iction.		-	3 103
	Valve control of Sequencing	Unable to open valve(s) (Note:	Unable to transfer gas					Valve command displayed								/ 7	
Control System	System	valves are normally closed)	between systems	7	Solenoid Failure	3	Solenoid credentials	on screen	5	105	Consider limit switches on valves	Powertech to source limit switches for Avs	1	imit switches added to valves	7	3	4 84
			Fail to detect gas temperature								Consider redundant thermocouples (TT 4-					/ 7	
	Temperature Measurement		that is too low causes								6), control system comparison, calibration		-	T4-6 give redundant feedback to			
H2 Receiving System	(+/- 1°C)	Temperature fail high	component damage	9	Faulty thermocouple	2	Thermocouple, dispenser credentials	Operator inspection	5	90	plan			pperator. Pre-test Inspection checklist	9	2	4 72
	D		Non-retail de la standina in				Daniel and auticle							explosion proof panel has many bolts, very		/ 7	
Control System	Proper sensor inputs (Class 1, Div 2)	Failure of explosion proof cabinent	Non rated electronics in classified area	9	Damaged door seal		Panel credentials, operating/maintenance instructions	Operator inspection	5	90	Door open switch?			unlikely to open panel except for maintenance.	9	,	3 54
donard dystem	5.7 2,	ranare or expression proof cashiene	ciassifica area		bumagea ador sea.		operating mantenance instructions	Operator inspection		- 50	Boot open switch.		i	Explosion proof panel has many bolts, very		ĤΤ	<u> </u>
	Proper sensor inputs (Class 1,		Non rated electronics in											ınlikely to open panel except for		/ 7	
Control System	Div 2)	Failure of explosion proof cabinent	classified area	9	Damaged connection seals	2	Seal credentials, installation	Operator inspection	5	90	Door open switch?			naintenance.	9	2	3 54
		Tanks not vented when subjected			TPRD Fails to activate when						Sandia's quantitative risk assesment.					/ 7	
Tank System	Vent tanks in case of fire	to fire	Tank rupture		subjected to fire	1	TPRD credentials	Operator inspection	9	90	Consider fire/heat detection in device						
	Temperature Measurement										Consider redundant thermocouples,					/ 7	
H2 Receiving System	(+/- 1°C)	Temperature fail low	System Shutdown	6	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	90	control system comparison, calibration plan					/ 7	
TIZ Necerving System	(17 2 9)	Temperature familien	System snataown	_	radicy chermocoapie	J	memocoapie eredentidas	Operator inspection		30	prom						
			Fail to detect gas pressure													/ 7	
112 December Content	Pressure Measurement (0.1%	Pressure fail low	that is too high - exceeds	,	Facility processing transducer		DT avadantials	Onesates increation		0.4	Consider pressure relief valve					/ 7	
H2 Receiving System	(5)	Pressure fall low	MAWP of components	/	Faulty pressure transducer	3	PT credentials	Operator inspection	4	84	Consider pressure relief valve					+	
	Hydrogen particulate quality		Damage to downstream		Wrong filter element						Filter installation procedure, detection will					/ 7	
H2 Receiving System	(<5 μm)	Allows >5um particles into system	components (valves)	6	installed	2	Operating instructions/procedures	Operator inspection	7	84	be improved if included						
			Damage to downstream		Wrong filter element						Filter installation procedure, detection will					/ 7	
Purge System	Particulate filtration	Allows >5um particles into system	_		installed	2	Operating instructions/procedures	Operator inspection	7	84	be improved if included					/ 7	
,			i i					·									
											Determine safe location (i.e. distance from					/ 7	
			Explosive atmosphere in		Operator placement of vent stack, improper						dispenser and trailer, height, vent hose path), consultation with site owner,					/ 7	
Defuel System	Safe location for exhaust gas	Exhaust gas in unsafe location	unsafe area		training	3	Operating instructions/procedures	Operator inspection	3	81	feedback from DMS					/ 7	
Defuel System	Contain Hydrogon	Loss of containment (major leakage)	Hydrogen Leakage external to trailer under dispenser canopy		PRV Failure or activation	,	PRV credentials	Operator inspection	3	01	Review if PRV is required			PRV removed - determined to be required by Project Team			
Deluei system	Contain Hydrogen Controlled unidirectional	ieakdge)	trailer under dispenser canopy	9	rnv railure or activation	3	rny credefittals	Operator inspection	3	61	neview ii PKV is required		<u> </u>	by Froject realii			
	Purge gas passage to	Hydrogen flow back through check												Note: PRV replaced with burst disk for			
Purge System	Sequencing System	valve	trailer under dispenser canopy	9	PRV activation	3	Check valve credentials	Operator inspection	3	81			i	mproved reliability with vibration	9	3	3 81
	Controlled unidirectional gas	Uncontrolled release of gas to			Flow control valve open			Operating Inspections,						l			
Defuel System	exhaust to atmosphere	atmosphere	Noise from fast venting		too much	5	Operating instructions/procedures	Procedures, Audible	2	80	Muffler considered on vent stack						0
,			Maximum allowable defuel								Solution for defueling below maximum			1			
0.6.10	Controlled unidirectional gas	Uncontrolled release of gas to	rates exceeded, tank liner		Flow control valve open			Operating Inspections,			allowable defuel rate (find out from			l			
Defuel System	exhaust to atmosphere	atmosphere	damage	8	too much	5	Operating instructions/procedures	Procedures, Audible Operator inspection,	2	80	Quantum)						
	Valve control of Sequencing		Undesired gas transfer					Valve command displayed									
Control System	System	Valves fail open	between systems	8	Solenoid Failure	2	Solenoid credentials	on screen	5	80	Consider limit switches on valves						0
	Data collection, processing,				DAQ hardware/software		DAQ credentials, robust commissioning	g			Consider if bad data then potentially						
Control System	logic control	Data processed incorrectly	Bad data		failure, programmer error		data handling system	Data report	5	80	certifying station not meeting J2601			l			
·		Loss of containment (minor					Rated components, acceptance testing	g, Operator inspection,									
H2 Receiving System	Contain Hydrogen	leakage)	Bad test results	5	Component Leak		checks	hydrogen sensors	4	80							
Sequencing System	Contain Hydrogen	Loss of containment (minor leakage)	Bad test results	5	Component Leak		Rated components, acceptance testing checks	g, Operator inspection, hydrogen sensors	4	80				l			
requesting system	Contain gas (up to 70 MPa	Loss of containment (minor	u coc.could				Rated components, acceptance testing	, ,	-	- 50							
Tank System	NWP, 87.5 MAWP)	leakage)	Bad test results	5	Component Leak		checks	hydrogen sensors	4	80							
·					· 			·			·	·	·				

Temperature Measurement (+/-1°C) Temperature fail high Bal data 5 Faulty thermocopile of Paulty thermocopile of Pa									1				T				
Column C		Temperature Measurement										Consider redundant thermocouples,					1
Company Comp	H2 Receiving System		Temperature fail high	Bad data	5	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	75						0
March Marc	3 ,					,		·	·			, ,					
Secretary of the control of the cont	U2 Barabia - Cartana		T 6-111	D- d d-t-	_	Facility the annual annual a	_	The construction of the second of the least	0	-							
March Marc	H2 Receiving System	(+/- 1 C)	Temperature fall low	Bad data	5	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5	/5	pian					
March Control Contro		In-tank Temperature						Thermocouple credentials, redundant	Operator inspection,								1
March Marc	Tank System	Measurement (+/- 1°C)	Temperature fail high	Bad data	5	Faulty thermocouple	3	thermocouple element in tank	control comparison	5	75						0
March Marc		In-tank Temperature						Thermosouple credentials redundant	Operator inspection								
Manual Control Contr	Tank System		Temperature fail low	Bad data	5	Faulty thermocouple	3			5	75						
Marie Mari	,	, , ,				, , , , , , , , , , , , , , , , , , , ,			, , , , , , , , , , , , , , , , , , ,								
Commonwealth Comm																	
	Tank System	NWP, 87.5 MAWP)	leakage)	trailer under dispenser canopy	9		2	TPRD credentials	Audible	4	72						
March Marc				Explosive atmosphere in								Determine proper securing method,					
Part	Defuel System	Safe location for exhaust gas	Exhaust gas in unsafe location	unsafe area	9		4	Operating instructions/procedures	Operator inspection	2	72						
Part																	
Page			Hydrogen flow back through check	Overnressurize nurge system				Check valve credentials PRV in nurge						Note: PRV replaced with burst disk for			
Segregation of the control of the co	Purge System				9	Check valve fails open				4	72				9 2	4	72
Segregation of the control of the co																	
Segregation of the control of the co								Pated components, acceptance testing									
Set plane and approximation of the process of the p				Exceed pressure rating of					·			Label for max inlet pressure for purge gas					
The content of the				purge system causing				maximum T-cylinder pressure (PRV is	pressure gauge, audible if			connection, see above for check valve					
Processor State Control of Contro	Purge System	Prevent overpressurization	Overpressurization	component failure	9	Check-valve failure	2	considered for check valve failure only)	PRV activates	4	72	failure mode		improved reliability with vibration	9 2	4	72
Processing and the control of the co									Operator inspection .								
Section Section Control Contro								Sensor credentials, sensor connections									
Consistence of the control of the co			Sensors not suitable for Class 1, Div						maintenance and								
Service for several process of the several pr	Control System	Div 2)	2	classified area	9	Non-rated sensors installed	2	safe wiring	calibration procedures	4	72						
Service for several process of the several pr																	
Service for several process of the several pr																	
Service de control de la contr																	
Self-ordinary and extractions are consistent and an extraction of the control of																	
The Proposition of State																	
Control contro																	
South Systems of Manufactur Control Systems (Manufactur Co																	
Color Select unificacional par Controlled revisure di part to descriptione de la dissipation de la dis	Defuel System		_	Noise from fast venting	۰	-	2			2	72						
Macronal surface interval gas. Obtail Spatian Should spatian	Derder System	extraust to atmosphere	autiospilere	Noise from fast venting		pressure	3	control valve downstream	Addible	3	72	closed? On Fivil during activation of AV4					
Control distance de l'authorité production d									l l								
Soften yellow and protection of the protection o		Controlled unidirectional ass	Uncontrolled valence of one to			Failed regulator increases			l l								
Central de sixtem de los de central de la six, cannot de la six, c	Defuel System				8	-	3			3	72						
Counted yearsom or fine control yearsom or fine control yearsom for fine control yearsom yearsom for fine control yearsom						p. 444											
Pressure Measurement (0.15) Pressure Sequence (1.15) Pressure Measurement (1.15) Pressur																	
As Pressure fail high poses of the Speciming System of Speciming System of Security System of System of Security System of Security System of Security System of System of Security Syst	Defuel System	exhaust to atmosphere	No Flow	transport trailer	8	failed closed	3	maintenance plan	Procedures	3	72						
As present failings from the financial process of the financial process		Pressure Measurement (0.1%										Consider redundant PTs, control system					
1.9 Receiving System	H2 Receiving System	FS)	Pressure fail high	System Shutdown	6	Faulty pressure transducer	3	PT credentials	Operator inspection	4	72						
1.9 Receiving System																	
Helevelving System Sequenting System Sequenting System Sequenting System Sequenting System Sequenting System System Shuddown prematurity Syste	H2 Peceiving System		Low gas flow to sequencing system	Rad test outcome	6	Clogged Filter	4	Operating instructions/procedures	Operator inspection	2	72	· · · · · · · · · · · · · · · · · · ·					
Segmenting System Low gas flow to sequencing system all select outcome 0 Obstruction in gas line 0 Obstruc	112 Necelving System		Low gas now to sequencing system	bad test outcome	-	Clogged Filter	7	Operating instructions, procedures	Operator inspection	3	/2	be improved if included					
Tank System S Pressure fail high 67.5 MPa 6 Faulty pressure transducer 3 PT credentials Control System Supplying power to the Control System Supplying power to the S	H2 Receiving 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 S Pressure fall high 67.5 MPa) 6 Faulty pressure transducer 3 PT credentials Operator inspection 4 PT Control System Supplying power to the Control System Supplying power to the Supplying power to t													 				
Supplying power to the	Tank System	Pressure Measurement (0.1%	Pressure fail high		6	Faulty pressure transducer	3	PT credentials	Operator inspection	4	72						
System System No main power to control system of 20 Poerating procedures system on display system system on display system on display system on display system on display system system on display system system on display system system on display system system system on display system system on display system s	rank system		coourc run riigii	(C5 Wil u)		. autry pressure transducer		c.cucinaais	operator inspection	-	,,	comparison, canonation plan					
Supplying power to the system on the system of the system									l l								
Control System System No main power to control system Power loss shutdown occurs of all to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure transducer, Fail to detect gas pressure transducer, FS) Pressure fail low MAWP of components A Derating procedures System on display Consider redundant PTs, control system Consi	Control System	system	No main power to control system	Device inoperable	6	of 120VAC	4	Operating procedures	system on display	3	72	follow-up on what battery back-up covers					0
Control System System No main power to control system Power loss shutdown occurs of all to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure that is too high - exceeds FS) Fail to detect gas pressure transducer, Fail to detect gas pressure transducer, FS) Pressure fail low MAWP of components A Derating procedures System on display Consider redundant PTs, control system Consi		Supplying power to the				Accidental disconnection			Feedback from control			Assumption: hattery back-up for DAO					
Pressure Measurement (0.1% Pressure fail to detect gas pressure that is too high - exceeds MAWP of Components and a source turner to high System shutdown when System does not shutdown when System system same shutdown when System sounds calibration plan calibration plan competitions, Procedures A Gas pressure tails too high specificate such standards and such standards specificated such such samples calcibration plan calcibration such such such samples system system such such such s	Control System		No main power to control system	Power loss shutdown occurs	6		4	Operating procedures		3	72						
Pressure Measurement (0.1% Pressure fail low MAWP of components 8 Faulty pressure transducer, FS) Pressure fail low MAWP of components 8 Faulty pressure too high 2 PT credentials Operator inspection 4 Gallbration plan Pressure Measurement (0.1% Pressure fail low MAWP of components 8 Pressure too high 2 PT credentials Operator inspection 4 Gallbration plan Pressure fail low MAWP of components 8 Pressure too high 2 PT credentials Operator inspection 4 Gallbration plan Pressure Measurement (0.1% Pressure fail low MAWP of components 8 Pressure too high 2 PT credentials Operator inspection 4 Gallbration plan Pressure fail low MAWP of components 8 Pressure too high 4 G4 callbration plan Procedures 4 G4 Callbration plan Procedures 4 G4 Callbration plan Procedures 5 PT credentials Operator inspection 4 Gallbration plan Procedures 4 G4 Callbration plan Procedures 5 PT credentials Operator inspection 4 GA Callbration plan Procedures 4 G4 Callbration plan Procedures 5 PT credentials Operator inspection 4 GA Callbration plan Procedures 5 PT credentials PT credentials PT cannot be callbrated by a callbration plan Procedures 6 GA Callbration plan Procedures 7 GA CACCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC																	
Tank System FS Pressure fail low MAWP of components 8 Pressure too high 2 Procedentials Operator inspection 4 64 Calibration plan Controlled unidirectional gas exhaust to atmosphere No Flow Tansport trailer System		Dragging Marriage 1 (2)				Faultu nua tu											
Controlled unidirectional gas exhaust to atmosphere No Flow transport trailer 8 Obstruction in gas line Incorrect Lower Temperature Limit Setpoints, signal output fails (Digital output Modern System shutdown when System does not shutdown when Sys	Tank System	FS)	Pressure fail low	=	8		2	PT credentials	Operator inspection	4	64						
Defuel System exhaust to atmosphere No Flow transport trailer 8 Obstruction in gas line Incorrect Lower Temperature Limit System shutdown when System does not shutdown during Fail to detect gas temperature falls (Digital output Fails (Digital output Falls (Digital	22,2.2	-1		S. Somponento	Ť	, seem too mgn	-		- parata moperation								
System shutdown when Temperature Limits exceeded Foundation of the Control System does not shutdown during Temperature Limit sexceeded Foundation for the Control System does not shutdown during Temperature Limits exceeded Foundation for the Control System does not shutdown when System does not shutdown wh						[
System shutdown when System does not shutdown during Temperature Limit Setpoints, signal output fails (Digital output Systems shutdown when System shutdown when System does not shutdown	Defuel System	exhaust to atmosphere	No Flow	transport trailer	8		2	Purging System	Procedures	4	64						
System shutdown when Control System Temperature Limits exceeded fueling when inlet gas is <-40C System does not shutdown when Control System System does not shutdown when System does not shutdown during Temperature Limits exceeded fueling when inlet gas is <-40C System does not shutdown when System do																	
System shutdown when Control System System shutdown when Temperature Limits exceeded fueling when inlet gas is <-40C component damage System does not shutdown when Temperature Limits exceeded fueling when inlet gas is <-40C component damage System does not shutdown when Syste				Fail to detect gas temperature		l '						Link back to individual sensors in other					
System shutdown when System does not shutdown when System does not shutdown when acceeds MAWP of System does not s						fails (Digital output											
System shutdown when System does not	Control System	Temperature Limits exceeded	fueling when inlet gas is <-40C	component damage	8	module)	2	device shut-downs	Operator inspection	4	64	manual					0
System shutdown when System does not						Incorrect upper pressure											
												Link back to individual sensors in other					
Control System pressure limits exceeded pressure is >87.5 MPa components 8 module) 2 shut-downs, PRV Operator inspection 4 64 manual 0								-									
	Control System	pressure limits exceeded	pressure is >87.5 MPa	components	8	module)	2	snut-downs, PRV	Operator inspection	4	64	manual	<u> </u>				. 0

	IRDA signals to Dispenser		Non-comm fueling testing				IR Transmitter credentials, robust	Feedback from dispenser,			Test sequence planning (ABORT command			1				
Control System	nozzle	Loss of IRDA signal	only	7	Failure of IR transmitter	3	commissioning	operator	3	63	as first test)							0
Control System	IRDA signals to Dispenser nozzle	Loss of IRDA signal	Non-comm fueling testing only		Failure of IR signal generator	2	IR Signal Generator credentials, robust commissioning	Feedback from dispenser, operator	3	63	Test sequence planning (ABORT command as first test)							
Control System	1102210	E033 OF INDA Signal	Office		generator	,	Commissioning	орегисы	,	- 03	us mise eesey							
	IRDA signals to Dispenser		Non-comm fueling testing		Failure of communication from DAQ controls to			Feedback from dispenser,			Test sequence planning (ABORT command							
Control System	nozzle	Loss of IRDA signal	only		signal generator	3	DAQ credentials, robust commissioning		3	63	as first test)							
	System shutdown during ESD	No shutdown when ESD button	Overpressure, temperatures				ESD button credentials, maintenance	ESD check as part of										
Control System	event	pressed	too high/low, H2 leaks	10	ESD button sticking	2	plan	operating procedures	3	60	ESD shutdown procedure						4	
	System shutdown during ESD	No shutdown when ESD button	Overpressure, temperatures		Water infiltration bridging		ESD button credentials/enclosure/installation,	ESD check as part of										
Control System	event	pressed	too high/low, H2 leaks	10	ESD contacts	2	maintenance plan	operating procedures	3	60							4	
	System shutdown during ESD	No shutdown when ESD command	Overpressure, temperatures					Feedback from control			Watchdog timer, heartbeat (control health			cDAQ Health Check included in Alarm				
Control System	event	from DAQ system	too high/low, H2 leaks	10	DAQ failure	2	DAQ credentials, robust commissioning	system on display	3	60	status), communcation loss shutdowns?			Matrix	10	2	3	60
		No shutdown when H2 sensors	Overpressure, temperatures				H2 Sensor credentials, robust	Feedback from control	_									
Control System	event	alarm	too high/low, H2 leaks	10	H2 Sensor failure	2	commisioning	system on display	3	60								
H2 Receiving System	Pressure Measurement (0.1%	Pressure fail high	Bad data		Faulty pressure transducer	,	PT credentials	Operator inspection	4	60	Consider redundant PTs, control system comparison, calibration plan							0
mz keceiving system	(73)	rressure fail fligh	bau uata	3	radity pressure transducer	3	ri ciedentiais	Operator inspection	-	60	companson, cambration plan							,
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		Consider redundant PTs, control system comparison, calibration plan							0
	Drace use Management (0.19)										Consider redundant PTs, control system comparison (receiving PT, other tanks),							
Tank System	Pressure Measurement (0.1% FS)	Pressure fail low	Bad data	5	Faulty pressure transducer	3	PT credentials	Operator inspection	4	60	calibration plan							
	Controlled unidirectional Purge gas passage to										Filter installation procedure, detection will							
Purge System	Sequencing System	Low gas flow to sequencing system	Slow purging	5	Clogged Filter	4	Operating instructions/procedures	Operator inspection	3	60	be improved if included							
											Link back to individual sensors in other							
	Proper sensor inputs (Class 1,		Inaccurate measurements or		Installation/maintenance			Operator inspection,			systems, maintenance captured in device							
Control System	Div 2)	Sensors not properly installed	no measurements, bad data	5	error, incorrect wiring	3	Sensor credentials, robust comissioning	control comparison	4	60	manual							0
	Proper sensor inputs (Class 1,		Inaccurate measurements or		Installation/maintenance			Operator inspection,			Link back to individual sensors in other systems, maintenance captured in device							
Control System	Div 2)	Sensor inputs wrong scale	no measurements, bad data	5	error	3	Sensor credentials, robust comissioning		4	60	manual							
											Link back to individual sensors in other							
	Proper sensor inputs (Class 1,		Inaccurate measurements or		Installation/maintenance			Operator inspection,	_		systems, maintenance captured in device							
Control System	Div 2)	Sensors not calibrated	no measurements, bad data	5	error, incorrect wiring	3	Sensor credentials, robust comissioning	control comparison	4	60	manual							
	Proper sensor inputs (Class 1	Sensors do not meet electrical	Inaccurate measurements or		Installation/maintenance			Operator inspection,			Link back to individual sensors in other systems, maintenance captured in device							
Control System	Div 2)	specifications (24VDC, 4-20 mA)	no measurements, bad data		error	3	Sensor credentials, robust comissioning		4	60	manual							
											Control system comparison, calibration							
	In-line Temperature										plan, Determine how warning/alarm							
Tank System	The state of the s	Temperature fail high	Bad data	4	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5		processed by controls. Assumption is these sensors not used for control.							0
											Control system comparison, calibration							
	In-line Temperature										plan, Determine how warning/alarm							
Tank System	Measurement (+/- 1°C)	Temperature fail low	Bad data	4	Faulty thermocouple	3	Thermocouple credentials	Operator inspection	5		processed by controls. Assumption is these sensors not used for control.							
	Gas passage to/from	No hydrogen flow to sequencing					Filtration in H2 Receiving System and	Operating Inspections,										
Tank System	Sequencing System	system	Not able to defuel tanks	7	Obstruction in gas line	2	Purging System	Procedures	4	56								
	Gas passage to/from	No hydrogen flow from sequencing					Filtration in H2 Receiving System and	Operating Inspections,										
Tank System	Sequencing System	system	Not able to test	7	Obstruction in gas line	2	Purging System	Procedures	4	56								
	Gas passage to/from	No nitrogen flow to/from					Filtration in H2 Receiving System and	Operating Inspections,										
Tank System	Sequencing System	sequencing system	Not able to purge tanks	7	Obstruction in gas line	2	Purging System	Procedures	4	56								
		Loss of containment (major	Purge gas leakage external to				Hose/connection creditials, operator	Operator inspection,										
Purge System	Contain purge gas	leakage)	trailer under dispenser canopy	7	Hose or connection Failure	4	instructions/procedures	Audible	2	56	Review N2 source and installed locatation							
					Damage, defect or			Operator detects audible										
H2 Receiving System	Connection to H2 dispenser nozzle	Loose Connection	Hydrogen Leakage		obstruction to nozzle/receptacle	2	SAE J2600 H70, protected during transport, plastic cap	leak or dispenser leak detection	3	54								
											Condicts augustitative of the control of							
Tank System	Vent tanks in case of fire	Tanks not vented when subjected to fire	Tank damage		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							
					Blocked vent line prevents													
		Tanks not vented when subjected			gas from escaping after		Plastic cap on vent to prevent				Sandia's quantitative risk assesment.							
Tank System	Vent tanks in case of fire	to fire	Tank damage	9	TPRD activation	2	water/contamination ingress	Operator inspection	3	54	Consider fire/heat detection in device		1					

											Г			
					Flow control valve open									
	_	Uncontrolled release of gas to	Ignition of hydrogen at vent		too much plus ignition		Operating instructions/procedures, ven							
Defuel System	exhaust to atmosphere	atmosphere	stack	9	event	3	stack design, placement, stability	Procedures, Audible	2	54			CGA Vent stack considerations	
							Operating instructions/procedures,	Operating Inspections,						
					Failed regulator increases		secondary flow control with flow	Procedures, pressure						
Defuel System	Controlled unidirectional gas exhaust to atmosphere	Uncontrolled release of gas to atmosphere	Ignition of hydrogen at vent stack		pressure plus ignition event		control valve downstream, vent stack design, placement, stability	indicator for operator, Audible	3	54			CGA Vent stack considerations	
Derder System	exitaust to atmosphere	autiospilere	Stack	,	event		design, placement, stability	Addible	,	34			COA VEII STACK CONSIDERATIONS	
		Loss of containment (major	Hydrogen Leakage external to		Hose or connection Failure		Hose/connection creditials, operator	Operator inspection,						
Defuel System	Contain Hydrogen	leakage)	trailer under dispenser canopy	9	(trailer to vent stack)	2	instructions/procedures	Audible	3	54				
	System shutdown during FSD	ESD circuit shuts down when not			Operator error (ESD button			Feedback from control						
Control System	event	required	Prevent testing		pushed)	3	Operator training	system on display	3	54	Software acknoledgment			
											Is check valve required? Check valve included in quick-connect? Assumption:			
											pressure downstream when mixed with 1			
	Controlled unidirectional gas		Allows air into defuel system								atm air reduces level below explosion limit			
Defuel System	exhaust to atmosphere	Reverse flow	causing gas mixure	3	Failed check valve	2	Check valve credentials	None	9	54	and pushed out of vent stack.			
								Operating Inspections,						
	Controlled unidirectional gas		Cannot defuel tanks, cannot		Regulator fails, no		Regulator credentials, operating	Procedures, pressure						
Defuel System	exhaust to atmosphere	No Flow	transport trailer	8	regulated pressure		instructions/procedures	gauge	3	48				
	Valvo control of Comment		Underinad ass transfer		Wrong connection of the		Pohust commissioning L - /L	Operator inspection,						
Control System	Valve control of Sequencing System	Valves fail open	Undesired gas transfer between systems		Wrong connection of air supply to valves	2	Robust commissioning, valve/hose identification	Valve command displayed on screen	3	48	Maintenance manual			
		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		Incorrect Lower									
					Temperautre Limit									
	System shutdown when	System does not shutdown during	Fail to detect gas temperature		Setpoints, signal output		DAO cradantials robust sommissis	Operator inconstica			Link back to individual sensors in other			
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown during defueling when tank gas is <-40 C			fails (Digital output module)		DAQ credentials, robust commissioning device warning and shut-downs	feedback from controls	3	48	systems, maintenance captured in device manual			
control system	Temperature Emiles exceeded	derdeling when tank gas is 4 40 C	component damage	Ť	Incorrect Lower	_	device warning and shar downs	recubuck from controls	,	70	manadi			
					Temperautre Limit									
	Contain the transfer of the con-	Contain de la co	Fail to detect gas temperature		Setpoints, signal output		DAO and auticle achieve accoming to the	0			Link back to individual sensors in other			
Control System	System shutdown when Temperature Limits exceeded	System does not shutdown during defueling when tank gas is <-40 C			fails (Digital output module)		DAQ credentials, robust commissioning device warning and shut-downs	feedback from controls	3	48	systems, maintenance captured in device manual			
control system	Temperature Emiles exceeded	derdeling when tank gas is 4 40 C	damage	Ť	Incorrect upper	_	device warring and shar downs	recubuck from controls	,	70	manadi			
					Temperautre Limit									
			Fail to detect gas temperature		Setpoints, signal output						Link back to individual sensors in other			
	System shutdown when	System does not shutdown when												
Control System	Temperature Limits exceeded		that is too high, tank liner		fails (Digital output	2	DAQ credentials, robust commissioning device warning and shut-downs		3	48	systems, maintenance captured in device			
Control System	Temperature Limits exceeded		damage		module)	2	DAQ credentials, robust commissioning device warning and shut-downs	g, Operator inspection, feedback from controls	3	48	systems, maintenance captured in device manual			
Control System	Temperature Limits exceeded		= '	8	module) Incorrect tank pressure	2			3	48	manual			
Control System		tank gas is >85 C	damage	8	module) Incorrect tank pressure differential Setpoints,		device warning and shut-downs	feedback from controls	3	48	manual Link back to individual sensors in other			
	Prevent uncontrollable flow	tank gas is >85 C Uncontrolled gas transfer between	damage Excced allowable defuel rate,	8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital		device warning and shut-downs DAQ credentials, robust commissioning	feedback from controls			manual Link back to individual sensors in other systems, maintenance captured in device			
Control System Control System		tank gas is >85 C	damage	8	module) Incorrect tank pressure differential Setpoints,		device warning and shut-downs	feedback from controls	3		manual Link back to individual sensors in other			
	Prevent uncontrollable flow between tanks	tank gas is >85 C Uncontrolled gas transfer between	damage Excced allowable defuel rate, temperature swings in tanks	8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital	2	device warning and shut-downs DAQ credentials, robust commissioning	feedback from controls			manual Link back to individual sensors in other systems, maintenance captured in device			
Control System	Prevent uncontrollable flow between tanks Supplying power to the system	tank gas is >85 C Uncontrolled gas transfer between tanks	Excced allowable defuel rate, temperature swings in tanks	8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module)	2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms	g, Operator inspection, s audible	3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual			
Control System Control System	Prevent uncontrollable flow between tanks Supplying power to the	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable	8 8 8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails	2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms	g, Operator inspection, s audible Blank screen	3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system			
Control System	Prevent uncontrollable flow between tanks Supplying power to the system	tank gas is >85 C Uncontrolled gas transfer between tanks	Excced allowable defuel rate, temperature swings in tanks	8 8 8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module)	2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms	g, Operator inspection, s audible	3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual			
Control System Control System H2 Receiving System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS)	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak	8 8 8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer	2 2 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials	g, Operator inspection, s audible Blank screen Operator inspection	3 3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system			
Control System Control System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS)	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable	8 8 8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails	2 2 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials	g, Operator inspection, s audible Blank screen	3 3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan			
Control System Control System H2 Receiving System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak	8 8 8	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer	2 2 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials	g, Operator inspection, s audible Blank screen Operator inspection	3 3	48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan			
Control System Control System H2 Receiving System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak	8 8 8 4	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer	2 2 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials	g, Operator inspection, s audible Blank screen Operator inspection	3 3	48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system			
Control System Control System H2 Receiving System Tank System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak	8 8 8 4	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer	2 2 3 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection	3 3 4	48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low No gas flow to sequencing system	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible	8 8 8 4 4 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer	2 2 3 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection Operator inspection	3 3 4	48 48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible	8 8 8 4 4 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer	2 2 3 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection	3 3 4	48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low No gas flow to sequencing system	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible	8 8 8 4 4 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer	2 2 3 3 3 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection Operator inspection	3 3 4	48 48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low No gas flow to sequencing system	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible	8 8 4 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer	2 2 3 3 3 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection Operator inspection	3 3 4	48 48 48 48	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible	8 8 4 7 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed	2 2 3 3 3 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection	3 3 4	48 48 48 48 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible No purging possible	8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line	2 2 3 3 3 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection Operator inspection Operator inspection	3 3 4	48 48 48 48 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible	8 8 8 4 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation	2 2 3 3 3 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection	3 3 4	48 48 48 48 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing,	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage)	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy	8 8 4 4 7 7 7 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software	2 2 3 3 3 2 2 2 3 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data	3 3 4	48 48 48 48 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible No purging possible	8 8 4 4 7 7 7 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation	2 2 3 3 3 2 2 2 3 3	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures	g, Operator inspection, s audible Blank screen Operator inspection operator inspection, audible	3 3 4	48 48 48 48 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage)	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy	8 8 4 4 7 7 7 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software	2 2 3 3 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report	3 3 4	48 48 48 48 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Purge System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage)	damage Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software	2 2 3 3 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report	3 3 4	48 48 48 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Purge System Control System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure	2 2 3 3 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report g, Control feedback, data report checks	3 3 4 4 2 3 3 3	48 48 48 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Purge System Control System Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly	2 2 3 3 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report checks g, Control feedback, data	3 3 4 4 2 2 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure	2 2 3 3 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report g, Control feedback, data report checks	3 3 4 4 2 3 3 3	48 48 48 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly	2 2 3 3 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report checks g, Control feedback, data	3 3 4 4 2 2 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed format	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly	2 2 3 3 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection operator inspection, audible g, Control feedback, data report checks g, Control feedback, data report checks	3 3 4 4 2 2 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System Data Report Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed format	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available No data report available	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly File corrupted	2 2 3 3 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report checks G, Control feedback, data report checks	3 3 3 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed format	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available	8 8 8 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly	2 2 3 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system DAQ credentials, robust commissioning data handling system, size of storage and operator downloading instructions	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report checks g, Control feedback, data report checks G, Control feedback, data report checks	3 3 4 4 2 2 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			
Control System Control System H2 Receiving System Tank System Purge System Purge System Purge System Control System Data Report	Prevent uncontrollable flow between tanks Supplying power to the system Pressure Measurement (0.1% FS) Pressure Measurement (0.1% FS) Controlled unidirectional Purge gas passage to Sequencing System Contain purge gas Data collection, processing, logic control Provide Electronic File of relevant data in prescribed format Provide Electronic File of relevant data in prescribed format	tank gas is >85 C Uncontrolled gas transfer between tanks Loss of 24 VDC power Pressure fail low No gas flow to sequencing system No gas flow to sequencing system Loss of containment (major leakage) No data collection No electronic file	Excced allowable defuel rate, temperature swings in tanks ESD Shutdown mode, system inoperable False indication of leak False indication of leak No purging possible No purging possible No purging possible Purge gas leakage external to trailer under dispenser canopy Loss of test results No data report available No data report available	8 8 8 4 4 7 7 7	module) Incorrect tank pressure differential Setpoints, signal output fails (Digital output module) 24VDC Power supply fails Faulty pressure transducer Faulty pressure transducer Filter clogged Check valve fails closed Obstruction in gas line PRV Failure or activation DAQ hardware/software failure File not saved properly File corrupted	2 2 3 3 2 2 2 2 2	device warning and shut-downs DAQ credentials, robust commissioning device alarms, tank temperature alarms Power supply credentials PT credentials PT credentials Filter credentials, operating instructions/procedures Check valve credentials, operating instructions/procedures Operating instructions/procedures PRV credentials DAQ credentials, robust commissioning data handling system	g, Operator inspection, s audible Blank screen Operator inspection Operator inspection, audible g, Control feedback, data report checks g, Control feedback, data report checks G, Control feedback, data report checks	3 3 3 3 3 3	48 48 48 42 42 42 42 42	manual Link back to individual sensors in other systems, maintenance captured in device manual Consider redundant PTs, control system comparison, calibration plan Consider redundant PTs, control system comparison, calibration plan Filter installation procedure, detection will be improved if included Determine feedback loop to operator Note: hardcopy/printer to be discussed in			

						1		T			
								Assume that leak is detected after			
		Loss of containment (major	Explosive atmosphere inside		Rated components, acceptance testing	ing Operator inspection		occurance in time for safe shutdown, consider appropriate sensor placement			
H2 Receiving System	Contain Hydrogen	leakage)	trailer	10 Component Rupture	2 checks	hydrogen sensors	2	and flow path			
<u> </u>	, ,	Loss of containment (major	Explosive atmosphere inside		Rated components, acceptance testing			·			
Sequencing System	Contain Hydrogen	leakage)	trailer	10 Component Rupture	2 checks	hydrogen sensors	2 4)			
- 10 .	Contain gas (up to 70 MPa	Loss of containment (major	Explosive atmosphere inside	40	Rated components, acceptance testin						
Tank System	NWP, 87.5 MAWP)	leakage)	trailer	10 Component Rupture	2 checks	hydrogen sensors	2 4	0			
					Gauge credentials, calibration check						
			Regulated defuel pressure set		plan, flow control downstream is						
Defuel System	Pressure Indication	Pressure fail low	higher than expected	5 Damaged/defective gai	ge 2 secondary flow restriction	Operator inspection	4				
	Controlled unidirectional Purge gas passage to	Hydrogen flow back through check	Hydrogon miving with nurgo		Check valve credentials, Purge system	Operator inspection, m pressure gauge, audible if					
Purge System	Sequencing System	valve	gas	5 Check valve fails open	2 components rated for hydrogen use		4				
r dige system	Sequencing System	Loss of containment (major	Explosive atmosphere inside	Circuit taite tails open	Rated components, acceptance testing						
Defuel System	Contain Hydrogen	leakage)	trailer	10 Component Rupture	2 checks	hydrogen sensors	2 4				
Comband Combana		ESD circuit shuts down when not	Daniel de La dia a	6 FSD circuit failure	ESD circuit credentials, robust	Feedback from control		_			
Control System	event	required	Prevent testing	6 ESD circuit failure	2 comissioning	system on display	3				
	Supplying power to the				Fuse sized appropriately, fuse	Feedback from control		Assumption: battery back-up for DAQ,			
Control System	system	No main power to control system	Device inoperable	6 Fuse blown	2 credentials	system on display	3 3	follow-up on what battery back-up covers			
Control Sustam	Supplying power to the	No main nower to central aurtaus	Davica inaparable	Encility passes as to	3 None	Feedback from control	,	Assumption: battery back-up for DAQ,			
Control System	system	No main power to control system	Device moperable	6 Facility power outage	2 None	system on display	3	follow-up on what battery back-up covers	+		
	Supplying power to the				Fuse sized appropriately, fuse	Feedback from control		Assumption: battery back-up for DAQ,			
Control System	system	No main power to control system	Power loss shutdown occurs	6 Fuse blown	2 credentials	system on display	3	controlled shutdown sequence			
Control C	Supplying power to the	No sector and the sec	Daniel I I I	6 Facility	2 North	Feedback from control		Assumption: battery back-up for DAQ,			
Control System	system Supplying power to the	No main power to control system	Power loss shutdown occurs ESD Shutdown mode, system	6 Facility power outage	Z None Fuse sized appropriately, fuse	system on display	3	5 controlled shutdown sequence			
Control System	system	Loss of 24 VDC power	inoperable	6 Fuse blown	credentials	Blank screen	3				
	Provide Electronic File of										
	relevant data in prescribed		Loss of productivity - operator		DAQ credentials, robust commissioni	ing, Control feedback, data					
Data Report	format	File in wrong format	tries to sort out data	6 Programming error	2 data handling system	report checks	3	5			
	Provide Electronic File of relevant data in prescribed		Loss of productivity operator		DAQ credentials, robust commissioni	ing Control foodback data					
Data Report	format	File in wrong format	Loss of productivity - operator tries to sort out data	6 File corrupted	2 data handling system	report checks	3 3	5			
				Failure of pressure	and the same of th	Top or to the one					
			Exceed rating of defuel/vent	regulator with defuel v	alve	Operator inspection,		Review if PRV is required (see above).			
		Overpressurization of defuel/vent	components causing	open and blockage in v	ent	pressure gauge, audible if		Assumption: operator cannot exceed		Note: PRV removed from Defuel System	
Defuel System	Prevent overpressurization	Overpressurization of defuel/vent components					4 3	Assumption: operator cannot exceed		Note: PRV removed from Defuel System (rated components up to vent stack)	
Defuel System	Prevent overpressurization	components	components causing component damage	open and blockage in v	PRV downstream of regulator	pressure gauge, audible if PRV activates	4 :	Assumption: operator cannot exceed			
Defuel System Purge System	Prevent overpressurization Contain purge gas		components causing	open and blockage in v	ent	pressure gauge, audible if PRV activates	4 3	Assumption: operator cannot exceed recommended regulated pressure.			
,	Contain purge gas Touch screen to provide	components Loss of containment (major leakage)	components causing component damage Waste of purge gas, oxygen displacement in trailer	open and blockage in v	PRV downstream of regulator Rated components, acceptance testing	pressure gauge, audible if PRV activates ing, Operator inspection,		Assumption: operator cannot exceed recommended regulated pressure.			
Purge System	Contain purge gas Touch screen to provide operator Interface suitable for	components Loss of containment (major leakage) Touch screen not suitable for Class	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in	open and blockage in v line Component Rupture	PRV downstream of regulator Rated components, acceptance testing the checks, trailer ventilation	pressure gauge, audible if PRV activates ing, Operator inspection, Audible	2 :	Assumption: operator cannot exceed recommended regulated pressure.			
,	Contain purge gas Touch screen to provide	components Loss of containment (major leakage)	components causing component damage Waste of purge gas, oxygen displacement in trailer	open and blockage in v	PRV downstream of regulator Rated components, acceptance testing the checks, trailer ventilation	pressure gauge, audible if PRV activates ing, Operator inspection,	2 :	Assumption: operator cannot exceed recommended regulated pressure.			
Purge System	Contain purge gas Touch screen to provide operator Interface suitable for	components Loss of containment (major leakage) Touch screen not suitable for Class	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in	open and blockage in v line Component Rupture	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list	2 :	Assumption: operator cannot exceed recommended regulated pressure.			
Purge System	Contain purge gas Touch screen to provide operator Interface suitable for	components Loss of containment (major leakage) Touch screen not suitable for Class	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in	open and blockage in v line Component Rupture	Rated components, acceptance testing the checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing the checks are components.	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list	2 :	Assumption: operator cannot exceed recommended regulated pressure.			
Purge System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed)	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems	9 component Rupture 9 Non-rated display insta 7 Loss of air supply	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list	2 :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel	9 line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm	4 3	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed)	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems	9 component Rupture 9 Non-rated display insta 7 Loss of air supply	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low	2 :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks	9 component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical)	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm	4 3	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel	9 line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm	4 3	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks	9 line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (conti	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection	2 i	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials Solenoid credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection	4 :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Not able to test or defuel tanks	9 line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (conti	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection	2 i	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contisignal)	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison,	2 i	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes	9 line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (conti	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage	9 Ine 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c.	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contrained) Faulty thermocouple, contrained	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison,	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System Tank System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, b.	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown control comparison, alarm/shutdown control comparison, alarm/shutdown	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contrained) Faulty thermocouple, contrained	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison,	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System Tank System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, b.	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, h. gas	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple credentials, redundant thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Control System Sequencing System Sequencing System Sequencing System Tank System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, b.	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple credentials, redundant thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, h. gas	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, h. gas	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, trailer ventilation Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple credentials, redundant thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, c. gas Faulty thermocouple, h. gas	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System	Contain purge gas Touch screen to provide operator interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, of gas Faulty thermocouple, he gas Damaged/defective gai	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Coperator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Operator inspection	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C) Pressure Indication	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, of gas Faulty thermocouple, he gas Damaged/defective gai	Rated components, acceptance testing checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testing checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundang thermocouple element in tank Thermocouple credentials, redundang thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Coperator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Operator inspection	2 : : : : : : : : : : : : : : : : : : :	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System Purge System H2 Receiving System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C) Pressure Indication Temperature Measurement	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low Pressure fail null Temperature fail null	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure reading Bad data	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contribute) signal) Faulty thermocouple, of gas Faulty thermocouple, he gas 4 Damaged/defective gas 5 Faulty thermocouple	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction 3 Thermocouple credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Operator inspection Control comparison, alarm/shutdown sequence Operator inspection Control comparison, alarm/shutdown sequence Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence	2 3 1 2 3 2 3 2 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 4 3 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 4 3 4 3 4 3 4 3 4 4 3 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 4	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD Determine how this this processed by controls. Determine how this this processed by			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C) Pressure Indication Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low Pressure fail null	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure reading	9 Open and blockage in v line 9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (contissignal) Faulty thermocouple, cases gas Faulty thermocouple, bases gas Damaged/defective gases	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction 3 Thermocouple credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Control comparison, alarm/shutdown sequence Operator inspection Operator inspection	2 3 1 2 3 2 3 2 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 4 3 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 4 3 4 3 4 3 4 3 4 4 3 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 4	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD Determine how this this processed by controls.			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System Purge System H2 Receiving System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C) Pressure Indication Temperature Measurement (+/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low Pressure fail null Temperature fail null	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure reading Bad data	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contribute) signal) Faulty thermocouple, of gas Faulty thermocouple, he gas 4 Damaged/defective gas 5 Faulty thermocouple	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Thermocouple credentials 3 Thermocouple credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control System flag Control System flag	2 3 1 2 3 2 3 2 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 3 4 3 4 3 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 3 4 3 3 4 4 3 4 3 4 3 4 3 4 4 3 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 3 4 3 4 4 4	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD Determine how this this processed by controls. Determine how this this processed by			
Purge System Control System Sequencing System Sequencing System Sequencing System Tank System Tank System Purge System Purge System H2 Receiving System	Contain purge gas Touch screen to provide operator Interface suitable for Class 1, Div 2 Valve control of Sequencing System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System Bi-direction gas flow to/from Tank System In-tank Temperature Measurement (+/- 1°C) In-tank Temperature Measurement (+/- 1°C) Pressure Indication Temperature Measurement (-/- 1°C) Pressure Measurement (-/- 1°C) Pressure Measurement (-/- 1°C) Pressure Measurement (-/- 1°C)	components Loss of containment (major leakage) Touch screen not suitable for Class 1, Div 2 Unable to open valve(s) (Note: valves are normally closed) No flow of hydrogen from Tank System No flow of hydrogen from Tank System Temperature fail high Temperature fail low Pressure fail low Pressure fail null Temperature fail null	components causing component damage Waste of purge gas, oxygen displacement in trailer Non rated electronics in classified area Unable to transfer gas between systems Not able to test or defuel tanks Not able to test or defuel tanks Fail to detect gas temperature that is too low causes component damage Fail to detect gas temperature that is too high causes component damage Regulated purge pressure set higher than expected Lack of confidence in pressure reading Bad data	9 Component Rupture 9 Non-rated display insta 7 Loss of air supply Valve fails closed (mechanical) Valve fails closed (air supply - solenoid failure Valve fails closed (contribute) signal) Faulty thermocouple, of gas Faulty thermocouple, he gas 4 Damaged/defective gas 5 Faulty thermocouple	Rated components, acceptance testic checks, trailer ventilation 1 Touch Screen credentials Rated components, acceptance testic checks, pressure switch, operating procedure 2 Valve credentials 2 Solenoid credentials DAQ credentials Thermocouple credentials, redundant thermocouple element in tank Thermocouple element in tank Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction Gauge credentials, calibration check plan, flow control downstream is secondary flow restriction 3 Thermocouple credentials	pressure gauge, audible if PRV activates ing, Operator inspection, Audible Design, equipment list ing, Operator inspection, Low air supply pressure alarm Operator inspection Operator inspection Control comparison, alarm/shutdown sequence Control System flag Control System flag	2 3 4 5 2 3 4 4 5 4 5 4 5 6 6 6 6 6 6 6 6 6 6 6 6 6	Assumption: operator cannot exceed recommended regulated pressure. Include Touch Screen classification in device manual Alarm/shutdown sequence TBD Alarm/shutdown sequence TBD Determine how this this processed by controls. Determine how this this processed by			

	In	I								la			
Tank System	Pressure Measurement (0.1%	Pressure fail null	Bad data	5 F	Faulty pressure transducer	3 PT credentials	Control System flag	2	30	Determine how this this processed by controls.			
Turk System	Controlled unidirectional	Tressure run nun	Sud dutu		dury pressure transdacer	. To redeficient	control system ring	_	- 55	controls.			
	Purge gas passage to												
Purge System	Sequencing System	Low gas flow to sequencing system	Slow purging		Obstruction in gas line ncorrect upper/lower	Operating instructions/procedures	Operator inspection	3	30				
					Temperautre Limit								
			Operator not alerted to		Setpoints, signal output					Link back to individual sensors in other			
Control System	System alarms when Temperature Limits exceeded		potential temperature sensor problem		fails (Digital output module)	DAQ credentials, robust commissioning device alarms	Operator inspection	3	30	systems, maintenance captured in device manual			
Control System	Temperature Limits exceeded	3611301 <-400 01 2000	problem	J	noutie)	2 device diairiis	Operator inspection	,	30	manuai			
	Connection to H2 dispenser				High ambient moisture,	SAE J2600 H70, protected during							
H2 Receiving System	nozzle Hydrogen passage from H2	Stuck Connection (frozen) No flow of gas from Receiving	Cannot remove nozzle		oack to back fills Valve fails closed	4 transport, plastic cap	Operator inspection	1	28				
Sequencing System	Receiving System	system	Not able to test			2 Valve credentials	Operator inspection	2	28				0
Soquencing System	Hydrogen passage from H2 Receiving System	No flow of gas from Receiving	Not able to test		Valve fails closed (air supply - solenoid failure)	2 Solenoid credentials	Operator inspection	2	28				
Sequencing System		system No flow of gas from Receiving	Not able to test		Valve fails closed (control	2 Solenoid Credentials	Operator inspection		28				
Sequencing System	Receiving System	system	Not able to test	7 si		2 DAQ credentials	Operator inspection	2	28				
		No flow of hydrogen to Tank			Valve fails closed								
Sequencing System	Tank System	System	Not able to test	7 (r	mechanical)	2 Valve credentials	Operator inspection	2	28				0
	Bi-direction gas flow to/from	No flow of hydrogen to Tank		V	Valve fails closed (air								
Sequencing System	Tank System	System	Not able to test		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		Valve fails closed (control signal)	2 DAQ credentials	Operator inspection	2	28				
		No flow of nitrogen to/from Tank			Valve fails closed	THE RESERVE	,						
Sequencing System	Tank System	System	Not able to purge tanks	7 (r	mechanical)	2 Valve credentials	Operator inspection	2	28				
	Bi-direction gas flow to/from	No flow of nitrogen to/from Tank		V	Valve fails closed (air								
Sequencing System	Tank System	System	Not able to purge tanks	7 s	supply - solenoid failure)	2 Solenoid credentials	Operator inspection	2	28				
		No flow of nitrogen to/from Tank			Valve fails closed (control								
Sequencing System	Tank System Connection to purge gas	System	Not able to purge tanks	7 si	signal) No nitrogen supply on site	2 DAQ credentials	Operator inspection	2	28	Check TDG requirements, etc. Nitrogen on-			
Purge System	supply tank	No connection	No purging		or delivered	4 Operator training, test planning	Operator inspection	1	28	board v. delivered.			
	Controlled unidirectional												
Duran Custom	Purge gas passage to	No see flow to convencing auston	No nursing possible	7 0	Ball valve fails closed	Ball valve credentials, operating instructions/procedures	Onesetes increation	,	28				0
Purge System	Sequencing System Controlled unidirectional	No gas flow to sequencing system	No purging possible	/ 6	sali valve falis closed	2 instructions/procedures	Operator inspection	2	28				
	Purge gas passage to					Regulator credentials, operating							
Purge System	Sequencing System	No gas flow to sequencing system	No purging possible	7 R	Regulator fails	instructions/procedures	Operator inspection	2	28				
	Controlled unidirectional Purge gas passage to					Needle valve credentials, operating							
Purge System	Sequencing System	No gas flow to sequencing system	No purging possible	7 N	Needle Valve fail closed	2 instructions/procedures	Operator inspection	2	28				
U2 Danis in a Contact	Connection to H2 dispenser	Lance Commention	Name of the same o		2	2 Out and the links	0		27				
H2 Receiving System	nozzle	Loose Connection	Nozzle pop-off	9 0	Operator Error	3 Operator training	Operator inspection	1	21				
		Loss of containment (major	Hydrogen Leakage external to							System conrols shutdown below PRV set	Note: PRV removed from Sequencing		
Sequencing System	Contain Hydrogen	leakage)	trailer under dispenser canopy	9 P	PRV Failure	1 PRV credentials	None	3	27	pressure	system as determined by Project Team		
		Tanks not vented when subjected		т	FPRD Fails to activate when					Sandia's quantitative risk assesment.			
Tank System	Vent tanks in case of fire	to fire	Tank damage		subjected to fire	1 TPRD credentials	Operator inspection	3	27	Consider fire/heat detection in device			
			Explosive concentration in		10.5								
Control System	Hydrogen Sensors	No H2 sensor reading	trailer with no hydrogen detection	9 0	H2 Sensor loose	Monitored by dection panel causing alarm condition, trailer vent	Supervised Input	1	27	Sensor shutdown plan	Shutdown plan included in Alarm Matrix		
7	Connection to H2 dispenser						, , , , , , , , , , , , , , , , , , ,			,			
H2 Receiving System	nozzle	No connection	No fueling		Operator Error	3 Operator training	Operator inspection	1	24		<u> </u>		
H2 Receiving System	Unidirectional Hydrogen Passage from Nozzle	Hydrogen not able to pass through receptacle	No hydrogen flow		Pressure too high in Receiving System	3 Operator training	Operator inspection	1	24				
, , , , , , , , , , , , , , , , , , ,			70.		0 - 1 · · ·	-							
	Di direction and flow to fire	No flow of hydrogen from Tax	Not able to test or defuel		Valve fails closed (air	Rated components, acceptance testing,	Operator inspection, Low						
Sequencing System	Tank System	No flow of hydrogen from Tank System			supply source failure)	checks, pressure switch, operating procedure	air supply pressure alarm	1	24	Add to main P&ID			
	Touch screen to provide operator Interface suitable for		Operator unable to interact	_	DAQ hardware/software	DAQ hardware credentials, robust							
Control System	Class 1, Div 4	Touch screen inoperable	with control system, no further testing		failure	3 commissioning	Operator inspection	1	24				
	In-line Temperature					-	·			Determine how warning/alarm processed			
Tank System	Measurement (+/- 1°C)	Temperature fail null		4 F	aulty thermocouple	3 Thermocouple credentials	Control System flag	2	24	by controls.			
Sequencing System	Pressure Indication to control panel	Pressure fail high	Lack of confidence in digital pressure	3 0	Damaged/defective gauge	Gauge credentials, calibration check	Operator inspection	4	24				0
ocquencing system	Pressure Indication to control	r ressure fair flight	Lack of confidence in digital	3 D	Jamagea/ derective gauge	Gauge credentials, calibration check	орегатог пізрестоп	-	-4		+		Ü
Sequencing System	panel	Pressure fail low	pressure	3 D	Damaged/defective gauge	2 plan	Operator inspection	4	24				
	Pressure Indication to control		Lack of confidence in digital			Gauge credentials, calibration check							
Sequencing System	Pressure Indication to control panel	Pressure fail null	pressure, operator to replace gauge	3 D	Damaged/defective gauge	2 plan	Operator inspection	4	24				
	Pressure Indication to control		Lack of confidence in digital			Gauge credentials, calibration check							
Tank System	panel Pressure Indication to control	Pressure fail high	pressure Lack of confidence in digital	3 D	Damaged/defective gauge	2 plan Gauge credentials, calibration check	Operator inspection	4	24		 		0
Tank System	panel	Pressure fail low		3 D	Damaged/defective gauge	2 plan	Operator inspection	4	24				
			Lack of confidence in digital				Í						
Tank Systom	Pressure Indication to control panel	Pressure fail null	pressure, operator to replace	,	Damaged/defective course	Gauge credentials, calibration check	Operator inspection	4	24				
Tank System	paner	r ressure rair fluii	gauge	ا د	Damaged/defective gauge	- İbiaii	Operator inspection	4	24	1	+		

											T.			
	Uludragan nassaga ta										Filter installation procedure detection will			
H2 Receiving System	Hydrogen passage to Sequencing System	No gas flow to sequencing system	No testing possible	7 Clo	logged Filter	3 Ope	erating instructions/procedures	Operator inspection	1	21	Filter installation procedure, detection will be improved if included			0
0.7	Hydrogen passage to		Up and the second				,,,,	.,			,			
H2 Receiving System	Sequencing System	No gas flow to sequencing system	No testing possible	7 Ob	bstruction in gas line	3 Ope	erating instructions/procedures	Operator inspection	1	21				
						Rate	ed components, acceptance testing,							
	Hydrogen passage from H2	No flow of gas from Receiving		Val	alve fails closed (air		cks, pressure switch, operating	Operator inspection, Low						
Sequencing System	Receiving System	system	Not able to test	7 sup	upply source failure)	3 proc	cedure	air supply pressure alarm	1	21	Add to main P&ID			
						Rate	ed components, acceptance testing,							
	Bi-direction gas flow to/from	No flow of hydrogen to Tank		Val	alve fails closed (air		cks, pressure switch, operating	Operator inspection, Low						
Sequencing System	Tank System	System	Not able to test	7 sup	upply source failure)	3 proc	cedure	air supply pressure alarm	1	21	Add to main P&ID			
						Rate	ed components, acceptance testing,							
		No flow of nitrogen to/from Tank			alve fails closed (air		cks, pressure switch, operating	Operator inspection, Low						
Sequencing System	Tank System	System	Not able to purge tanks	7 sup	upply source failure)	3 proc	cedure	air supply pressure alarm	1	21	Add to main P&ID			
Purge System	Connection to purge gas supply tank	No connection	No purging	7 On	perator Error	3 One	erator training	Operator inspection	1	21				
r dige system	эарргу сатк	THE CONTINUESTION	rio parging	, 05	Jerator Error	Орс	. acci craming	operator inspection	-					
							ige credentials, calibration check							
Defuel System	Pressure Indication	Pressure fail null	Lack of confidence, no readout	5 Da	amaged/defective gauge		n, flow control downstream is ondary flow restriction	Operator inspection	2	20				
					amage,defect or		,							
112 Descriping Control	Connection to H2 dispenser	Lacca Connection	Norrio non off		bstruction to	2 5:	annear Leak Cheek	Operator inco-stiles		10				
H2 Receiving System	nozzle Connection to purge gas	Loose Connection	Nozzle pop-off		ozzle/receptacle onnected to non-nitrogen		penser Leak Check Inector designed for N2 (inert gas) T	Operator inspection	1	18				
Purge System	supply tank	Connection to wrong supply gas			as supply	1 cylin		Operator inspection	2	18				
			Explosive concentration in		<u> </u>		nitarad by daction non-1							
Control System	Hydrogen Sensors	No H2 sensor reading	trailer with no hydrogen detection	9 H2	2 Sensor power failure		nitored by dection panel causing m condition, trailer vent	Supervised Input	1	18	Sensor shutdown plan	Shutdown plan included in Alarm Matrix		
	,,						,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				р.	, , , , , , , , , , , , , , , , , , , ,		
								Operating Inspections						
	Controlled unidirectional gas	Uncontrolled release of gas to	Tank temperature to cold,	Flo	low control valve open	Cont	trolled stop/shutdown if any in-tanl	Operating Inspections, k Procedures, Audible.						
Defuel System	exhaust to atmosphere	atmosphere	liner damage				sors <-40 C	Control system detection	1	16				
								Operating Inspections,						
								Procedures, pressure						
	Controlled unidirectional gas	Uncontrolled release of gas to	Tank temperature to cold,	Fai	ailed regulator increases	Cont	trolled stop/shutdown if any in-tanl	indicator for operator,						
Defuel System	exhaust to atmosphere	atmosphere	liner damage	8 pre	ailed regulator increases ressure		sors <-40 C	detection	1	16				
·			_											
	Touch screen to provide operator Interface suitable for		Operator unable to interact with control system, no			Tour	ch Screen credentials, laptop							
Control System	Class 1, Div 2	Touch screen inoperable	further testing	8 Fau	aulty/damaged display	2 back		Operator inspection	1	16	Review using laptop in classified area			0
	Touch screen to provide operator Interface suitable for		Operator unable to interact with control system, no	Co	onnection to DAQ system	Cont								
Control System	Class 1, Div 3	Touch screen inoperable					nection cable credentials, lanton							
		Touch screen moperable	further testing	8 fail	iled	2 back	nection cable credentials, laptop kup	Operator inspection	1	16				
			Not able to automatically					Operator inspection	1	16				
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to	Va	alve fails closed	2 back	kup		1					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 Not able to automatically	Va	alve fails closed	2 back		Operator inspection Operator inspection	2	16				0
		No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to	4 (m	alve fails closed mechanical) alve fails closed (air	2 back	kup ve credentials	Operator inspection		16				0
Sequencing System Sequencing System	Gas passage to Defuel System Gas passage to Defuel System	No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel Not able to automatically	4 (m	alve fails closed mechanical) alve fails closed (air	2 back	kup		2	16				0
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to	Val 4 (m Val 4 sup	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control	2 Valve 2 Sole	ve credentials enoid credentials	Operator inspection Operator inspection	2	16				0
		No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically	Val 4 (m Val 4 sup	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control	2 Valve 2 Sole	kup ve credentials	Operator inspection	2	16				0
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel tanks, need to manually defuel	Val 4 (m Val 4 sup Val 4 sig	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control	2 Valv 2 Sole 2 DAQ	ve credentials enoid credentials	Operator inspection Operator inspection	2	16				0
Sequencing System	Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to	4 Value Valu	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control	2 Valv 2 Sole 2 DAQ	ve credentials enoid credentials Q credentials	Operator inspection Operator inspection	2	16				0
Sequencing System Sequencing System	Gas passage to Defuel System Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected	Val 4 (m Val 4 sup Val 4 sig	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal)	2 Valv 2 Sole 2 DAQ 2 Gau	ve credentials enoid credentials Q credentials uge credentials, calibration check	Operator inspection Operator inspection Operator inspection	2	16 16				
Sequencing System Sequencing System	Gas passage to Defuel System Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel tanks, need to manually defuel Regulated defuel pressure set	4 Val 4 sup Val 4 sig	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal)	2 Valv 2 Sole 2 DAQ 2 Gau	ve credentials enoid credentials Q credentials age credentials, calibration check age credentials, calibration check	Operator inspection Operator inspection Operator inspection	2	16 16				
Sequencing System Sequencing System Defuel System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected	Val 4 sup Val 4 sup Val 5 pa	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to	2 back 2 Valv 2 Sole 2 DAQ Gauplan Gauplan Conn	enoid credentials Coredentials Quedentials Ige credentials, calibration check	Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4	16 16 16				0
Sequencing System Sequencing System Defuel System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set	Val 4 sup Val 4 sup Val 5 pa	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amaged/defective gauge	2 back 2 Valv 2 Sole 2 DAQ Gauplan Gauplan Conn	ve credentials enoid credentials Q credentials age credentials, calibration check age credentials, calibration check	Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4	16 16 16				0
Sequencing System Sequencing System Defuel System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected	Val 4 sup Val 4 sup Val 5 pa	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to	2 Valv 2 Sole 2 DAQ Gauplan Gauplan Contrans	enoid credentials Coredentials Quedentials Ige credentials, calibration check	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4	16 16 16				0
Sequencing System Sequencing System Defuel System Purge System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to	Val 4 (m Val 4 sup Val 4 sig 2 Da Da 7 cor Val	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to onnector	2 back 2 Valv 2 Sole 2 DAQ Gauq 2 plan Conr 2 tran: Ratec chec	enoid credentials Q credentials Ige credentials Ige credentials, calibration check Ige credentials, calibration check Innector assembly stored during Insport ed components, acceptance testing, cks, pressure switch, operating	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4 1 1	16 16 16 16 16				0
Sequencing System Sequencing System Defuel System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel of tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically	Val 4 (m Val 4 sup Val 4 sig 2 Da Da 7 cor Val	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to onnector	2 back 2 Valv 2 Sole 2 DAQ Gauq 2 plan Conr 2 tran: Ratec chec	ve credentials credentials credentials ge credentials, calibration check nector assembly stored during assport ed components, acceptance testing,	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4	16 16 16				0
Sequencing System Sequencing System Defuel System Purge System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to	Val 4 (m Val 4 sup Val 4 sig 2 Da Da 7 cor Val	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to onnector	2 back 2 Valv 2 Sole 2 DAQ Gauq 2 plan Conr 2 tran: Ratec chec	enoid credentials Q credentials Ige credentials Ige credentials, calibration check Ige credentials, calibration check Innector assembly stored during Insport ed components, acceptance testing, cks, pressure switch, operating	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection	2 2 4 4 1 1	16 16 16 16 16				0
Sequencing System Sequencing System Defuel System Purge System Purge System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to	Val (m Val sup Val 4 sig Val 2 Da Da 7 con Val 4 sup Val	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amage or defect to onnector	2 Valv 2 Sole 2 DAQ Gauplan Gauplan Conn 2 trans Rate chec a proc	enoid credentials Q credentials Ige credentials Ige credentials, calibration check Ige credentials, calibration check Innector assembly stored during Insport ed components, acceptance testing, cks, pressure switch, operating	Operator inspection Operator inspection, Low air supply pressure alarm	2 2 4 4 1 1	16 16 16 16 16			1	0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks	Val (m Val sup Val 4 sig Val 2 Da Da 7 con Val 4 sup Val	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control gnal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure)	2 Valv 2 Sole 2 DAQ Gauplan Gauplan Conn 2 trans Rate chec a proc	ve credentials enoid credentials credentials ge credentials, calibration check ge credentials, calibration check nucctor assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure	Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures	2 2 4 4 1 1 1	16 16 16 16 16 14			1	0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks	4 (m	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control gnal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure)	2 Valv 2 Sole 2 DAQ Gauq 2 plan Gauq 2 plan Rate chec 3 proc	ve credentials enoid credentials credentials ge credentials, calibration check ge credentials, calibration check nucctor assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure	Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections,	2 2 4 4 1 1 1	16 16 16 16 16 14			1	0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System Tank System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system No hydrogen flow from sequencing system	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel anks, need to manually defuel Regulated to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks	4 (m	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control gnal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure)	2 Valv 2 Sole 2 DAQ Gauq 2 plan Gauq 2 plan Rate chec 3 proc	enoid credentials Q credentials Q credentials age credentials, calibration check nector assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures Operating Inspections, Procedures	2 4 4 1 1 1 1	16 16 16 16 16 11 11 12 12				0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System Tank System Tank System	Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System Gas passage to/from Sequencing System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system No hydrogen flow from sequencing system No nitrogen flow to/from	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated to to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks Not able to defuel tanks	Val 4 (m Val 4 sig 2 Da 2 Da 7 Cot Val 4 suj 4 Ma	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure) Annual ball valves closed Manual ball valves closed	2 Valv 2 Sole 2 DAQ Gauqu 2 plan Gauqu 2 plan Conri 2 tran: 3 Ope	enoid credentials coredentials coredentials ge credentials ge credentials, calibration check nector assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure erating instructions/procedures	Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures Operating Inspections, Procedures Operating Inspections, Procedures	2 2 4 4 1 1 1 1 1 1	16 16 16 16 14 12 12				0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System Tank System	Gas passage to Defuel System Gas passage to Defuel System Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system No hydrogen flow from sequencing system	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel anks, need to manually defuel Regulated to manually defuel Regulated defuel pressure set lower than expected Regulated purge pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks	Val 4 (m Val 4 sig 2 Da 2 Da 7 Cot Val 4 suj 4 Ma	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control gnal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure)	2 Valv 2 Sole 2 DAQ Gauqu 2 plan Gauqu 2 plan Conri 2 tran: 3 Ope	enoid credentials Q credentials Q credentials age credentials, calibration check nector assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures Operating Inspections, Procedures	2 4 4 1 1 1 1	16 16 16 16 16 11 11 12 12				0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System Tank System Tank System Tank System	Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System Gas passage to/from Sequencing System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system No hydrogen flow from sequencing system No nitrogen flow to/from sequencing system No nitrogen flow to/from sequencing system	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel Regulated defuel pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks Not able to test Not able to test Not able to purge tanks Not able to purge tanks Not able to automatically purge tanks, need to manually	Value	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control ignal) amaged/defective gauge amaged/defective gauge amage or defect to onnector alve fails closed (air upply source failure) fanual ball valves closed fanual ball valves closed fanual ball valves closed	2 back 2 Valv 2 Sole 2 DAQ Gauq 2 plan Conr 2 tran Rate chec 3 proc 3 Ope 3 Ope	enoid credentials Coredentials Quedentials Ige credentials Ige credentials, calibration check Ige credentials Ige	Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures Operating Inspections, Procedures Operating Inspections, Procedures	2 2 4 4 1 1 1 1 1 1	16 16 16 16 16 11 12 12 12			1	0 0
Sequencing System Sequencing System Defuel System Purge System Purge System Sequencing System Tank System Tank System	Gas passage to Defuel System Pressure Indication Pressure Indication Connection to purge gas supply tank Gas passage to Defuel System Gas passage to/from Sequencing System Gas passage to/from Sequencing System Gas passage to/from Sequencing System	No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System No flow of hydrogen to Defuel System Pressure fail high Pressure fail high No connection No flow of hydrogen to Defuel System No hydrogen flow to sequencing system No hydrogen flow from sequencing system No nitrogen flow to/from sequencing system No nitrogen flow to/from sequencing system	Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Not able to automatically defuel tanks, need to manually defuel Regulated tanks, need to manually defuel tanks, need to manually defuel Regulated defuel pressure set lower than expected No purging Not able to automatically defuel tanks, need to manually defuel Not able to defuel tanks Not able to defuel tanks Not able to test	Value	alve fails closed mechanical) alve fails closed (air upply - solenoid failure) alve fails closed (control gnal) amaged/defective gauge manage or defect to onnector alve fails closed (air upply source failure) fanual ball valves closed fanual ball valves closed	2 back 2 Valv 2 Sole 2 DAQ Gauq 2 plan Conr 2 tran Rate chec 3 proc 3 Ope 3 Ope	enoid credentials coredentials coredentials ge credentials ge credentials, calibration check nector assembly stored during sport ed components, acceptance testing, cks, pressure switch, operating cedure erating instructions/procedures	Operator inspection Operator inspection, Low air supply pressure alarm Operating Inspections, Procedures Operating Inspections, Procedures Operating Inspections, Procedures	2 2 4 4 1 1 1 1 1 1	16 16 16 16 14 12 12			1	0 0

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