U.S. Department
of Transportation
National Highway
Traffic Safety
Administration

www.nhtsa.gov

DOT HS 811 075 February 2009

Failure Modes and Effects Analysis for Hydrogen Fuel Cell Vehicles – Subtask 1

Final Report

DISCLAIMER

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. DOT HS 811 075	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Failure Modes and Effects Analysis for Hydrogen Fuel Cell Vehicles – Subtask 1		5. Report Date February 2009 6. Performing Organization Code
7. Author(s) Denny R. Stephens, Susan E. Rose, Stephanie A. Flamberg, Stephen M. Ricci, and Paul E. George II		8. Performing Organization Report No.
9. Performing Organization Name and Address Battelle Memorial Institute 505 King Ave Columbus, OH 43201		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTNH22-02-D-02104
12. Sponsoring Agency Name and Address National Highway Traffic Safety Administration 1200 New Jersey Avenue SE. Washington, DC 20590		13. Type of Report and Period Covered Final 14. Sponsoring Agency Code Office of Applied Vehicle Safety Research – Structures and Restraints Research Division, NVS-321
15. Supplementary Notes		

16. Abstract

Hydrogen fuel cell vehicles (HFCVs) offer the promise of significantly reducing the amount of pollutants expelled into the environment. However, the technology that is needed to store the hydrogen fuel onboard and deliver it to the propulsion system is different from what consumers and even engineers currently know and understand. As an early step in identifying critical safety requirements for these vehicles and, if needed, developing appropriate Federal Motor Vehicle Safety Standards, the National Highway Traffic Safety Administration requested that Battelle undertake a high-level failure modes and effects analysis to characterize potential hazards from compressed-hydrogen fuel cell vehicles and identify potential safety issues. The objective of this effort is to review and assesses safety issues for hydrogen vehicles and to identify areas that NHTSA may consider addressing in the FMVSS.

The investigation found that, overall, the failure modes that appear to have the greatest hazard in hydrogen vehicles are large releases of hydrogen and rupture of the fuel container. The FMEA results show that if high-pressure components in compressed-hydrogen fuel systems lack redundancy, a single-point failure of the container, PRD, or first valve, can result in a large-scale release or venting of hydrogen and, for containers, release of mechanical energy. Small releases of hydrogen and rupture of other components may also be hazardous, but do not have the potential destructive force of large releases and fuel container rupture.

17. Key Words hydrogen, fuel cell, compressed hydrogen, fuel storage, FMEA, HFCV, risk, hazard	18. Distribution Statement This report is free of charge from the NHTSA Web site at www.nhtsa.dot.gov

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 170	22. Price

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

TABLE OF CONTENTS

Page

Executive Summary .... **v**

Acronyms and Abbreviations .... **vii**

1.0 Introduction **1**
- 1.1 Project Objectives 1
- 1.2 Technical Approach 2

2.0 NHTSA and FMVSS Background **4**

3.0 Elements of Compressed-Hydrogen Fuel Cell Vehicles **6**
- 3.1 Hydrogen Fueling and Fuel Storage Subsystem 8
- 3.2 Hydrogen Fuel Delivery Subsystem 9
- 3.3 Fuel Cell Subsystem 9
- 3.4 Electric Propulsion and Power Management Subsystem 10

4.0 Unique Hazards of Compressed-Hydrogen Vehicles **11**
- 4.1 Combustion Hazards 11
- 4.2 High-Pressure Hazards 14
- 4.3 Electrical Hazards 16
- 4.4 Crash Hazard 18
- 4.5 Fire Hazards 20

5.0 Failure Modes and Effects Analysis of Compressed-Hydrogen Fuel Cell Vehicle **21**
- 5.1 Description of the FMEA Development Process 21
- 5.2 Description of the Results 24

6.0 Comparison of FMEA Results With Fuel Cell Vehicle Codes and Standards **52**
- 6.1 Review of Codes and Standards 52
- 6.2 Review of FMEA and Related Codes and Standards 53
- 6.3 Potential Gaps in Standards 72

7.0 Resulting Assessment of Safety Issues **75**
- 7.1 High-Consequence Failure Modes 76
- 7.2 Root Causes and Design Controls 77
- 7.3 Highly Variable Hazards 78

8.0 References **81**

Appendix A: Summary of Hydrogen Vehicle Codes and Standards **A-1**
- SAE Recommended Practices A-1
- ISO Safety Specifications A-8
- CSA Draft Standards A-13
- Japanese HFCV Standard A-16
- European Working Group A-19

Appendix B: Failure Modes and Effects Analysis of Compressed-Hydrogen Fuel Cell Vehicles With Codes and Standards **B-1**

TABLE OF CONTENTS (Continued)

Page

List of Tables

Table 1. Organization of FMVSS Standards 5
Table 2. Comparative Transportation Fuel Properties 12
Table 3. HFCV Concept Model Systems, Subsystems, and Components 22
Table 4. Likelihood Categories 24
Table 5. Consequence Categories 24
Table 6. FMEA of Compressed-Hydrogen Fuel Cell Vehicle 28
Table 7. Overview of FCV Codes and Standards 54
Table 8. Summary of Content of Compressed FCV Codes, Standards, and Analogous FMVSS 57
Table 9. Summary of HFCV FMEA and Codes and Standards 61

List of Figures

Figure 1. High-Level Schematic of Compressed-Hydrogen Fuel Cell Vehicle Subsystems 7
Figure 2. Schematic of Compressed-Hydrogen Fuel Cell Vehicle Component Locations and Mass Distribution 7
Figure 3. Comparison of Fuels on a Mass Energy Density Basis 15
Figure 4. Comparison of Fuels on a Volumetric Energy Density Basis 15
Figure 5. Conventional Time/Current Zones of Effects of AC Currents (15 Hz to 100 Hz) on Persons for a Current Path Corresponding to Left Hand to Feet (Source: IEC 60479-1) 17
Figure 6. Conventional Time/Current Zones of Effects of DC Currents on Persons for a Longitudinal Upward Current Path (Source: IEC 60479-1) 18
Figure 7. Schematic of Compressed-Hydrogen Fuel Cell Vehicle Component Locations and Mass Distribution 19
Figure 8. Simplified Diagram of Compressed-Hydrogen Fuel Cell Vehicle Systems 23
Figure 9. Risk Matrix 24

EXECUTIVE SUMMARY

Hydrogen-fueled vehicles offer the promise of significantly reducing the amount of pollutants expelled into the environment. However, the technology that is needed to store the hydrogen fuel onboard and deliver it to the propulsion system is different from what consumers and even engineers currently know and understand. As an early step in identifying critical safety requirements for these vehicles and, if needed, develop appropriate Federal Motor Vehicle Safety Standards, the National Highway Traffic Safety Administration requested that Battelle undertake a high-level failure modes and effects analysis to characterize potential hazards from compressed-hydrogen fuel cell vehicles and identify potential safety issues. The objective of the effort reported here is to review and assesses safety issues for hydrogen vehicles and to identify areas that NHTSA may consider addressing in the FMVSS.

Along with NHTSA, other government and industrial organizations are looking closely at hydrogen vehicle safety needs and are developing standards for hydrogen vehicle components, integrated subsystems (fuel storage and delivery, electrical, etc.) and fully integrated hydrogen vehicles. It is expected that NHTSA will not need to duplicate the work that is being done elsewhere to address safety of hydrogen vehicles. Consequently, Battelle has focused this assessment on two fundamental questions:

- In its regulatory function, what safety issues should NHTSA consider prioritizing for compressed-hydrogen vehicles?
- Are there potential gaps in the coverage of safety standards for compressed-hydrogen vehicles that merit NHTSA's consideration?

To address these challenging questions, Battelle adopted a structured approach that included the following activities.

- Review of NHTSA's safety objectives and the general topics addressed by the FMVSS to characterize NHTSA's potential roles in hydrogen safety;
- Review of the unique elements of compressed-hydrogen vehicles in an effort to narrow the scope of the assessment to those elements that are unique to hydrogen vehicles;
- Review of the unique hazards of compressed-hydrogen vehicles;
- Failure modes and effects analysis of a conceptual compressed-hydrogen fuel cell vehicle to characterize potential hazards and potential controls to mitigate these hazards; and
- Comparison of the results of the FMEA with fuel cell vehicle codes and standards to identify potential gaps in safety coverage that may need to be considered.

The conclusions of the investigation centered on high-consequence failure modes, root causes of failure, design controls to reduce the likelihood of failure, and potential gaps in the current codes and standards.

The investigation found that, overall, the unique failure modes that appear to have the greatest hazard in hydrogen vehicles are large releases of hydrogen and rupture of the fuel container. The FMEA results show that high-pressure components in compressed-hydrogen fuel systems lack redundancy such that single-point failure of the container, PRD, or first valve can result in a large scale release or venting of hydrogen and, for containers, release of mechanical energy. Small releases of hydrogen and rupture of other components may also be hazardous, but do not have the potential destructive force of large releases and fuel container rupture.

The primary failure modes considered in the FMEA for the compressed-hydrogen fueling and fuel storage system include leak or rupture of the fuel container, fuel delivery lines, and associated components. Consequences of a compressed-hydrogen container rupture vary depending on the circumstances. Secondary failure modes considered include failure of PRDs or valves to open or close when required.

Industry codes and standards currently exist or are in development to address the design, manufacture, installation, and integration for the safe use of compressed-hydrogen fuel containers. However there is currently no FMVSS specific to the concerns related to compressed-hydrogen fuel containers and the integrated fuel cell systems during a crash. Due to the potential severity of container failure, NHTSA may want to evaluate the sufficiency of proposed tests and standards.

As part of the FMEA process, the analysts identified typical HFCV safety features and methods designed to prevent a failure or help to mitigate potential consequences. These features and methods include crash test requirements, impact sensors, design/qualification/manufacturing/quality control/installation and maintenance requirements, fail-safe design, leak detection, pressure relief, pressure sensor, temperature sensors, thermal protection and fire test requirements, ventilation, and voltage monitoring.

Vehicle engineering is problematic in that vehicles are used in such a wide variety of applications and environments for which worst case conditions cannot be readily defined or measured. Two examples of such hazards are vehicle crash and fire. Both are difficult to characterize because their severity depends upon multiple random variables. Nevertheless, each of these is critically important for hydrogen vehicle safety, because they have the potential to contribute to or cause serious failure modes of container rupture and/or large hydrogen release. NHTSA has successfully improved crash safety by defining minimum crash safety requirements and crash safety ratings for vehicles.

Fire is a hazard for hydrogen vehicles because it can cause catastrophic rupture of the hydrogen fuel container and fuel system if they are not properly vented. Fire is highly variable, like crash events. The potentially catastrophic nature of container burst due to fire suggests the need to consider conducting an analysis that defines typical and atypical vehicle fire scenarios, their likelihood and the likelihood they will affect fuel containers. From this, government and industry can develop a more comprehensive and representative approach to fire qualification testing, thus improving safety and reducing the likelihood of container rupture.

ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
CGA	Compressed Gas Association
CNG	compressed natural gas
EPRI	Electric Power Research Institute
EV	electric vehicle
FMEA	failure modes and effects analysis
FMVSS	Federal Motor Vehicle Safety Standards
HEV	hybrid electric vehicle
HFCV	hydrogen fuel cell vehicle
HGV	hydrogen gas vehicle
ICE	internal combustion engines
IEC	Electro Technical Commission
ISO	International Organization for Standardization
MIE	minimum-ignition energy
MPH	miles per hour
NACE	National Association of Corrosion Engineers
NFPA	National Fire Protection Agency
NGV	natural gas vehicle
NHTSA	National Highway Traffic Safety Administration
PEM	polymer electrolyte membrane – also known as proton exchange membrane
PRD	pressure relief device
PRV	pressure relief valve
QC	quality control
SAE	Society of Automotive Engineers
SUV	sport utility vehicles
UL	Underwriters Laboratories
U.S. DOT	U.S. Department of Transportation

FAILURE MODES AND EFFECTS ANALYSIS FOR HYDROGEN FUEL CELL VEHICLES

Final Report

by

Denny R. Stephens, Susan E. Rose, Stephanie A. Flamberg, Steven M. Ricci, and Paul E. George II

1.0 INTRODUCTION

Hydrogen-fueled vehicles offer the promise of significantly reducing the amount of pollutants expelled into the environment. Furthermore, hydrogen can be generated from any of a number of diverse energy sources, including hydrocarbon, nuclear, solar and wind, thereby helping address energy security as well as environmental concerns. While very promising from both perspectives, the technology needed to store hydrogen fuel onboard and deliver it to the propulsion system is different from what consumers, mechanics, fire safety personnel, the public, and even engineers currently know and understand. As the number of hydrogen vehicles increases, the likelihood of hazardous events will also increase. Although hydrogen vehicles present new challenges, government, industry, and the public expect that they will not be more hazardous to own and operate than conventional gasoline- or diesel-fueled vehicles.

Recognizing that hydrogen vehicles are becoming a reality, the National Highway Traffic Safety Administration is taking a proactive approach to identifying critical safety requirements for these vehicles and, if needed, developing appropriate Federal Motor Vehicle Safety Standards to ensure the safety of passengers and the public. As an early step in this effort, NHTSA has requested that Battelle undertake two tasks relevant to safety of hydrogen fueled vehicles: Subtask 1 activities included a failure modes and effects analysis to characterize potential hazards from compressed-hydrogen fuel cell vehicles and identify potential safety issues. Subtask 2 activities included a review of available data and the drafting of a viable electrical isolation test procedure for compressed-hydrogen fuel cell vehicles. This document is the final draft report for Subtask 1.

1.1 PROJECT OBJECTIVES

NHTSA promotes the safety of vehicles through several means, including education and regulation. One route in which NHTSA promotes vehicle safety is by setting and enforcing safety performance standards for motor vehicles and associated equipment through regulations such as those set forth in the Federal Motor Vehicle Safety Standards. The objective of this effort is to review and assesses safety issues for hydrogen vehicles and to identify areas that NHTSA may consider addressing in the FMVSS. Battelle's strategy for accomplishing this task is described in the next section.

1.2 TECHNICAL APPROACH

Compressed hydrogen is a substantially different fuel from conventional liquid gasoline and diesel fuels. While it has much in common with CNG as a vehicle fuel, its properties introduce different design and hazards concerns. Along with NHTSA, many other government and industrial organizations are looking closely at the hydrogen vehicle safety. An Internet search of hydrogen safety standards will quickly show that there is a substantial amount of work in progress now on the development of codes and standards for safety of hydrogen-fueled vehicles. Organizations conducting these efforts include the Society of Automotive Engineers, the International Organization for Standardization, and CSA America. The Japanese and the European Working Group have also developed technical standards for hydrogen vehicles. These include unique standards for hydrogen vehicle components, integrated subsystems (fuel storage and delivery, electrical, etc.) and fully integrated hydrogen vehicles. It is expected that NHTSA will not need to duplicate the work that is being done worldwide to address safety of hydrogen vehicles. Consequently, Battelle has focused this assessment on two fundamental questions:

- In its regulatory function, what safety issues should NHTSA consider prioritizing for compressed-hydrogen vehicles?
- Are there potential gaps in the coverage of safety standards for compressed-hydrogen vehicles that merit NHTSA's consideration?

To address these very challenging questions, Battelle adopted a structured and systematic approach that is organized and presented in the following sequence:

- **NHTSA and FMVSS Background –** This section provides a summary of NTHSA's safety objectives and the general topics addressed by the FMVSS to characterize NHTSA's potential role in hydrogen safety
- **Elements of Compressed-Hydrogen Vehicles –** This section contains a description of the unusual elements of compressed-hydrogen vehicles to introduce them and to narrow the scope of the assessment to those elements that are unique to hydrogen vehicles.
- **Hazards of Compressed-Hydrogen Vehicles –** This section provides a summary of the primary hazards and failure consequences of compressed-hydrogen vehicle systems including combustion, high pressure, electrical, crash, and fire hazards.
- **Failure Modes and Effects Analysis of Compressed-Hydrogen Fuel Cell Vehicle –** This section presents an evaluation of hazards by conducting a high-level failure modes and effects analysis (FMEA) to characterize the potential hazards in a generic compressed-hydrogen fuel cell vehicle and potential controls to mitigate these hazards.
- **Comparison of FMEA Results With Fuel Cell Vehicle Codes and Standards –** This section contains the results of a review of existing and developing codes and standards, including the FMVSS, to characterize current requirements and coverage. Next, the FMEA of the compressed HFCV was compared with applicable codes and standards to identify gaps in safety coverage that may need to be addressed by FMVSS.

- **Resulting Assessment of Safety Issues –** This section presents a summary of the assessment, highlighting high-consequence failure modes, root causes, design controls, and potential gaps in the current codes and standards.

This investigation is focused on compressed hydrogen, polymer electrolyte membrane (PEM) fuel cell vehicles. While other fuel storage and fuel cell options are under development, compressed hydrogen is believed to be the most likely near-term implementation. Secondly, electrical shock hazards are investigated in a complementary subtask[1] under this contract and, for completeness, are addressed, but only at a high level in this report. Last, this task has drawn liberally from a complementary contract for NHTSA being conducted in parallel[2] that is focused on collecting and summarizing current codes and standards efforts for compressed-hydrogen fuel cell vehicles.

2.0 NHTSA and FMVSS BACKGROUND

In early 2002, the Bush Administration announced the FreedomCAR initiative, an industry-government cooperative effort, to advance the development of fuel cell vehicles and associated infrastructure. The President expanded this program in 2003 with the Hydrogen Fuel Initiative with the goal of making fuel cell vehicles a practical and cost-effective choice of Americans by 2020.[3] NHTSA's safety initiative complements these efforts through risk assessment studies to quantify potentially unsafe conditions, development of performance tests to address these conditions, and evaluation of procedures to ensure hydrogen-fueled vehicles exhibit an equivalent level of safety to that of conventionally fueled vehicles.

As identified earlier, one route in which NHTSA promotes vehicle safety is by setting and enforcing safety performance standards for motor vehicles through the FMVSS. The safety philosophy of NHTSA has been to establish performance standards where possible rather than prescribe design standards. That is, instead of explicitly specifying the material or size of seat belt webbing or brake hoses, the regulations establish various tests of strength to allow manufacturers to select any material or design capable of passing the tests. NHTSA does not certify vehicles for compliance with the FMVSS; manufacturers must certify the vehicles themselves. NHTSA does conduct tests of vehicles on the market, sometimes on its own initiative and sometimes in response to consumer complaints, and it can order a recall if a vehicle does not meet one of the standards or has a safety-related defect.

The majority of the FMVSS are organized into three groups, which essentially cover safety performance of a vehicle before, during, and after a crash. Table 1 gives a general overview of how the FMVSS are organized.

Table 1. Organization of FMVSS Standards

Series Number	Description of Standards
100	Series of standards intended to prevent crashes. Topics include: • Lighting • Braking • Tires
200	Series of standards that govern occupant protection during a crash. Topics include: • Seating systems • Seat belts • Child restraint systems
300	Series of standards that govern flammability of interior materials and the integrity of fuel systems. Topics include: • Fuel system integrity (conventional fuels and CNG) • Flammability of interior materials • Electric powered vehicles

Note: A few standards, pertaining to non-crash safety and to low-speed vehicles, fall outside the scope of the above three groups.

A vehicle is made of many parts, and therefore there are standards that regulate the safety of the vehicle as a whole, as well as a vehicle's individual systems and components. For example, FMVSS No. 135; Light Vehicle Brake Systems, prescribes stopping distances, which are a test performed on the entire vehicle. There are additional tests specific to the braking system in that failures of the system must be induced. Requirements on the reservoir capacity and resistance to leaks govern subsystems of the braking system. Finally, there are regulations at the component level, such as those on the label height and wording (FMVSS No. 135 and FMVSS No. 101) and about brake fluid (FMVSS No. 116).

3.0 ELEMENTS OF COMPRESSED-HYDROGEN FUEL CELL VEHICLES

Battelle carried out a project for the Safety Working Group of USCAR in 2004[4 5] that included a survey of hydrogen vehicles at that time. It showed that hydrogen fuel cells are currently being implemented on existing vehicle platforms, including compact cars such as the Mercedes A-class, minivans such as the Dodge Caravan and sport utility vehicles such as the Ford Explorer. It is expected that, in the near term, hydrogen propulsion will be implemented on existing vehicle platforms, and only in the longer term will new platforms designed specifically for hydrogen propulsion be developed. The survey assessment showed that the construction of a fuel cell drivetrain and fuel storage systems is significantly different from that of conventional, fossil-fueled vehicles.

The 2004 Survey of Potential Safety Issues With Hydrogen-Powered Vehicles Report for the Safety Working Group of USCAR highlighted that many different fueling options are being considered for hydrogen vehicles, such as storing hydrogen onboard in compressed or cryogenic liquefied form, or producing hydrogen from hydrocarbons using onboard reformers. There is substantial flexibility in configuring a fuel cell system and innovative approaches appear regularly. At the forefront of hydrogen-powered vehicle technology are the compressed hydrogen fueled fuel cell vehicle systems that are the most advanced in design and are likely to be the first hydrogen vehicles to the market. For these reasons, the focus of this Task is on compressed hydrogen fueled vehicle systems, illustrated schematically in Figure 1. Figure 2 illustrates one auto manufacturer’s implementation.

Hydrogen fuel cell vehicles have an electric drivetrain powered by a fuel cell that generates electricity electrochemically from hydrogen. The major subsystems as illustrated in Figure 1 are:

- Hydrogen fueling and fuel storage subsystem;
- Hydrogen fuel delivery subsystem;
- Fuel cell subsystem; and
- Electric propulsion and power management subsystem.

In addition to these primary subsystems, some FCVs are equipped with other advanced technologies to increase efficiency, such as regenerative braking systems that capture the energy lost during braking and store it in an upsized battery. Following is a description of each of these subsystems and their typical location within a hydrogen vehicle drivetrain.

The focus of this study is on the hydrogen fueling and fuel storage, hydrogen fuel delivery, and fuel cell and therefore does not address the electric propulsion and power management subsystem.

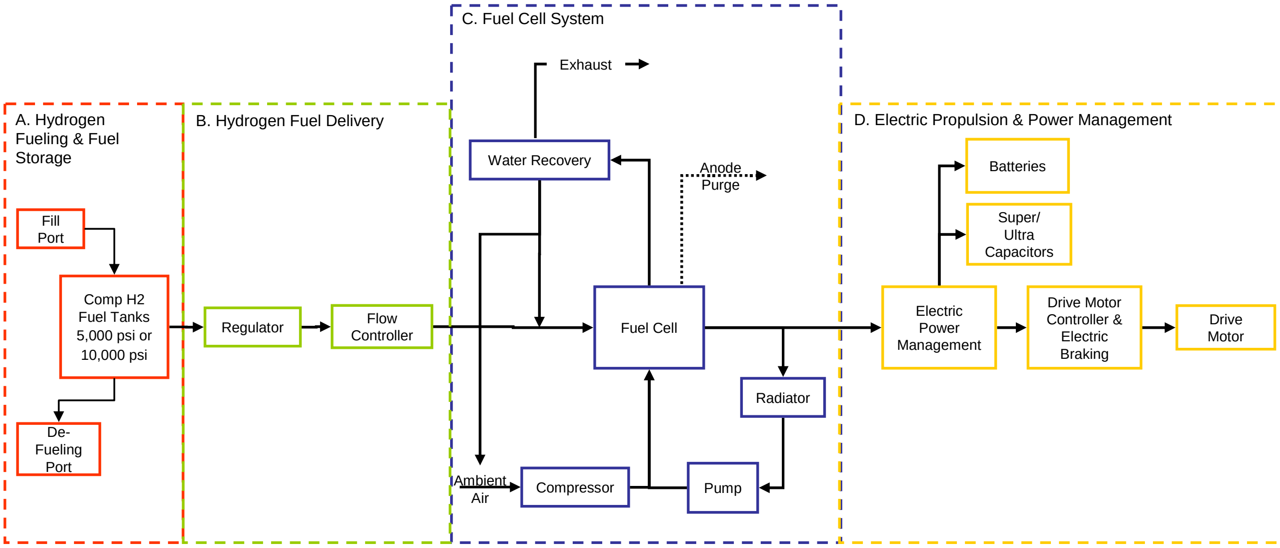


Figure 1. High-Level Schematic of Compressed-Hydrogen Fuel Cell Vehicle Subsystems

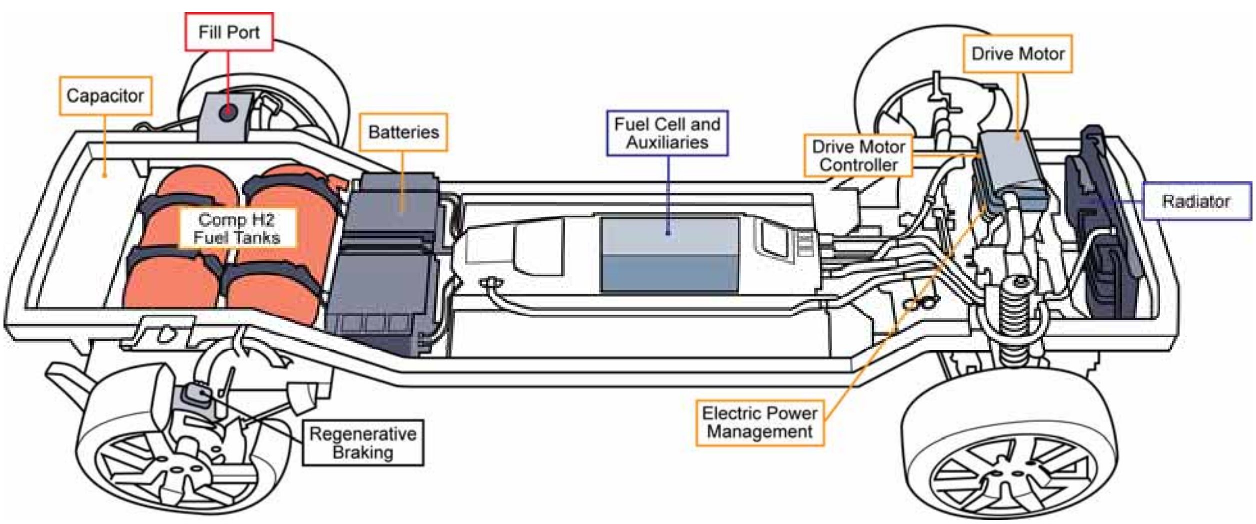


Figure 2. Schematic of Compressed-Hydrogen Fuel Cell Vehicle Component Locations and Mass Distribution

3.1 HYDROGEN FUELING AND FUEL STORAGE SUBSYSTEM

At present, the most common method of storing and delivering hydrogen fuel onboard is in compressed gas form. Hydrogen is typically stored on current developmental vehicles at 5,000 psi (34.5 MPa).[*] Compressed-hydrogen systems operating at 10,000 psi (70 MPa) are also in development. The hydrogen fuel from the storage containers is supplied to the fuel cell by pressure piping with two or three stages of regulation that reduce the pressure to approximately 5 psi (.034 MPa) before entering the fuel cell stack. For this report, fuel storage and delivery are discussed separately.

The primary components within the hydrogen fueling and fuel storage subsystem are the compressed-hydrogen fuel containers. Because the hydrogen fuel has a low energy density per unit volume, storage containers must be designed to supply an adequate amount of hydrogen to achieve realistic vehicle driving ranges. Hydrogen fuel containers and fuel cell stacks also add weight and cost to the vehicle that compounds the challenge of achieving desirable driving ranges. To overcome these limitations, hydrogen fuel containers are being designed to take up as little space as possible using lightweight composite materials. In addition, these fuel containers are specially designed to allow the storage of hydrogen at very high pressures to overcome the low energy density. These fuel containers are designed and tested to safety standards such as ANSI/CSA HGV2, Basic Requirements for Compressed-Hydrogen Gas Vehicle (HGV) Fuel Containers, CSA B51, Part 2 Boiler, Pressure Vessel and Pressure Piping Code, SAE J2579, Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles, and ISO DIS 15869.2, Gaseous Hydrogen and Hydrogen Blends – Land Vehicle Fuel Tanks. These standards are intended to ensure the tanks maintain high pressures and prevent leakage or rupture in the rigors of vehicle service.

Currently, containers constructed with composite materials meet the high-pressure, lower-container-weight design challenges and are already in use in prototype hydrogen-powered vehicles. Most high-pressure hydrogen fuel containers evaluated at the time of this study were constructed of multi-component systems typically described as either a Type 3 or Type 4 container. A Type 3 container is typically constructed with an inner aluminum liner that serves as the gas-containing membrane, wrapped with a load-bearing carbon fiber composite structural layer. The Type 4 container is similar in concept to the Type 3 container except that the inner liner is constructed of a permeation-resistant thermoplastic liner.

Fuel containers are typically located in the rear of the vehicle, mounted transversely in front of or above the rear axle, as shown in Figure 2. Hydrogen fuel containers are pressure vessels, whether or not the fuel is compressed or liquefied. Consequently, hydrogen fuel containers will be cylindrical vessels for the foreseeable future to reduce weight, particularly for the higher-pressure vessels. Even so called “conformable containers” in development are based upon packaging of multiple cylindrical or near-cylindrical containers.

[*] Some early developmental vehicles stored hydrogen at 3,600 psi (24.8 MPa), using natural gas vehicle fuel system components.

In addition to the fuel containers, the hydrogen fuel storage system consists of a number of auxiliary components needed for fueling/de-fueling and system safety such as pressure relief devices and container shut-off valves.

In the event of a fire, pressure relief devices (PRDs) vent (i.e., provide a controlled release at a remote site) the gas contained in compressed-hydrogen fuel containers to prevent rupture. High temperatures in a fire will degrade the strength of metal, thermoplastic, and composite container materials and raise the internal pressure of the container, potentially causing rupture.

PRD venting of hydrogen vehicle fuel containers in the event of a fire is different from conventional boiler and pressure vessel applications, where pressure relief valves allow venting of temporary overpressures and the devices reseat and reseal after the pressure is returned to normal conditions. In conventional applications, overpressures typically arise from internal heating of the vessel contents and there is no damage to the vessel. PRDs for hydrogen vehicle fuel containers are intended solely to prevent container rupture in the event of an external fire. Containers and PRDs that have been subjected to fire should be removed from service and destroyed. Hence, these PRDs are designed to vent the entire contents of the container rapidly and do not reseat or allow repressurization of the container.

3.2 Hydrogen Fuel Delivery Subsystem

Hydrogen is delivered from the storage containers to the fuel cell stack via a series of piping, pressure regulators, valving, filters, and flow meters. The fundamental purpose of a hydrogen flow control system is to reliably deliver fuel to the fuel cell stack at a specified, stable pressure and temperature for proper fuel cell operation over the full range of vehicle operating conditions. Fuel must be delivered at a specified rate, even as the pressure in the fuel containers drop or the ambient temperature changes. The fuel system delivery specifications are determined by the initial container storage pressure, the vehicle, and the vehicle duty cycle.

Since sections of the piping system will see container pressures of up to 10,000 psig (70 MPa) standards intend to ensure they are designed and tested to maintain this pressure safely without leakage or rupture throughout their service life.

3.3 Fuel Cell Subsystem

The fuel cell provides the electricity needed to operate the drive motors and charge vehicle batteries and/or capacitors. There are several kinds of fuel cells, but Polymer Electrolyte Membrane (PEM) – also known as Proton Exchange Membranes - fuel cells are the type typically used in automobiles at this time. The PEM fuel cell consists of a “stack” of hundreds of cells in which hydrogen and oxygen combine electrochemically to generate electrical power. Fuel cells are capable of continuous electrical generation when supplied with pure hydrogen and oxygen, simultaneously generating electricity and water, with no carbon dioxide or other harmful emissions typical of gasoline-powered internal combustion engines.

In this report, the “fuel cell subsystem” consists of a number of auxiliary components needed for the effective and efficient operation. These components include such items as an air pump for supply air to the stack and heat exchangers to recover waste heat and maximize efficiency. Figure 1 illustrates that, while this class of fuel cell is intended to operate on nearly pure hydrogen, the system includes some form of intermittent purge to remove diluents and contaminants to extend the life of the fuel cell.

Likely due to the inherently flat nature of the stack itself, most of the fuel cell and auxiliaries are packaged in a flat box located between the front and rear axles, under the passenger compartment. The same is true for hydrogen concept cars, suggesting that fuel cell and vehicle manufacturers expect this to be the typical location for the fuel cell package.

The electricity generated by the fuel cell is used to drive electric motors that ultimately propel the vehicle. Because fuel cells within vehicles operate at high voltage and, in some cases, are equipped with auxiliary propulsion batteries, they are designed to standards that intend to avoid the risk of electrical shock, loss of isolation, and potential ignition of surrounding materials.

3.4 Electric Propulsion and Power Management Subsystem

Hydrogen fuel cell vehicles are powered by electric motors in which the electrical energy provided by the fuel cell is converted to the mechanical energy necessary to drive the wheels of the vehicle. The electric drive system has similarities to electric vehicles. It may also use batteries and ultracapacitors similar to those used in hybrid vehicles.

Many hydrogen fuel cell vehicles are front-wheel drive, typically with the electric drive motor and drivetrain located in the “engine” compartment mounted transversely over the front axle. This pattern is consistent for small fuel cell automobiles that are similar in size to existing economy cars. Some larger SUV-type fuel cell vehicles are all-wheel drive with two electric motors, one each over the front and rear axle, while other designs use four compact motors, one at each wheel. In this study the FMEA assumes a front-wheel-drive fuel cell vehicle.

Generally the electrical power generated by the fuel cell may go directly to the end use or may be stored in a capacitor or battery when needed for acceleration. Since fuel cell voltage varies with load, a key aspect of power management is voltage control for the fuel cells and voltage conversion to the desired output. In automotive applications, the power will primarily be used by the propulsion system with auxiliary power units powering components such as valves, sensors, fans, and compressors.

Some fuel cell propulsion system designs have batteries and/or ultracapacitors to buffer the power delivery from the cell. These are also used to recapture energy during stopping through regenerative braking. However, as fuel cell technologies advance they are increasingly able to scale their electric output to meet the propulsion needs of the vehicle, eliminating the need for a battery buffer on many vehicles. It is expected that manufacturers will try to minimize the use of batteries to reduce both cost and weight from the vehicle. It is unclear whether batteries will be needed for regenerative braking energy storage in future fuel cell vehicles. If the fuel cell efficiency is sufficient, this may not be required.

4.0 UNIQUE HAZARDS OF COMPRESSED-HYDROGEN VEHICLES

Hydrogen is clearly different from conventional gasoline and diesel fuels. It is a gas that must be stored onboard at high pressure or as a cryogenic liquid. It tends to dissipate when released and does not pool. It has a much broader flammability range (fuel/air ratio) than conventional fuels. While these and other characteristics are different, the potential hazards of hydrogen can be prevented or mitigated through sound, systematic engineering methods. Sound engineering can ensure that hydrogen vehicles are as safe in total as conventional vehicles, although the individual hazards are different.

Prior to exploring the failure modes and effects analysis, this section of the report provides a description of some key safety hazards of compressed-hydrogen fuel cell vehicles. The discussion that follows is organized into five broad categories:

- Combustion hazards;
- High pressure hazards;
- Electrical hazards;
- Crash hazards; and
- Fire hazards.

These categories have been introduced in the technical literature.[3]

4.1 COMBUSTION HAZARDS

The literature has ample documentation of combustion hazards associated with hydrogen.[6 7 8] Before discussing hydrogen fuel specifically, the basic principles of flammability (i.e., the "fire triangle") need to be considered. With any fuel, for ignition to be possible the following elements must occur simultaneously:

1. A flammable chemical, with a concentration within its flammability limits;
2. An oxidant, at a concentration putting the combustible in its flammable range; and
3. A thermal or electrical ignition source having some minimum energy.

If all three prerequisites are satisfied, ignition and either deflagration (subsonic combustion) or detonation (supersonic combustion) can take place, creating the fire hazard.

To provide a basis for characterizing hydrogen chemical and combustion risks and hazards, Table 2 lists average data for the relevant fuel properties for gasoline, natural gas, and hydrogen.

As a first characterization, hydrogen is odorless. Unlike gasoline vapor and natural gas, which are typically spiked with odorant, hydrogen offers no olfactory warning signal of its presence. Similar to natural gas and gasoline vapor, hydrogen is colorless.

The basic risks and hazards assessed were as follows:

(1) Stored energy in the fuel to be released upon ignition;
(2) Likelihood of becoming flammable;
(3) Likelihood of being ignited; and
(4) Consequences of ignition.

Recognizing that hydrogen and natural gas are gases, whereas gasoline is a liquid under normal conditions of use, comparisons here are made with gasoline vapor. This exclusion eliminates the need to discuss apples-versus-oranges differences in terms of other metrics, such as vapor pressure and flash point.

Table 2. Comparative Transportation Fuel Properties

Fuel Property	Gasoline	Natural Gas	Hydrogen
Buoyancy (density as a percent of air, %)	~400	~55	~7
Diffusion Coefficient (centimeters per second squared, cm/s^2)	~0.5	~0.16	~0.61
Lower Calorific Fuel Value (mega-Joules/kilogram, MJ/kg)	~45	~50	~120
TNT Equivalent of Fuel	~0.38	~0.42	~1
Lower Calorific Mixture Value (mega-Joules/cubic meter, $MJ/m^{3)}$	~4.5	~3.1	~2.9
Lower Flammability Limit (%)	~1	~5	~4
Upper Flammability Limit (%)	~8	~15	~75
Lower Detonation Limit (%)	~1	~6	~18
Upper Detonation Limit (%)	~3	~14	~59
Stoichiometric Concentration (%)	~1.8	~9.5	~30
Minimum Ignition Temperature (°C)	~370	~630	~580
Minimum Ignition Energy (milli-Joules, mJ)	~0.2	~0.3	~0.02
Minimum Quenching Distance (millimeters, mm)	~2.8	~1.2	~0.6
Adiabatic Flame Temperature (°C)	~1,250	~2,050	~2,250
Maximum Overpressure Ratio	~5.1	~7.7	~8.4
Maximum Explosion Overpressure (pounds per square inch, psi)	~75	~110	~125
Maximum Flame Speed (meters/second, m/s)	~0.5	~0.4	~3.2
Relative Thermal Radiation (%)	~50	~33	~10

References: 8,9

The goal of this analysis was to determine, using common characteristics, the comparative degree of risks and hazards posed by the transportation fuels under consideration. The goal was to reveal characteristics that were “more, less, or equally hazardous.” The results of this comparative assessment of relative risks are summarized as follows:

- On a mass, fuel-only calorific basis, hydrogen has about three times the energy content of gasoline, a value nearly equivalent to TNT, a solid high explosive, which sounds very hazardous. However, on a volumetric, fuel-air mixture calorific basis, gasoline-air has about twice the energy content as a hydrogen-air mixture.

- Because gasoline vapor has the lowest lower flammability limit (a critical flammability-limit metric for unconfined or open-air releases), it appears to be more hazardous than hydrogen in terms of how little quantity of released fuel is needed to create a flammable atmosphere. However, because it is flammable over a 10-times wider range of concentrations, hydrogen has a greater probability of being present at flammable levels during leaks.

- Because gasoline has the lowest lower detonation limit (a critical flammability-limit metric for confined releases), it appears to be more hazardous than hydrogen in terms of how little quantity of released fuel is needed to create a detonable (supersonic combustion) atmosphere. However, because it is detonable over a 20-times wider range of concentrations, hydrogen has a greater probability of being present at levels during leaks that could result in detonation. Moreover, it is more difficult to initiate the detonation of gasoline and natural gas than hydrogen, which itself requires on the order of 10 kilo-Joules.

- During leaks into the open air, gasoline accumulates as a liquid on surfaces or in a pool, then evaporates slowly, allowing extended time for a “fuel source” to be active, whereas, because of its high buoyancy and diffusivity in air, hydrogen would disperse very rapidly and allow only a limited duration over which any mixture of it in air were within its flammability range. Moreover, hydrogen dispersion would be up and away from the source, whereas gasoline vapor would remain close to ground level.

- During leaks into confined spaces, gasoline vapor tends to increase in concentration from the bottom (floor) up, soon exceeding its upper flammability limit, whereas hydrogen will tend to increase in concentration from the top (ceiling) down, and remain flammable for a longer period of time because of its nearly 10-times higher upper flammability limit.

- Because it requires the lowest minimum-ignition temperature, gasoline would appear to be more prone to ignite in air than hydrogen or natural gas when exposed to a hot surface. This effect is a function of the nature of the hot surface, and is quite variable.

- Because it requires 10-times lower minimum-ignition energy (MIE), hydrogen would be more prone to ignite in air than gasoline vapor or natural gas when exposed to the discharge of static electricity. For reference, the spark from a human electrostatic discharge can be up to 500 times that needed to ignite hydrogen. However, this comparison needs qualification because MIE usually occurs at near-stoichiometric fuel/air ratios. At off-stoichiometric fuel/air ratios, especially near the lower and upper flammability limits, the MIE for hydrogen, natural gas, and gasoline become comparable (~10 mJ), and, therefore, are equally safe (or hazardous).

- Hydrogen has been known to self-ignite during rapid discharge. While hydrogen has a low MIE, the exact ignition mechanism is unknown. It may be caused by heating during discharge due to negative Joule-Thomson effects or charging and electrical discharge of small particles in the air.[10][11]

- If ignited, hydrogen leaks burn with a non-luminous, nearly invisible and difficult-to-detect bluish flame. (These flames are more easily seen in the dark.) In contrast, the flames of hydrocarbon-based fuels are luminous (reddish-yellow), because of the incandescence of the soot present.
- Because it emits about 5 times less thermal radiation as a gasoline vapor-air fire, a hydrogen-air fire has a much lower propensity to cause skin burns on subjects outside of the fire zone in the case of a large substantial “venting” or “blowdown” release of hydrogen.
- Because of its 6-times faster burning velocity, which reflects overall reaction rate, hydrogen fires can be of much shorter duration than fires involving gasoline vapor or natural gas.
- Hydrogen-air flames will more readily propagate through structures because hydrogen flames have the smallest quenching distance. A hydrogen flame will not be prevented from passing though openings as readily as fires involving gasoline vapor and natural gas.
- Because it has the hottest adiabatic flame temperature, hydrogen-air deflagration (sub-sonic combustion) generates about a 1.5-times higher maximum explosion overpressure, which would directly translate into more physical damage as a result of the explosion. If the ignition resulted in a detonation instead of a deflagration, the magnitude of the resulting overpressure could be up to 20 times higher on a TNT-equivalent basis. Such detonation is more prone in confined spaces than in the open air.

As illustrated, the risks and hazards of hydrogen as a transportation fuel are sometimes better, sometimes worse, and sometimes different from hydrocarbon-based transportation fuels. This does not imply one fuel is inherently safer than another, merely that the appropriate engineering controls must be developed and applied for each to ensure the overall desired level of safety is achieved.

4.2 High-Pressure Hazards

While the energy content per unit mass of hydrogen is substantially more than other fuels, because it is naturally a gas, its energy content per unit volume is low. Hydrogen must be compressed to high temperatures or liquefied at cryogenic temperatures in order to fit enough fuel onboard vehicles to achieve typical driving ranges. Figures 3 and 4 compare fuels on a mass and volumetric basis. Due to the low volumetric energy content, the industry is developing compressed-hydrogen fueling and storage technology that operates at nominal 5,000 (34.5 MPa) and 10,000 psi (70 MPa), whereas natural gas vehicles nominal operating pressure is 3,600 psi (24.8 MPa). Hence, in addition to the chemical energy stored in hydrogen, there is substantial potential mechanical energy stored in the gas itself, as well as the container in which it is stored. The potential mechanical energy of 1 kg of hydrogen compressed to 5,000 (34.5 MPa) and 10,000 psi (70 MPa) is roughly the equivalent of 0.58 and 0.61 kg of TNT.

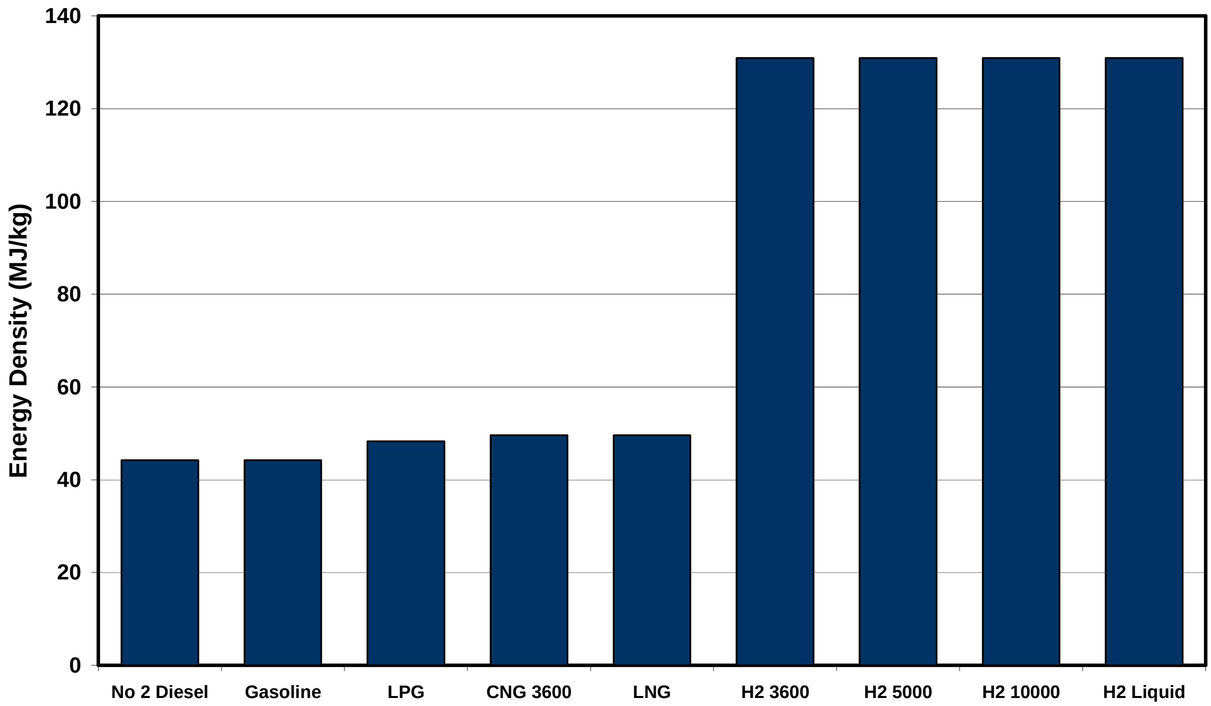


Figure 3. Comparison of Fuels on a Mass Energy Density Basis

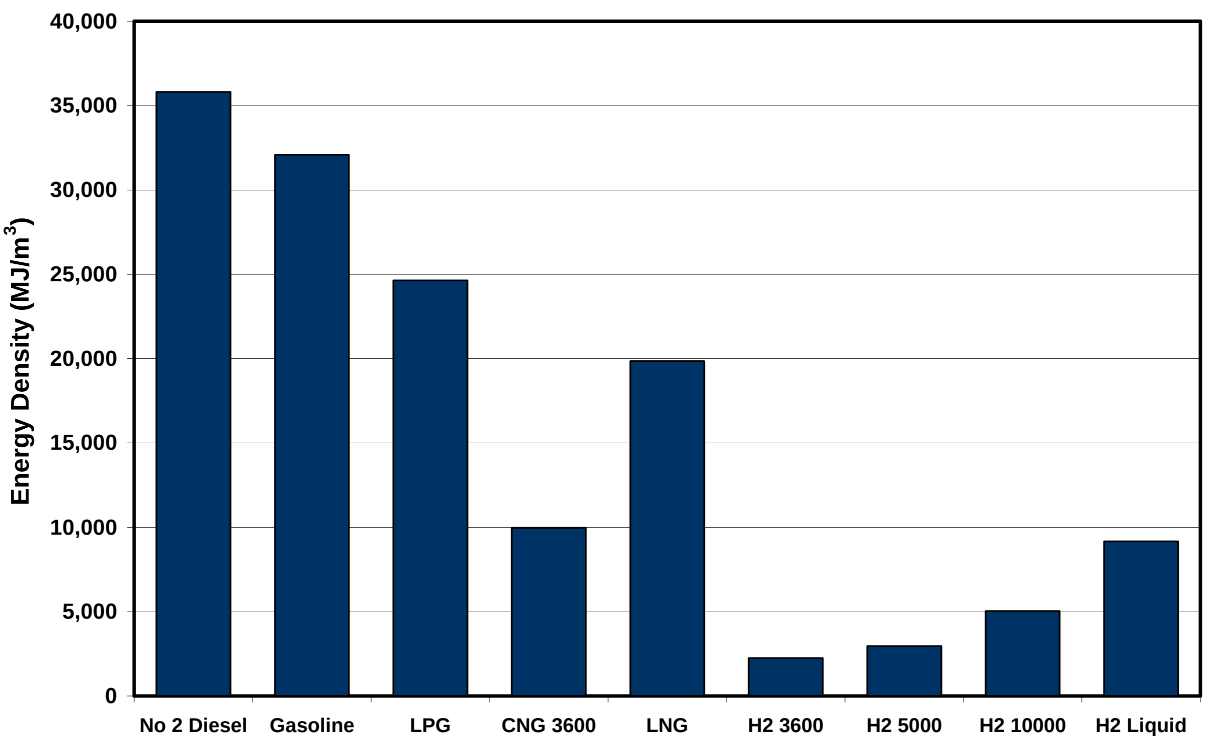


Figure 4. Comparison of Fuels on a Volumetric Energy Density Basis

Clearly failure of fuel containers resulting in an explosive release of the potential mechanical energy and chemical energy of compressed hydrogen is not acceptable. Indeed standards for fuel container design are intended to ensure they are rugged and durable and will not rupture in the most severe service. They are designed and tested to prevent failure due to

- improper design, installation, or maintenance of equipment;
- external fire impacting the fuel storage container and/or associated supply components;
- external mechanical damage to equipment; or
- external chemical damage to equipment (i.e., battery acid).

The minimum burst pressure of 5,000 (34.8 MPa) and 10,000 (70 MPa) psi fuel containers is over 11,000 (75.8 MPa) and 22,000 psi (151.7 MPa) respectively. This results in high-strength composite containers that are typically greater than ¾ inch thick and far stronger than the surrounding vehicle.

As noted earlier, compressed hydrogen is not inherently less safe than other fuels. The same level of safety can be achieved with hydrogen as other fuels with suitable engineering design and manufacturing controls.

4.3 Electrical Hazards

Electrical energy has been on board automobiles since inception. From the addition of lighting and electrical starters, battery voltages have increased from 6 volts to 12 volts. More recently, two PowerNet 42V battery systems have been proposed,[12] [13] but have not been widely fielded. These electrical systems have a long running history and are widely understood. Recently hybrid electric vehicles from a variety of manufacturers have been introduced to the public market. Vehicle manufacturers report the batteries used in their hybrids range from approximately 150 volts dc to nearly 300 volts. Manufacturers report the output voltage of vehicle fuel cells may be of the order of 480 volts. This information suggests that electrical safety research and policies applying to HEV batteries are expected to be applicable to fuel cell vehicles.

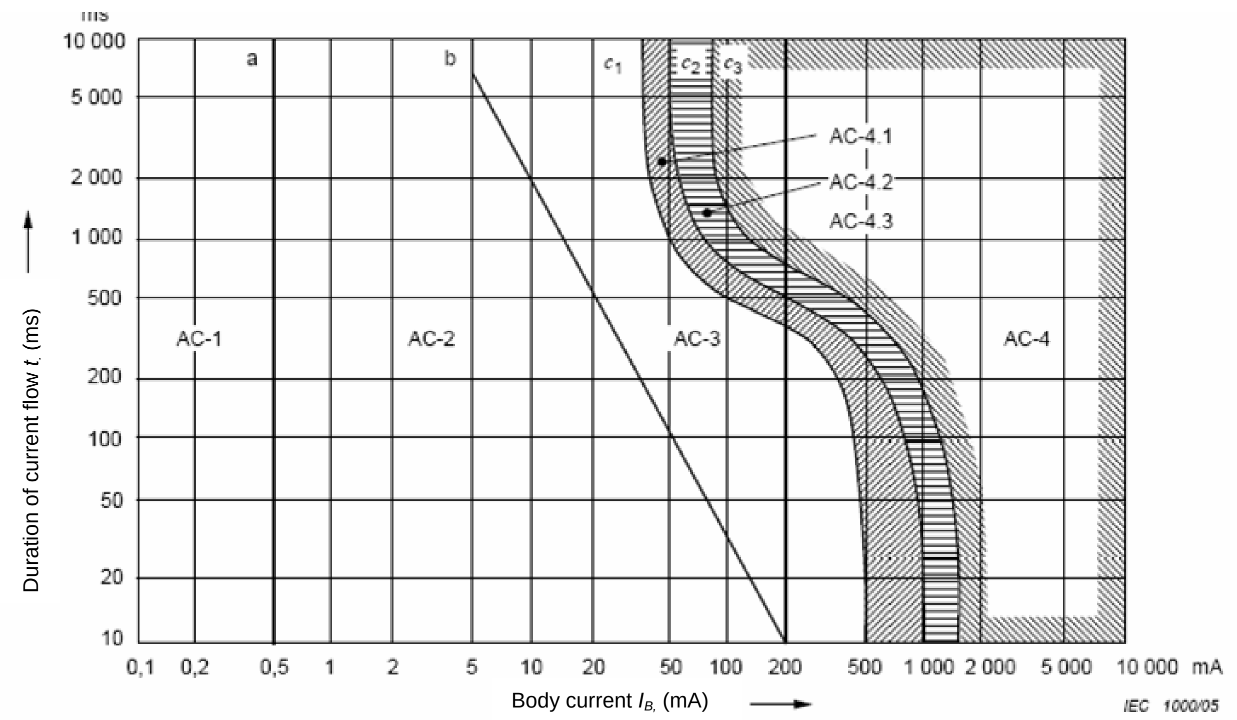
The voltage and current available on fuel cell vehicles is certainly sufficient to cause cardiac arrest, breathing arrest, burns or other cellular damage (IEC 60479-1 Zone 4) if an individual were to come into contact with exposed conductors. For normal vehicle operating conditions, normal methods of electrical isolation protection are sufficient for both fuel cell voltages and currents. However, protecting the driver, passengers, repair technicians, and first responders in the event of an accident is unique from past experience and is under careful consideration. [*]

---

[*] Existing standards applicable to fuel cell vehicle electrical safety consideration include:
- SAE J1766-2005, "Recommended Practice for Electric and Hybrid Electric Vehicle Battery Systems Crash Integrity Testing"
- CEI IEC 60479-1, Technical Report, "Effects of current on human beings and livestock"

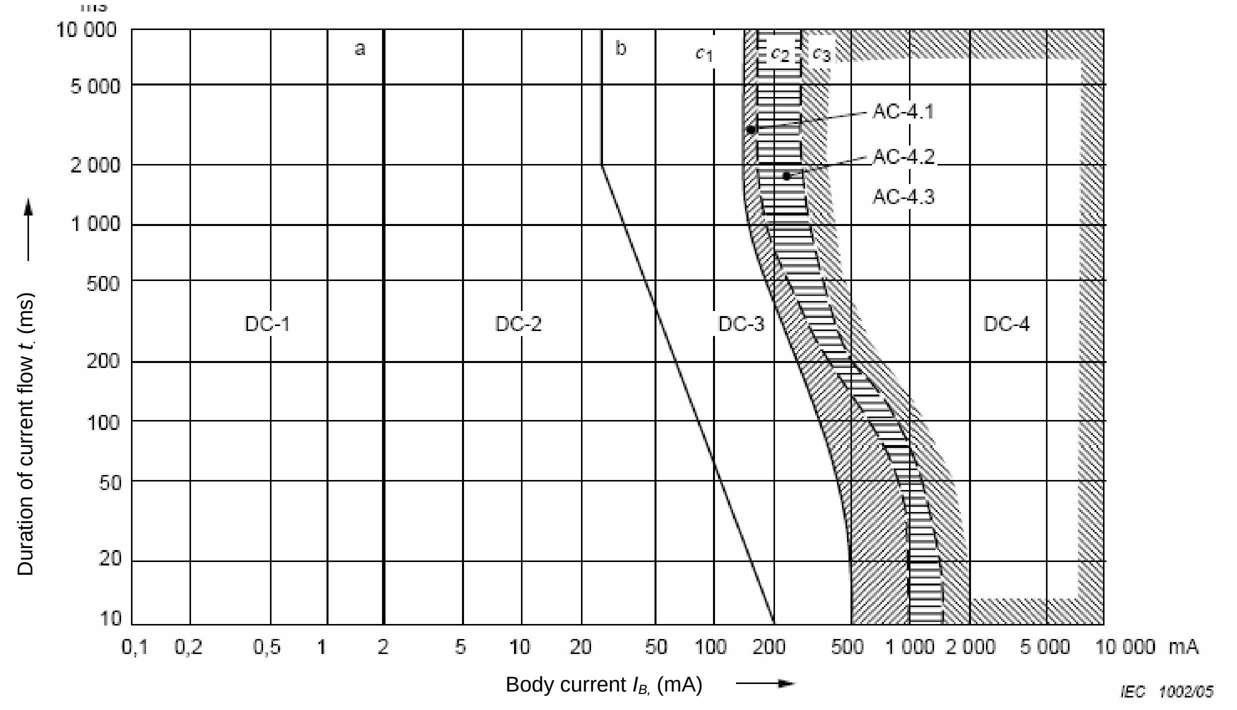
A detailed analysis of fuel cell automotive crash electrical hazards is presented in the final report of Battelle contract DTNH22-02-D-02104, Task Order 08, prepared for the National Highway Traffic Safety Administration. This report evaluates the J1766 recommended practices and the effects on the human body model as defined by IEC 60479-1. The report also considers the special dc and ac current super position case.

The Society of Automotive Engineers' J1766-1998 was updated to J1766-2005 to include recommended practices for automotive fuel cells and revisions for isolation requirements. The Ohms per volt threshold for physiological effects have been revised. Segregating alternating current and direct current thresholds as illustrated in Figures 5 and 6. The recommended practice keeps the electrical shock hazard within the IEC AC-2 and DC-2 zone as shown in the figures.



AC-1	Perception possible, but usually no "startled" reaction
AC-2	Perception and involuntary muscular contractions likely but usually no harmful electrical physiological effects
AC-3	Strong involuntary muscular contractions. Difficulty in breathing. Reversible disturbances of heart function. Immobilization may occur. Effects increasing with current magnitude. Usually no organic damage to be expected.
AC-4	Patho-physiological effects may occur such as cardiac arrest. Breathing arrest and burns or other cellular damage. Probability of ventricular fibrillation increasing with current magnitude and time.

Figure 5. Conventional Time/Current Zones of Effects of AC Currents (15 Hz to 100 Hz) On Persons for a Current Path Corresponding to Left Hand to Feet (Source: IEC 60479-1).



DC-1	Slight pricking sensation possible when making, breaking or rapidly altering current flow
DC-2	Involuntary muscular contractions likely especially when making, breaking or rapidly altering current flow bu usually no harmful electrical physiological effects
DC-3	Strong involuntary muscular reactions and reversible disturbances of formation and conduction of impulses in the heart may occur, increasing with current magnitude and time. Usually no organic damage to be expected.
DC-4	Patho-physiological effects may occur such as cardiac arrest, breathing arrest, and burns or other cellular damage. Probability of ventricular fibrillation increasing with current magnitude and time.

Figure 6. Conventional Time/Current Zones of Effects of DC Currents on Persons For a Longitudinal Upward Current Path (Source: IEC 60479-1)

4.4 CRASH HAZARD

In terms of overall safety, the passenger compartments of hydrogen vehicles must have the same level of integrity as the passenger compartments of conventional vehicles. Figure 2 earlier demonstrates the substantial differences between hydrogen and conventional vehicles in components and their locations. Hydrogen vehicle fuel system and drivetrain components can be expected to have different mass and stiffness characteristics, both of which are critical to a vehicle's crash energy management strategy.

The schematic in Figure 1 shows the basic components of an example hydrogen-fueled FCV,[4 5] corresponding to Figure 2. Figure 7 provides a schematic of a compressed-hydrogen fuel cell vehicle with estimated weights taken from an MIT report "On the Road in 2020, A Life-Cycle Analysis of New Automobile Technologies."[14] As part of their assessment of the total ownership costs for 2020 vehicles, the MIT authors developed an energy consumption model for each of these technologies, including an analysis of mass of major subsystems and the complete vehicles.

They extrapolated current technology developments to the year 2020 and provide a comparison of the total estimated mass of potential vehicles, drivetrains and bodies in that era, including direct hydrogen fueled FCVs. Their baseline vehicle was a 1996 Ford Contour that has a total mass of 1,322 kg without passengers. The authors of the MIT study assumed that there will be a 15-percent reduction in weight of conventional vehicles in 2020 over 1996 vehicles by replacement of mild steel by high-strength steel. They further assumed that advanced vehicles in 2020 will employ aluminum, rather than steel, resulting in a total reduction of 35 percent over the baseline 1996 vehicle.

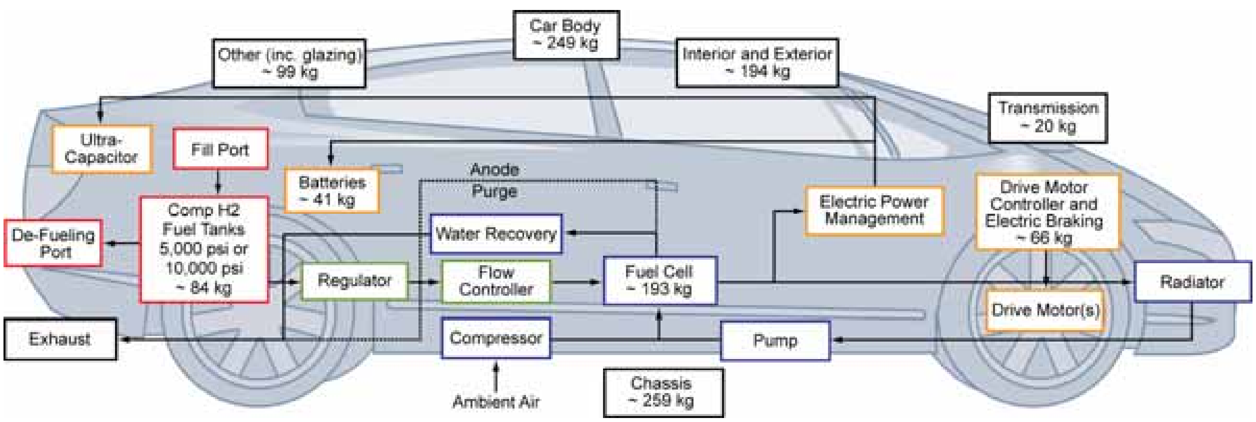


Figure 7. Schematic of Compressed-Hydrogen Fuel Cell Vehicle Component Locations And Mass Distribution.

The MIT authors project that a direct hydrogen-powered fuel cell vehicle may be approximately 70 pounds heavier than the baseline gasoline counterpart. The main differences in the vehicle mass are related to the propulsion system (58% greater for the FCV) and fuel storage (87% greater for the FCV). They suggest that fuel cell vehicles will still weigh less than comparable gasoline vehicles manufactured in 1996 (approximately 11% less in total weight).

While based on numerous assumptions, the MIT paper strongly suggests that there is a potential for at least doubling the mass in the front engine compartment in hydrogen vehicles compared to conventional vehicles and/or adding significant mass under the passenger compartment, depending upon the final vehicle design. These increases are likely to occur at the same time that mass is removed from elsewhere in the vehicle such that the total mass does not change substantially.

A Battelle assessment of these results suggests that, while the mass distribution may be different between conventional gasoline vehicles and fuel cell vehicles, fuel cell vehicles do not appear to have a different enough mass profile to necessitate differences in crash energy management strategies. In general, a crash management strategy is built around the total mass of the vehicle while trying to maintain the integrity of the passenger compartment and minimizing the forces exerted on the occupants. From a crash safety perspective, the mass and stiffness of a direct fueled fuel cell vehicle do not appear to be different enough from conventional vehicles to suggest that a radically different engineering approach will be required. In fact, this has been demonstrated with the Honda FCX production prototype FCV that has been self-certified as meeting all existing FMVSS and has been crash-tested in front, offset, side, and rear crash modes without failure of the fuel system or occupant protection requirements.[3]

4.5 Fire Hazards

Fire represents a unique hazard for gaseous fueled vehicles, including hydrogen, because, if not mitigated, it can cause fuel containers to rupture, rapidly releasing mechanical energy with destructive force and the potential for explosion of the fuel. Hydrogen and other gaseous fuel storage and delivery systems are designed to prevent rupture by venting hydrogen contents of fuel tanks through thermally activated pressure relief devices in case of an encroaching fire.

Vehicle fires are not a well characterized hazard and, consequently, present a significant design challenge. Fire can be caused by many factors, can originate inside or outside the vehicle and can travel different paths and speeds depending upon many factors. Currently the "design" fire for gaseous fuel vehicles is embodied in the fuel container bonfire tests such as in FMVSS 304 in which a container is suspended 4 inches over a "uniform fire source" 1.65 meters (65 inches) in length and required either to vent its contents through a PRD or to not burst within 20 minutes. The containers are protected by thermally activated pressure relief devices typically located at a port at each end of the container. Long tanks, such as those used on buses, may have piping exterior to the container to locate another PRD midway along its length.

Current thermally activated PRDs are local heat detectors only. Hence, they activate when their immediate surroundings are heated, but cannot detect localized heat sources elsewhere in the middle of the container. They protect containers from large, distributed fires, but not highly localized fires. Technology and standards to address localized fire are under investigation and consideration by the hydrogen and natural gas vehicle industry. Further discussion of this topic is provided in the final section of this report on assessment of safety issues.

5.0 FAILURE MODES AND EFFECTS ANALYSIS OF COMPRESSED-HYDROGEN FUEL CELL VEHICLE

The failure modes and effects analysis is a structured methodology for identifying potential modes by which a system can fail and identifying remedial measures, such as design changes or safety tests that can help engineers prevent the failure or mitigate its effects. The objective of this task order is to perform an FMEA to identify potential hazards of compressed-hydrogen fuel cell vehicles and identify remedial measures and potential issues for FMVSS for these vehicles. The FMEA results offer NHTSA a better understanding of the safety of hydrogen vehicles and therefore may inform NHTSA's activities concerning compressed-hydrogen vehicles.

5.1 DESCRIPTION OF THE FMEA DEVELOPMENT PROCESS

The FMEA methodology uses a brainstorming approach to identify failure modes and postulate the effects of the potential system failures on the system. The failure mode describes how equipment fails; the effect of the failure mode is determined by the system's response to the equipment failure. An FMEA identifies single failure modes that either directly result or contribute significantly to a failure event.

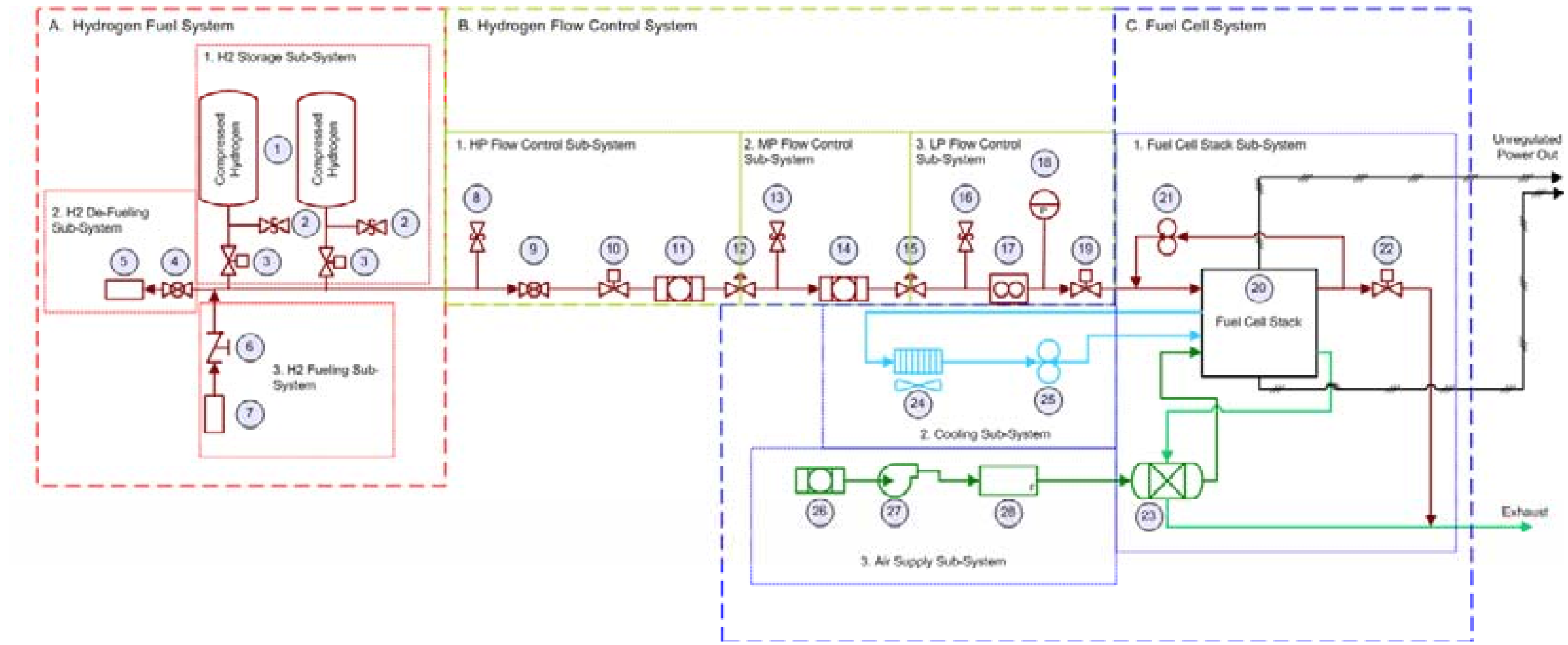
First, a high-level conceptual model of a compressed-hydrogen fuel cell vehicle system was prepared. The model focuses on key components specific to the hydrogen fuel system that may affect safety. For the purpose of the analysis, the model was divided into systems, sub-systems, and key components as shown in Figure 8 and listed below in Table 3.

The analysis of the HFCV was performed at the component level. For each key component, the analysts identified its function followed by potential failure modes. A failure mode is defined as the manner or mechanism in which a component, subsystem, or system could potentially fail to meet or deliver the intended function. In a multilayer system, a potential failure mode in one layer could also be the cause of a potential failure in a higher level system or be the effect of failure in a lower level component. For this high-level FMEA, the likelihood of occurrence of the potential failure mode was rated on a three-point scale of Low, Medium, and High (see Table 4).

The analysts then postulated the effects or consequences of those failures on the sub-system and system and their associated impacts. The potential seriousness or severity of the impacts was then rated also on a scale of Low, Medium, and High (see Table 5). The Likelihood (L) and Consequence (C) ratings were then used to determine the relative Risk value (R) for the potential failures (see Figure 9).

Table 3. HFCV Concept Model Systems, Subsystems, and Components

System	Subsystem	ID#	Component
Compressed-Hydrogen Fuel Storage and Filling	Hydrogen Storage	1	Compressed-Hydrogen Storage Containers
		2	Thermally Activated PRD
		3	Container Shut-Off Valve
	Hydrogen De-Fueling	4	De-Fueling Manual Valve
		5	De-Fueling Port
	Hydrogen Fueling	6	Fill Stop/Check Valve
		7	Fill Port
Hydrogen Fuel Delivery	High-Pressure Flow Control	8	High-Pressure Safety Relief
		9	Main System Manual Valve
		10	Main System Solenoid Valve
		11	High-Pressure Hydrogen Filter
		12	High-Pressure Regulator
	Mid-Pressure Flow Control	13	Mid-Pressure Safety Relief
		14	Mid-Pressure Hydrogen Filter
		15	Anode Pressure Regulator
	Low-Pressure Flow Control	16	Anode Safety Relief
		17	Hydrogen Flow Meter
		18	Hydrogen Pressure Sensor
		19	Hydrogen Pressure Solenoid Valve
Fuel Cell	Fuel Cell Stack	20	Fuel Cell Stack
		21	Anode Recirculation Pump
		22	Anode Purge Valve
		23	Cathode Humidifier
	Cooling	24	Radiator
		25	Stack Coolant Pump
	Air Supply	26	Cathode Air Filter
		27	Cathode Air Blower
		28	Air Flow Meter



A. Hydrogen Fuel Storage System

- 1. Hydrogen Storage Sub-system
  - 1) Compressed Hydrogen Storage Tanks
  - 2) Thermally Activated PRD
  - 3) Container Shut-off Selector Valve
- 2. Hydrogen De-Fueling Sub-System
  - 4) De-Fueling Manual Valve
  - 5) De-Fueling Port
- 3. Hydrogen Fueling Sub-System
  - 6) Fill Stop/Check Valve
  - 7) Fill Port

B. Hydrogen Flow Control System

- 1. High Pressure (HP) Flow Control Sub-system
  - 8) HP Safety Relief
  - 9) Main System Manual Valve
  - 10) Main System Solenoid Valve
  - 11) HP Hydrogen Filter
  - 12) HP Regulator
- 2. Mid-Pressure (MP) Flow Control Sub-System
  - 13) Mid-pressure Safety Relief
  - 14) Low Pressure Hydrogen Filter
  - 15) Anode Pressure Regulator
- 3. Low Pressure (LP) Flow Control Sub-System
  - 16) Anode Safety Relief
  - 17) Hydrogen Flow Meter
  - 18) Hydrogen Pressure Sensor
  - 19) Final Hydrogen Solenoid Valve

C. Fuel Cell System

- 1. Fuel Cell Stack Sub-System
  - 20) Fuel Cell Stack
  - 21) Anode Recirculation Pump
  - 22) Anode Purge Valve
  - 23) Cathode Humidifier
- 2. Cooling Sub-System
  - 24) Radiator
  - 25) Stack Coolant Pump
- 3. Air Supply Sub-System
  - 26) Cathode Air Filter
  - 27) Cathode Air Blower
  - 28) Air Flow Meter

Figure 8. Simplified Diagram of Compressed-Hydrogen Fueled FCV Systems

Table 4. Likelihood Categories

Rating	Description
High (H)	Almost certain to occur repeatedly
Medium (M)	Likely to occur to rarely likely to occur
Low (L)	Unlikely that failure would occur

Table 5. Consequence Categories

Rating	Description
High (H)	Potential for great harm or death
Medium (M)	Harm would likely require medical treatment
Low (L)	No injuries likely

Likelihood \ Consequence	LOW	MED	HIGH
HIGH	M	H	H
MED	L	M	H
LOW	L	L	M

Figure 9. Risk Matrix

5.2 DESCRIPTION OF THE RESULTS

The purpose of the FMEA was to perform a systematic evaluation of the compressed-hydrogen fuel cell vehicle system to identify and evaluate the various failure modes of key components, their potential effects on system safety, and identify actions to reduce the risk. The analysis focused on components and failure modes that could impact the safety of passengers, the public and first responders in the event of a crash, such as rupture of high-pressure components, release of fuel or fire.

As mentioned earlier, the main concerns associated with the use of compressed hydrogen in a fuel cell vehicle include the following:

- Ignition of a hydrogen leak (combustion hazards),
- Potential energy of high-pressure storage (high-pressure hazards),
- Electrical energy in the fuel cell system (electrical hazards),
- Response of the vehicle in a crash (crash hazards), and
- Response of the vehicle to an external fire (fire hazards).

Table 6 presents the results of the FMEA. The following provides a summary of the failure modes, consequences for the three main systems included in the analysis and a discussion of the current controls to both prevent and mitigate risk.

5.2.1 Failure Modes and Consequences

Compressed-Hydrogen Fueling and Fuel Storage System. For the FMEA the compressed-hydrogen fueling and fuel storage system was divided into three subsystems consisting of the (1) hydrogen storage sub-system, (2) hydrogen defueling sub-system, and (3) hydrogen fueling sub-system. As such, the failure modes associated with this system are related to the fuel containers, fueling/de-fueling lines, and associated equipment such as the thermally activated pressure relief device and container shut-off selector valve.

The primary failure modes considered in the FMEA for the compressed-hydrogen fueling and fuel storage system include leak or rupture of the fuel container, fuel delivery lines and associated components. Secondary failure modes considered include failure of PRDs or valves to open or close when required. As detailed in the FMEA there are a number of potential causes for these component failure modes that can be grouped as follows:

- Inadequate design, testing, manufacturing, installation, or maintenance of equipment
- Damage caused by external fire or localized fire
- Damage caused by external impact (including crashes and road debris)

Potential consequences of a hydrogen leak or rupture can vary depending on the circumstances under which the leak is caused. Since the compressed-hydrogen fueling and fuel storage system contains a large amount of fuel at high pressures the main consequences of a hydrogen leak or rupture may include:

- Immediate ignition of released fuel resulting in a high-pressure hydrogen jet flame hazard;
- Collection of a combustible mixture in a closed environment leading to a fire hazard;
- Collection of hydrogen in a closed environment leading to an asphyxiation hazard;
- Delayed ignition of collected vapors leading to a potential explosion or detonation hazard;
- Explosive release of mechanical energy and of the container/component materials; and
- Dislodging/ejection of components due to an inertial release of the compressed hydrogen gas.

Hydrogen Fuel Delivery System. For the FMEA the hydrogen fuel delivery system was divided into three subsystems consisting of the (1) high-pressure delivery sub-system, (2) medium-pressure delivery sub-system, and (3) low-pressure delivery sub-system. The hydrogen fuel delivery system transfers the compressed gas to the fuel cell through a series of regulators, valves, filters, and a flow meter to deliver hydrogen at a reduced pressure to the fuel cell. Typical pressure ranges for each sub-section were generally assumed to be:

- High-pressure section: 3,600 - 10,000 psi (24.8 – 70 MPa);
- Medium-pressure section: 100 - 150 psi (.69 – 1 MPa); and

- Low-pressure section: 5 - 10 psi (.03 – .07 MPa).

Similar to the hydrogen fueling and fuel storage system the primary failure modes for the hydrogen delivery system include leaks or ruptures of the supply line and/or associated components. Again secondary causes of equipment leaks or ruptures from failed regulators, valves, or flow meters are possible; however design controls are in place to help minimize the consequences. As detailed in the FMEA there are a number of potential causes but they can generally be grouped as follows:

- Inadequate design, testing, manufacturing, installation, or maintenance of equipment
- Damage caused by external fire
- Damage caused by external impact (including crashes and road debris)

Potential consequences of a hydrogen leak or rupture can vary depending on the circumstances under which the release is caused (high-pressure versus low-pressure components). The FMEA identified several potential consequences of a hydrogen leak or rupture within the fuel delivery system and include:

- Immediate ignition of released fuel resulting in a high-pressure hydrogen jet flame hazard;
- Collection of a combustible mixture in a closed environment leading to a fire hazard;
- Collection of hydrogen in a closed environment leading to an asphyxiation hazard;
- Delayed ignition of collected vapors leading to a potential explosion or detonation hazard;
- Explosive release of mechanical energy and of the container/component materials (high-pressure components only); and
- Dislodging/ejection of components due to an inertial release of the compressed hydrogen gas (high-pressure components only).

Obviously, the consequences of a leak or rupture would be less severe as the pressure is reduced throughout the fuel delivery system. A rupture would be less likely to occur as the pressure is reduced through the flow supply line. The higher pressure portion of the line would also have a mass inertial release and mechanical energy release where the lower pressure portion would not.

Fuel Cell System. The fuel cell system uses the compressed hydrogen and air to produce electricity to power the electric motors. For the purpose of the FMEA it was divided into three subsystems: the fuel cell stack, cooling, and air supply.

The main failure modes for the fuel cell system include membrane failure and electrical short. The most critical appears to be the membrane failure and as detailed in the FMEA there are a number of potential causes (inadequate design, testing, manufacturing, installation, or maintenance; loss of moisture, loss of cooling, overpressure, degradation, reduced flow of hydrogen to the anode, etc.). A membrane failure would result in hydrogen coming in direct contact with air and the platinum catalyst at the cathode, which would lead to a fire. An electrical short could result in a shock hazard to vehicle occupants or emergency responders as well as a potential ignition source for any released hydrogen vapors.

The likelihood of a failure within the fuel cell system was considered higher than for the hydrogen storage and flow supply systems mainly due to the lack of performance data, ongoing research, and limited codes and standards. A failure of the fuel cell membrane or an electrical short could lead to a fire, which is considered to be a high consequence.

5.2.2 Basic Design Controls

As part of the FMEA process the analysts identified typical HFCV safety features designed to prevent a failure or help to mitigate potential consequences. These basic features are listed below.

- Design/Qualification/Manufacturing/Quality Control/Installation/Maintenance requirements – to ensure that all components used within the fuel storage, supply, and fuel cell systems are designed, appropriately tested, installed, and maintained for the service environment in which they will operate.
- Crash test requirements – to provide a systems approach to help ensure fuel system integrity to prevent or minimize the release of hydrogen in the event of a crash.
- Thermal protection and fire test requirements – to demonstrate that fire protection systems in the hydrogen storage systems will prevent the rupture of the containment vessel when exposed to fire.
- Pressure sensor – to provide an indication to the vehicle control system to help manage the hydrogen fuel pressure in the fuel supply system.
- Flow meter – to provide an indication to the vehicle control system to help manage the flow of hydrogen to the fuel cell.
- Fail-safe design – to prevent the unwanted discharge of fuel resulting from a single-point failure of the shutoff function.
- Impact sensors – to provide a means to detect a crash and send a signal to activate the automatic fuel shutoff(s) and electrical disconnect(s).
- Pressure relief – to provide a means to relieve excess pressure in a safe manner away from the vehicle and prevent a line or component rupture.
- Leak detection: Hydrogen leak sensors – to provide a means to detect hydrogen leakage and provide a warning and shut off of hydrogen fuel flow.
- Voltage monitoring – to monitor fuel cell stack performance and provide a means to detect low voltage or overcurrent that could lead to internal or external component failures and subsequent exposure of personnel to hazards.
- Ventilation – to provide a means to discharge leaked hydrogen away from the vehicle.

Table 6. FMEA of Compressed-Hydrogen Fuel Cell Vehicle

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A. Compressed-Hydrogen Fuel Storage System											
A.1 Compressed-Hydrogen Storage Sub-System											
A.1.1-a	Compressed-hydrogen fuel container	Compressed-hydrogen fuel container	Store and deliver hydrogen fuel to the fuel system. (5,000, 10,000 psi)	Inadequate design/test/manufacture/installation Degradation Seal failure Impact	Leak, loss of hydrogen without a substantial drop in pressure.	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Container design requirement • Container qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen leak sensors	Once there is a leak in the container, there is no way to stop the flow. Consider requiring flame arrestors.
A.1.1-b				Inadequate design/test/manufacture/installation Crash induced damage or penetration by external object. Fire induced damage	Rupture – loss of fuel and fragmentation of container (mechanically, chemically or thermally induced damage).	L	• Explosive release of mechanical energy (stored in the gas and the container) and explosive release of the container materials. • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Crash test requirements • Thermal protection & fire test requirements • Hydrogen leak sensors • PRD	In the event of a rupture of the container, there is nothing to prevent the severity of the impact except the integrity of surrounding compartment. Current thermally activated PRDs are local heat detectors only; they activate when their immediate surroundings are heated, but cannot detect localized heat sources elsewhere.

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.1.2-a	Thermally Activated Pressure Relief Device (PRD)	Thermally-activated device that vents the contents of the container when exposed to fire.	Maintains fuel container contents in normal service. Vents fuel containers in the case of a fire.	Inadequate design/test/manufacture/installation Mechanical failure	Fails to vent the contents in the event of a fire.	L	• Rupture of container, explosive release of mechanical energy (stored in the gas and the container) and explosive release of the container materials. • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• PRD design requirements • PRD qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Thermal protection & fire test requirements	There is no backup or redundant PRD in this conceptual design, so a failure of the PRD to vent could lead to severe consequences.
A.1.2-b				Inadequate design/test/manufacture/installation Mechanical/failure	Vents contents inappropriately (in the absence of fire)	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Mass inertial release (launch container – blow away anything near the container	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors (notify driver)	If the PRD vents inappropriately the contents of the container will be released and there is nothing to prevent the potential severe consequences.

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.1.2-c				Inadequate design/test/manufacture/installation Crash induced damage or penetration by external object. Mechanical failure of the PRD.	Venting of contents/blowdown,-- loss of fuel and pressure in the container without fragmentation of the container. (mechanically induced damage)	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Mass inertial release (launch container – blow away anything near the container)	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Crash test requirements • Hydrogen leak sensors (notify driver)	If the PRD vents inappropriately the contents of the container will be released and there is nothing to prevent the potential severe consequences.
A.1.2-d				Inadequate design/test/manufacture/installation Mechanical Crash /Fire induced	Rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Launch PRD	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Crash test requirements	If the PRD ruptures the contents of the container will be released and there is nothing to prevent the potential severe consequences..
A.1.3-a	Container Shut-off/Selector Valve	Manual or electronic valve to shut off fuel flow from a fuel storage container.	Shuts off fuel flow from a storage container.	Inadequate design/test/manufacture/installation Mechanical/electrical failure	Restrict or limit fuel flow. (*Assumes fuel meets purity levels required for PEM fuel cell operation and therefore will not clog)	L	• Performance issue – No Hazard • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	M	• Valve design requirements • Valve qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Monitor fuel cell voltage	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.1.3-b				Inadequate design/test/manufacture/installation Mechanical/electrical failure Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Crash test requirements • Thermal protection & fire test requirements • Downstream HP Safety Relief	If the container shut-off valve leaks or ruptures there is no way to prevent the contents of the container from releasing and leading to severe consequences.
A.1.3-c				Inadequate design/test/manufacture/installation Mechanical/electrical failure	Fail open	L	• Inability to shut off fuel flow (requires controlled de-fueling of the container) • Inability to shut off flow in an emergency or accident.	L	L	• Design/Qualification/Manufacturing/QC/Installation reqs.	
A.1.3-d				Inadequate design/test/manufacture/installation Mechanical/electrical failure	Fail closed	L	• Inability to supply fuel; Performance Issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Second container • Monitor fuel cell voltage	
A.1-a	Hydrogen fuel storage line and connections		Transfer compressed hydrogen to the HP flow control system.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact	Leak, rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Crash test requirements • Thermal protection & fire test requirements • Downstream HP Safety Relief • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.2 Hydrogen De-Fueling Sub-System											
A.2.4-a	De-fueling Manual Valve	Manual valve	Seal fuel from the environment when closed and permit emptying of fuel containers when open.	Inadequate design/test/manufacture/installation Mechanical failure	Restrict or limit fuel flow.	L	• Slows down emptying of fuel container	L	L	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements	
A.2.4-b				Inadequate design/test/manufacture/installation Mechanical failure Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements • Downstream HP Safety Relief (prevention)	
A.2.4-c				Inadequate design/test/manufacture/installation Mechanical failure	Fail open	L	• Inability to shut off fuel flow, Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Container shut-off valve	
				Inadequate design/test/manufacture/installation Mechanical failure	Fail closed	L	• Inability to empty fuel container	-		• Design/Qualification/Manufacturing/QC/Installation reqs.	
A.2.5-a	De-Fueling Port	Fitting for removal of fuel from containers, downstream of de-fueling valve.	Allow for connection to fuel containers and removal of fuel.	Inadequate design/test/manufacture/installation Mechanical failure	Restrict or limit fuel flow.	L	• Reduced de-fueling flow rate; takes longer to de-fuel.	-	L	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements	
A.2.5-b				Inadequate	Become bent or	L	• Unable to connect so	H	M	• Design/Qualification/Ma	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
				design/test/manufacture/installation	damaged.		unable to empty container. • May leak which could result in ignition			nufacturing/QC/Installation reqs.	
A.2-a	Hydrogen de-fueling line and connections		Allow de-fueling of compressed-hydrogen containers	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Crash test requirements • Thermal protection & fire test requirements • Downstream HP Safety Relief • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation	
A.3 Hydrogen Fueling Sub-System											
A.3.6-a	Hydrogen Fill Stop/Check Valve Required by J2579, 6.2.9 Article 100.3.1.3	Automatic valve	Allow filling of fuel containers when while preventing back flow when open and maintain container pressure when closed.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Restrict or limit fuel flow.	L	• Takes longer to fill fuel container, No Hazard	-	-	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements	
A.3.6-b				Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Fail open	L	• May lead to back flow, and potential release of fuel to the atmosphere, Fire	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs.	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.3.6-c				Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection	Fail closed	L	• Prevents flow of fuel to the container; performance issue; No Hazard • Potential back flow and release of fuel to the atmosphere	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs.	
A.3.7-a	Hydrogen Fill Port	Fitting for connection to fuel containers when filling.	Allow for connection to fuel containers when filling with fuel.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Restrict or limit flow	L	• Reduced fueling flow rate; takes longer to fill fuel container.	L	L	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements	
A.3.7-b				Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Become bent or damaged	L	• Unable to connect so unable to fill container – Performance Issue; No Hazard	-	-	• Design/Qualification/Manufacturing/QC/Installation reqs.	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
A.3-a	Hydrogen Fuel Filling Line and connections		Supply compressed hydrogen to the storage containers	Inadequate design/test/manufacture/installation Impact Overpressure Damaged Degraded Crash induced damage Fire induced damage	Leak/rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Crash test requirements • Thermal protection & fire test requirements • Downstream HP Safety Relief • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation	
B. Hydrogen Flow Control System											
B.1 High-Pressure Flow Control Sub-System											
B.1.8-a	High-Pressure Safety Relief Valve	Pressure activated valve.	Release fuel in the event of high pressure in the delivery line. Protects downstream components and prevents fuel-line rupture.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow.	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Downstream MP Safety Relief • Ventilation	
B.1.8-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Container Shut-off Valve	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.1.8-c				Inadequate design/test/manufacture/installation Mechanical	Fail open	L	• Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Container Shut-off Valve	
B.1.8-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Potential rupture of fuel line; Immediate ignition – Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Downstream MP Safety Relief • Hydrogen pressure sensor • Ventilation	
B.1.9-a	Main System Manual Valve	Manual valve	Permit fuel flow in the fuel line when open and isolate the fuel containers from downstream components when closed.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow.	L	• Performance issue – No Hazard	-	-	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen pressure sensor	
B.1.9-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation • Crash test requirements • Upstream Container Shut-off Valve • Thermal protection & fire test requirements • Upstream MP Safety Relief	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.1.9-c				Inadequate design/test/manufacture/installation Mechanical	Fail open (During maintenance or after crash – when you want it closed)	L	• Inability to isolate the fuel containers from downstream components.	M	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Downstream solenoid valves • Upstream Container Shut-off Valve	
B.1.9-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Performance issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Monitor fuel cell voltage • Upstream HP Safety Relief Valve	
B.1.10-a	Main System Solenoid Valve	Electronically-activated solenoid valve.	Permit fuel flow in the fuel line when open and isolate the fuel containers from downstream components when closed. Operated by vehicle control system. Closes when engine is not running and/or the ignition is off.	Inadequate design/test/manufacture/installation Electronic failure Clogged with contaminants	Restrict or limit fuel flow.	L	• Performance issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Monitor fuel cell voltage • Hydrogen pressure sensor	
B.1.10-b				Inadequate design/test/manufacture/installation Electronic failure Damaged during a fire Crash induced damage	Leak or rupture (out of system)	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main System Manual Valve & Container Shut-off Valve • Upstream HP Safety Relief	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.1.10-c				Inadequate design/test/manufacture/installation Electronic failure Stuck open due to contaminants	Fail open (During maintenance or after crash)	L	• Inability to stop fuel flow in an emergency or for maintenance	M	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Main System Manual Valve and Container Shut-off Valve	
B.1.10-d				Inadequate design/test/manufacture/installation Electronic failure Clogged with contaminants	Fail closed	L	• Stop, restrict, or limit flow of fuel, loss of power; potential for membrane rupture and fire.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Upstream HP safety relief valve • Monitor fuel cell voltage	
B.1.11-a	High-Pressure Hydrogen Filter	Filter with fuel inlet and outlet and media to capture particles and droplets in the fuel line.	Remove solid and liquid contaminants from the hydrogen fuel stream to prevent damage of downstream components.	Inadequate design/test/manufacture/installation Poor quality Hydrogen	Restrict or limit fuel flow (plugged/clogged) .	L	• Performance issue • Limited fuel flow could lead to lower pressure on anode, membrane failure, and potential fire.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen pressure sensor • Monitor fuel cell voltage • Filter replacement	
B.1.11-b				Inadequate design or testing for hydrogen service Damaged, deformed	Allow passage of contaminants (Leak or rupture)	L	• Potential malfunction of downstream components • Performance Issue	M	L	• Dsign/Qualification/ • Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor	
B.1.12-a	High-Pressure Regulator	Pressure regulator	Isolates high-pressure section of fuel line from the low-pressure section. Ensures delivery of fuel to downstream components at the proper pressure.	Inadequate design/test/manufacture/installation Damaged, deformed Clogged, plugged	Restrict or limit fuel flow.	L	• Performance issue • Limited fuel flow could lead to lower pressure on anode and membrane failure, potential rupture and fire	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen pressure sensor • Monitor fuel cell voltage	
B.1.12-b				Inadequate	Seal leak or	L	• Immediate ignition -	H	M	• Design/Qualification/Ma	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
				design/test/manufacture/installation Damaged, deformed Crash induced damage Fire induced damage	rupture (out of system)		Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.			nufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main System Solenoid Valve and Container Shut-off Valve • Upstream HP Safety Relief	
B.1.12-c				Inadequate design/test/manufacture/installation Damaged, deformed	Fail to control pressure – fail open	L	• Damage downstream components • Potential rupture and fire	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Downstream MP Safety Relief • Main System Solenoid Valve and Container Shut-off Valve • Monitor fuel cell voltage • Hydrogen pressure sensor • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation	
B.1.12-d				Inadequate design/test/manufacture/installation Damaged, deformed	Fails closed	L	• Prevents fuel flow, potential line rupture and fire • Performance issue	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Monitor fuel cell voltage • Upstream HP Safety Relief Valve	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.1-a	HP Hydrogen Flow Control Line		Transfers HP compressed Hydrogen to the MP flow section.	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements • HP Safety Relief	
B.2 Mid-Pressure Flow Control Sub-System											
B.2.13-a	Mid-Pressure Safety Relief Valve	Pressure-activated valve	Release fuel in the event of high pressure in the delivery line. Protects downstream components and prevents fuel-line rupture.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Downstream Anode Safety Relief Valve • Ventilation	
B.2.13-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main system solenoid valves; container shut-off selector valve	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.2.13-c				Inadequate design/test/manufacture/installation Mechanical	Fail open	L	• Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Main system solenoid valves; container shut-off selector valve • Ventilation	
B.2.13-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Ventilation • Anode Safety Relief • Hydrogen pressure sensor	
B.2.14-a	Low Pressure Hydrogen Filter	Filter with fuel inlet and outlet and media to capture particles and droplets in the fuel line.	Remove solid and liquid contaminants from the hydrogen fuel stream to prevent damage of downstream components.	Inadequate design/test/manufacture/installation Poor quality Hydrogen	Restrict or limit fuel flow (plugged/clogged)	L	• Performance Issue • Limited fuel flow could lead to lower pressure on anode and membrane failure.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen pressure sensor • Monitor fuel cell voltage • Filter replacement	
B.2.14-b				Inadequate design/test/manufacture/installation Degradation – wear/tear	Allow passage of contaminants to downstream components (leak or rupture)	L	• Potential malfunction of downstream components • Performance Issue	M	L	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.2.15-a	Anode Pressure Regulator	Pressure regulator	Isolates the anode from the medium pressure section of the fuel delivery line. Ensures delivery of fuel to the anode at the proper pressure.	Inadequate design/test/manufacture/installation Damaged, deformed Clogged, plugged	Restrict or limit fuel flow.	L	• Limit flow of fuel to engine – Performance Issue • Limited fuel flow could lead to lower pressure on anode and membrane failure. Potential rupture and fire	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Monitor fuel cell voltage • Hydrogen pressure sensor	
B.2.15-b				Inadequate design/test/manufacture/installation Damaged, deformed Crash induced damage Fire induced damage	Seal leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main system solenoid valves; container shut-off selector valve • Upstream MP Safety Relief	
B.2.15-c				Inadequate design/test/manufacture/installation Damaged, deformed	Fail to control pressure – Fails open	L	• Overpressure downstream components – membrane rupture/fire • Performance Issue	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Monitor fuel cell voltage • Flow meter • Anode Safety Relief • Main system solenoid valves; container shut-off selector valve • Hydrogen pressure sensor	
B.2.15-d				Inadequate design/test/manufacture/installation Damaged, deformed	Fails closed	L	• Prevents fuel flow, potential line rupture and fire • Performance issue	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Monitor fuel cell voltage • Upstream Safety Relief • Hydrogen pressure sensor	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.2-a	MP Hydrogen Flow Control Fuel Line		Transfers MP compressed Hydrogen to the LP flow section.	Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements • MP Safety Relief	
B.3 Low-Pressure Flow Control Sub-System											
B.3.16-a	Anode Safety Relief Valve	Pressure activated valve.	Release fuel in the event of high pressure in the fuel cell. Protects fuel cell from overpressure and rupture.	Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection or fire protection	Restrict or limit fuel flow.	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H		• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Ventilation	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.3.16-b				Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection or fire protection Crash induced damage Fire	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main system solenoid valves; container shut-off selector valve	
B.3.16-c					Fail open	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Main system solenoid valves; container shut-off selector valve	
B.3.16-d					Fail closed	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Ventilation • Hydrogen pressure sensor	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.3.17-a	Hydrogen Flow Meter	Flow meter	Measures the flow of fuel to the anode in the fuel cell.	Mechanical	Fail to function properly.	L	• If false high flow, will send signal to decrease flow unnecessarily – Performance issue or potential membrane failure and fire. • If false low flow, will send signal to increase flow when not needed, too much flow – damage fuel stack. Fire	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen pressure sensor	
B.3.17-b				Degradation, wear/tear	Leak or rupture.	L	• Damage downstream components – Fire	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen pressure sensor • Hydrogen leak sensors • Ventilation	
B.3.18-a	Hydrogen Pressure Sensor	Sensor for fuel-line pressure measurement.	Measure pressure in fuel line for feedback to vehicle control system. Controls the reaction rate	Electronic failure	Fail to function properly.	L	• If false high flow, will send signal to decrease flow unnecessarily; reduced flow of hydrogen to anode could rapidly lead to membrane failure, and fire. • If false low flow, will send signal to increase flow when not needed, too much flow – damage fuel stack. Fire	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Flow meter	
B.3.18-b					Leak or rupture.	M	• Fire	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Ventilation	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.3.19-a	Final Hydrogen Solenoid Valve	Electronically-activated solenoid valve.	Enable delivery of fuel to the fuel cell at the proper flow rate. Operated by vehicle control system.	Electronic failure Clogged with contaminants Inadequately designed or manufactured Damaged during installation	Restrict or limit fuel flow.	L	• Performance issue • Reduced flow of hydrogen to anode could rapidly lead to membrane failure, and fire.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Monitor fuel cell voltage • Hydrogen pressure sensor	
B.3.19-b				Inadequately designed or manufactured Damaged during installation Damaged during a fire Crash induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Main system solenoid valves; container shut-off selector valve • Upstream Anode Safety Relief	
B.3.19-c				Electronic failure Inadequately designed or manufactured Stuck open due to contaminants	Fail open (During maintenance or after crash)	L	• Inability to stop fuel flow in an emergency or for maintenance	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Main system solenoid valves; container shut-off selector valve	
B.3.19-d				Electronic failure	Fail closed	L	• Stop, restrict, or limit flow of fuel, loss of power; potential for membrane rupture and fire.	H	M	• Design/Qualification/Manufacturing/QC/Installation reqs. • Upstream Anode Safety Relief • Monitor fuel cell voltage	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
B.3-a	LP Hydrogen Flow Control Fuel Line		Transfers LP compressed Hydrogen to the fuel cell	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	M	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen leak sensors • Hydrogen pressure sensor • Ventilation • Crash test requirements • Thermal protection & fire test requirements • Anode Safety Relief	
C. Fuel Cell System											
C.1 Fuel Cell Stack Sub-System											
C.1.20-a	Fuel Cell Stack	Polymer Electrolyte Membrane (PEM) fuel cell	Convert hydrogen fuel to electric power	Inadequate design/test/manufacture/installation Overpressuring of the anode; wear and tear	Membrane rupture (or small holes)	M	• Hydrogen in contact with air and catalyst at cathode, fire likely; permanent damage to stack.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Hydrogen sensor on cathode • Oxygen sensor on anode. • Voltage Monitoring	
C.1.20-b				Inadequate design/test/manufacture/installation Manufacturing, assembly, overheating	Seal leakage	M	• Low pressure hydrogen leak within the stack; fire possible • Low pressure external hydrogen leak, potential fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs.	
C.1.20-c				Inadequate design/test/manufacture/installation	Short circuit	M	• Shock • Ignition of vapors	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs.	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
C.1.21-a	Anode Recirculation Pump	Pump for return of excess fuel from outlet to inlet of anode.	Allows for excess fuel to be pumped from the fuel cell back to the fuel inlet section. (low pressure 1-2 psi)	Inadequate design/test/manufacture/installation Pump damage or electrical failure	Fails to function	M	• Slow loss of electrical power – No Hazard.	-	-	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Cell voltage monitor with pump trip on low voltage • Thermal protection & fire test requirements	
C.1.21-b				Inadequate design/test/manufacture/installation	Leak	M	• Low pressure Hydrogen release, potential for fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors	
C.1.22-a	Anode Purge Valve	Valve	Allow release of water and contaminants from the anode of the fuel cell (to exhaust)	Inadequate design/test/manufacture/installation	Restrict or limit flow.	M	• Slow loss of electrical power • Possible membrane rupture and fire	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Voltage monitoring	
C.1.22-b				Inadequate design/test/manufacture/installation Crash induced damage Fire induced damage	Leak or rupture	M	• Low pressure Hydrogen release, potential for fire	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen leak sensors • Crash test requirements • Thermal protection & fire test requirements	
C.1.22-c				Inadequate design/test/manufacture/installation	Fail open	M	• Low pressure Hydrogen release, potential for fire	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Hydrogen Leak sensors	
C.1.22-d				Inadequate design/test/manufacture/installation	Fail closed	M	• Slow loss of electrical power – No Hazard.	-	-	• Design/Qualification/Manufacturing/QC/Installation reqs. • Voltage monitoring	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
C.1.23-a	Cathode Humidifier	Humidifier	Assists in regulating the amount of water in the fuel cell, particularly in the cathode, to maintain fuel cell activity.	Inadequate design/test/manufacture/installation	Not functional	M	• Loss of moisture from the fuel cell, gradual power loss • Possible cell failure, holes - fire	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Voltage monitoring	
C.1.23-b				Inadequate design/test/manufacture/installation	Leak from inlet to exit	M	• Loss of air to the fuel cell, rapid power loss. • Possible cell failure, holes - fire	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Voltage monitoring	
C.2 Cooling Sub-System											
C.2.24-a	Radiator	Heat exchanger	Fluid to air heat exchanger to prevent overheating of fuel cell.	Inadequate design/test/manufacture/installation Degradation/wear-tear	Restrict or limit coolant flow.	M	• Overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	
C.2.24-b				Inadequate design/test/manufacture/installation	Fails to function	M	• Overheat fuel cell, membrane failure, fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Fuel cell voltage monitoring • Temperature sensors	
C.2.25-a	Stack Coolant Pump	Pump	Pumps coolant fluid through the fuel-cell stack and back through the radiator.	Inadequate design/test/manufacture/installation Loss of power	Fails to function	M	• Overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
C.2.25-b				Inadequate design/test/manufacture/installation Impact External fire	Leak or rupture	M	• Overheat fuel cell, membrane failure, fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Fuel cell voltage monitoring • Temperature sensors	
C.2.25-c	Coolant line		Recirculates coolant through the fuel cell	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire	Leak, rupture	M	• Overheat fuel cell, membrane failure, fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Fuel cell voltage monitoring • Temperature sensors • Crash test requirements • Thermal protection & fire test requirements	
C.3 Air Supply Sub-System (to the cathode)											
C.3.26-a	Cathode Air Filter	Filter	Removes particles and droplets from air feed stream to cathode. Chemical – Activated carbon removes sulfur	Inadequate design/test/manufacture/installation Failure to replace at required intervals	Restrict or limit air flow (partially plugged/clogged)	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	
C.3.26-b				Degradation Failure to replace at required intervals	Hole in filter media	M	• Quickly contaminates fuel cell– performance issue (Contaminants take up room on the filter so efficiency is reduced.)	-	-	• Design/Qualification/Manufacturing/QC/Installation reqs. • Fuel cell voltage monitoring	
C.3.26-c				Contaminants Failure to replace at required intervals	Plugged	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	H	• Design/Qualification/Manufacturing/QC/Installation reqs. • Fuel cell voltage monitoring • Temperature sensors	

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	L*	Failure Mode Consequences	C*	R*	Controls	Comments
C.3.27-a	Cathode Air Blower	Blower/Fan	Forces ambient air into the cathode of the fuel cell.	Electrical/mechanical failure	Fails to function	M	• Sudden loss of power • Overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	
C.3.28-a	Cathode Air Flow Meter	Flow Meter	Measures the flow of air into the cathode.	Mechanical	Fails to function properly	M	• To much air flow will damage the membrane, fire • To little air flow is a performance issue, will lead to loss of power – but could also result in overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	
C.3-a	Air line		Supplies ambient air to the cathode of the fuel cell – line is heated to maintain design temperature for the fuel cell	Inadequate design/test/manufacture/installation	Leak, rupture	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	H	• Design requirements • Qualification test requirements • Manufacturing and QC requirements • Installation, design and test requirements • Fuel cell voltage monitoring • Temperature sensors	

*** Note: L – Likelihood; C – Consequence; R – Risk**

6.0 COMPARISON OF FMEA RESULTS WITH FUEL CELL VEHICLE CODES AND STANDARDS

Recognizing the safety hazards identified in the FMEA above, several new industry standards have been or are currently being developed by various national and international organizations to address the safety of FCVs and their required infrastructure development. In addition, in the United States the Federal Government regulates the safety of vehicles through the Federal Motor Vehicle Safety Standards, which emphasize vehicle safety before, during, and after a crash. As FCVs become more prevalent in the marketplace there may be a need for additional codes and standards to guide the development of hydrogen fuel systems and components more effectively. This section highlights the major organizations developing codes and standards for FCVs and provides a brief overview of the content of each code/standard as related to the safety of HFCVs. Next, the results of the FMEA are compared with these codes and standards at the vehicle, system, and sub-system levels to identify potential issues for FMVSS for these vehicles.

6.1 REVIEW OF CODES AND STANDARDS

The codes and standards included in this review were:

Society of Automotive Engineers

- SAE J2578: Recommended Practice for General Fuel Cell Vehicle Safety
- SAE J2579 (Draft): Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles (PropDFT 2006)

International Organization for Standardization

- ISO 23273-1:2006(E): Fuel Cell Road Vehicles -- Safety Specifications -- Part 1: Vehicle Functional Safety
- ISO 23273-2:2006: Fuel Cell Road Vehicles -- Safety Specifications -- Part 2: Protection Against Hydrogen Hazards For Vehicles Fueled With Compressed Hydrogen
- ISO/DIS 23273-3: Fuel Cell Road Vehicles -- Safety Specifications -- Part 3: Protection Of Persons Against Electric Shock

Japanese HFCV Standards

- Attachment 17: Technical Standard for Fuel Leakage in Collisions
- Attachment 100: Technical Standard for Fuel Systems of Motor Vehicles Fueled by Compressed Hydrogen Gas
- Attachment 101: Technical Standard for Protection of Occupants Against High Voltage in Fuel Cell Vehicles

United Nations Economic Commission for Europe

- WP.29 Draft Standard for Compressed Gaseous Hydrogen, Proposal for a New Draft Regulation for Vehicles Using Compressed Gaseous Hydrogen, 12.10.03

CSA America

- CSA HGV2 Fuel Containers (Draft), Basic Requirements for Compressed-Hydrogen Gas Vehicle Fuel Containers
- CSA HPRD1 (Draft), Pressure Relief Devices for Compressed-Hydrogen Vehicle Fuel Containers, March 28, 2007

Federal Motor Vehicle Safety Standards

- FMVSS 303: Fuel System Integrity of Compressed Natural Gas Vehicles
- FMVSS 304: Compressed Natural Gas Fuel Container Integrity
- FMVSS 305: Electric Powered Vehicles: Electrolyte Spillage and Electrical Shock Protection

While all standards development organizations agree on the need and the general intent for codes and standards to ensure the safety of hydrogen fuel cell vehicles, the implementation varies from country to country and from organization to organization due to differences in culture and technical approach. For example, some countries focus on performance-based requirements while others prescribe or assume specific designs. Also, response protocols for fire and rescue personnel differ by country, resulting in differences in how vehicle fire resistance is addressed. Consequently, design standards and regulations from different countries and from different controlling authorities do not lend themselves to easy “apples to apples” comparisons. For this reason, it is necessary to review and compare all available codes and standards to gain a better understanding of the magnitude of FCV safety concerns as well as to aid in identifying any safety gaps in the existing FCV standards.

Several different codes and standards related to compressed-hydrogen-fueled FCVs were reviewed to identify how particular safety issues are being addressed. Table 7 provides a brief overview of these standards. Table 8 provides a summary of the content of each standard. In addition, separate summary tables have been included to assist in understanding the scope of each code/standard developed to regulate FCVs (see Appendix A). The summary tables list key aspects of the contents of each standard as related to the system diagram developed for the FMEA (Figure 8).

It should be noted that the scope of each standard varies in that some standards focus on vehicle and system-level concerns (i.e., SAE J2578) while others deal with specific components such as the fuel container within the fuel system (i.e., HGV2). These distinctions are provided in the last column of Table 7.

6.2 Review of FMEA and Related Codes and Standards

Once the FMEA was completed, the analysts reviewed the failure modes, effects, and safety features that would typically be in place to help reduce the likelihood of the failure or help to lessen the effects of the consequence. For each failure mode, the team then reviewed applicable codes and standards from several different organizations to identify the requirements for the component and the respective safety features. The purpose was to reveal potential areas of the FMVSS in which NHTSA might consider addressing the specific hazards of the compressed-hydrogen fuel cell vehicle design. The results of this review are summarized in Table 9. The detailed analysis is provided in Appendix B.

Table 7. Overview of FCV Codes and Standards

Standard	Title	Scope	Purpose	Vehicle, System, or Component Level
SAE J2578	Recommended Practice for General Fuel Cell Vehicle Safety	Identifies and defines the preferred technical guidelines relating to the safe integration of fuel cell system, fuel storage, and electrical systems into the overall Fuel Cell Vehicle.	The purpose of this document is to provide introductory mechanical and electrical system safety guidelines that should be considered when designing fuel cell vehicles for use on public roads.	Vehicle and System
SAE J2579 (DRAFT)	Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles	Addresses systems used to store and handle hydrogen on-board vehicles. Handling includes processing (producing and chemically conditioning) and delivering (conditioning and conveying) hydrogen (or hydrogen rich gas) to a fuel cell stack, internal combustion engine or other power-generation system. The fuel, associated process streams, and byproducts within these systems may present potential hazards.	The purpose of this document is to provide guidance to minimize those hazards. This document identifies safety considerations to be used in the design and construction of these systems to minimize hazards in their operation and maintenance. This document also identifies performance criteria for hydrogen storage systems and the associated test protocols to verify that production hydrogen storage systems and design prototypes satisfy these performance criteria. Additionally this document addresses the following specific items: a. Approaches for the storage and supply of hydrogen within vehicles including compressed gaseous hydrogen, liquid hydrogen, chemical hydrides, and reversible metal hydrides. b. On-board generation of hydrogen (or hydrogen-rich) gas from liquids or solids containing chemically bound hydrogen.	System and Component
ISO 23273-1:2006(E)	Fuel Cell Road Vehicles – Safety Specifications -- Part 1: Vehicle Functional Safety	Specifies the essential requirements for the functional safety of fuel cell vehicles (FCVs) with respect to the hazards to persons and the environment inside and outside the vehicles caused by the operational characteristics of the fuel cell power system. Does not apply to manufacturing, maintenance, or repair of the vehicles. Requirements address both normal operating (fault free) and single fault conditions of the vehicles. Applies only when the maximum working voltage on-board electrical circuits is lower than that of 1,000 VAC or 1,500 VDC according to National or International Standards and/or legal requirements.	The purpose of this document is to provide fuel cell vehicle functional safety requirements with respect to the hazards to persons and the environment inside and outside the vehicles caused by the operational characteristics of the fuel cell power system.	Vehicle

Standard	Title	Scope	Purpose	Vehicle, System, or Component Level
ISO 23273-2:2006	Fuel Cell Road Vehicles – Safety Specifications -- Part 2: Protection Against Hydrogen Hazards For Vehicles Fueled With Compressed Hydrogen	Specifies the essential requirements for FCVs with respect to the protection of persons and the environment inside and outside the vehicle against hydrogen related hazards. Applies only to such FCVs where compressed hydrogen is used as a fuel for the fuel cell system. Does not apply to manufacturing, maintenance, and repair. Requirements address both normal operating (fault free) and single fault conditions of the vehicle.	The purpose of this document is to provide the essential requirements for FCVs with respect to the protection of persons and the environment inside and outside the vehicle against hydrogen related hazards.	System and Component
ISO/DIS 23273-3	Fuel Cell Road Vehicles – Safety Specifications -- Part 3: Protection Of Persons Against Electric Shock	Specifies the essential requirements for FCVs with respect to the protection of persons and the environment inside and outside the vehicle against electric shock. Applies only to onboard electrical circuits with working voltages between 25 VAC and 1,000 VAC or 60 VDC and 1,500 VDC (voltage class B). Does not apply to FCV connected to an external electric power supply, component protection, and manufacturing, maintenance, and repair.	The purpose of this document is to provide the requirements for FCVs with respect to the protection of persons and the environment inside and outside the vehicle against electric shock.	Vehicle and System
Japanese HFCV Standards	Attachment 17: Technical Standard for Fuel Leakage in Collisions, etc. Attachment 100: Technical Standard for Fuel Systems of Motor Vehicles Fueled by Compressed Hydrogen GasAttachment 101: Technical Standard for Protection of Occupants Against High Voltage in Fuel Cell Vehicles	Applies to the fuel tanks and fuel lines (gas containers, piping, and other devices on the hydrogen gas flow passage in the case of motor vehicles fueled by compressed hydrogen gas) of ordinary-sized motor vehicles exclusively for the carriage of passengers, small-sized motor vehicles, or mini-sized motor vehicles. Specifically excluded are vehicles with a passenger capacity of 11 or more, vehicles with a gross weight of more than 2.8 tons, motorcycles, and mini-sized vehicles with caterpillar tracks and sleds.	The purpose of these documents is to provide the requirements for the fuel tanks and fuel lines (gas containers, piping, and other devices on the hydrogen gas flow passage in the case of motor vehicles fueled by compressed hydrogen gas) of ordinary-sized motor vehicles.	Vehicle

Standard	Title	Scope	Purpose	Vehicle, System, or Component Level
WP.29 Draft Standard for Compressed Gaseous Hydrogen	Proposal for a New Draft Standard for Vehicles Using Compressed Gaseous Hydrogen	Sets forth uniform provisions for the approval of specific components of motor vehicles using gaseous hydrogen and the vehicle with regard to the installation of those components.	The purpose of this document is to provide the requirements for specific components of motor vehicles using gaseous hydrogen and the vehicle with regard to the installation of those components.	Vehicle, System, and Component
CSA HGV2	Hydrogen Gas Vehicle Fuel Containers (DRAFT)	This standard contains requirements for the material, design, manufacture and testing of serially produced, refillable Type HGV2 containers intended only for the storage of compressed hydrogen for vehicle operation. These containers are to be permanently attached to the vehicle. Type HGV2 containers shall not be over 1,000 liters (35.4 cu ft) water capacity.	The purpose of this document is to provide requirements for the material, design, manufacture and testing of serially produced, refillable Type HGV2 containers intended only for the storage of compressed hydrogen for vehicle operation.	Component
CSA HPRD1	Pressure Relief Devices for Compressed-Hydrogen Vehicle Fuel Containers (DRAFT)	This standard establishes minimum requirements for pressure relief devices intended for use on fuel containers that comply with ANSI/CSA HGV2, Basic Requirements for Compressed Hydrogen Gas Vehicle (HGV) Fuel Containers and/or CSA B51, Part 2 Boiler, Pressure Vessel and Pressure Piping Code, SAE J2579, Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles, and ISO DIS 15869.2, Gaseous Hydrogen and Hydrogen Blends – Land Vehicle Fuel Tanks.	The purpose of this document is to provide requirements for the material, design, manufacture and testing of pressure relief devices intended for use on hydrogen fuel containers used onboard vehicles.	Component

Table 8. Summary of Content of Compressed FCV Codes, Standards and Analogous FMVSS

Code	SAE J2578	SAE J2579	CSA HGV2	FMVSS 49 CFR 571.303 (FMVSS 303)	FMVSS 49 CFR 571.304 (FMVSS 304)	FMVSS 49 CFR 571.305 (FMVSS 305)
Title	Recommended Practice for General Fuel Cell Vehicle Safety	Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles	Compressed-Hydrogen Gas Vehicle Fuel Containers (DRAFT)	Fuel System Integrity of Compressed Natural Gas Vehicles	Compressed Natural Gas (CNG) Fuel Container Integrity	Electric-Powered Vehicles: Electrolyte Spillage and Electrical Shock Protection
Scope	Safe integration of FCV fuel cell, fuel storage, and electrical systems	Safety considerations for storage and handling of H_2 for fuel cell, ICE, or other H_2 fueled vehicles	Compressed-hydrogen vehicle fuel containers	All motor vehicles < 10,000 GVWR and all school buses – using CNG	CNG motor vehicle fuel containers	All high-voltage electric vehicles <10,000 GVWR; >48 V of electricity as propulsion power; sped >40 km/hr
System or Component	System	System	Component	System	Component	System
Specific Systems or Components	Almost all, fuel cell, fuel storage, and electrical systems	Focus on compressed H_2 system (tank, valves, & PRD) and downstream H_2 piping for delivery	Fuel container only	Crash testing of CNG vehicles to verify achieving allowable fuel spillage rate	Fuel container only	Crash testing of electric-powered vehicles achieving allowable electrolyte spillage rate
Non-Hardware Items						
Component Documentation/Manuals	Yes – Discusses items to address in Owner's, Emergency Response, and Maintenance Manuals	Refers to J2578	No	No	Yes	No
Labels/Signage	Yes – Safety labeling to warn of hazards	Yes, components and safety labels	No	Yes	Yes	No
Training	No	No	No	No	No	No
Procedures/Procedure Requirements	Yes – does not provide procedures but discusses the need for specific procedures (defueling, response, operation)	Yes – fueling/defueling procedure	Yes; test requirements	Yes	Yes	Yes
Cross Cutting Issues						
Materials	No	Yes	Yes	No	Yes	No
Fabrication Guidelines	Some coverage – use of standard engineering practice	Some coverage – use of standard engineering practice	Yes	No	No	No
Operating Guidelines	Yes	Yes	Yes	No	No	No

Code	SAE J2578	SAE J2579	CSA HGV2	FMVSS 49 CFR 571.303 (FMVSS 303)	FMVSS 49 CFR 571.304 (FMVSS 304)	FMVSS 49 CFR 571.305 (FMVSS 305)
Operating Conditions	Yes	Yes, pressure, temperature, fuel quality, shock & vibration	Yes	No	No	No
Crashworthiness	Refers to FMVSS301 and 303 except test gas is He, pressure drop is 5.2% of service pressure, and T/V_{FS} is 2640 to 3730	Refers to J2578	No	Yes	No	Yes
Special Features						
Pertinent References	SAE, ANSI, FMVSS, IEC, ISO, UL, DGMK, EPRI, NFPA	SAE, ASME, CSA, FMVSS, EIHP, IEC, ISO, UL	SAE, ISO, ASTM, ASQ, BSI, CSA, CGA, FMVSS, NACE, NFPA	49 CFR 571.301	None	DOT, SAE J1766
Schematics	No	Yes	Yes	No	No	Yes
FMEA – Design, Production	Yes	Yes	No	No	No	No
Fault Tree Analysis	No	No	No	No	No	No
Glossary/Definitions	Yes	Yes	Yes	Yes	Yes	Yes
Tests	Yes, normal discharges, high-voltage isolation and withstand	Yes, chemical exposure & surface damage, extended & extreme pressure exposure, pressure cycling, permeation, penetration, bonfire, localized fire, burst test, leak, proof pressure, NDE	Yes, bonfire; environmental; Charpy impact; tensile; SLC; corrosion; shear; UV; pressure cycling, burst, hold; temperature cycle; leak; permeation; NDE & visual for flaws; penetration; drop	Yes, front, rear, and side impact	Yes, pressure cycling, hydrostatic burst, and bonfire	Yes, front, rear, and side impact

Code	CSA HPRD1	ISO 23273-1:2006	ISO 23273-2:2006	ISO/DIS 23273-3	Japanese Standards	WP.29
Title	Pressure Relief Devices for Compressed-Hydrogen Vehicle Fuel Containers (DRAFT)	Fuel Cell Road Vehicles – Safety Specifications – Part 1: Vehicle Functional Safety	Fuel Cell Road Vehicles – Safety Specifications – Part 2: Protection Against Hydrogen Hazards for Vehicles fueled with Compressed Hydrogen	Fuel Cell Road Vehicles – Safety Specifications – Part 3: Protection of Persons Against Electric Shock	Attachment 17: Fuel Leakage in Collisions Attachment 100: Fuel Systems of Motor Vehicles Fueled by Compressed Hydrogen Gas Attachment 101: Protection of Occupants Against High Voltage in Fuel Cell Vehicles	Draft Standard for Compressed Gaseous Hydrogen
Scope	Compressed-hydrogen container pressure relief device (PRD)	Functional safety of fuel cell vehicles	Protection against hydrogen hazards	Protection against electric shock	Safe integration of FCV fuel cell, fuel storage, and electrical systems for ordinary sized passenger vehicles	Approval and installation of components for gaseous hydrogen vehicles
System or Component	Component	System	Both	System	System	Both
Specific Systems or Components	Thermally-activated PRD only	Integrated vehicle systems	Fuel system, fuel container, PRD, shut-off valves	Electric system	Almost all, fuel cell, fuel storage, and electrical systems	Almost all, fuel storage, fuel supply, and electrical systems
Non-Hardware Items						
Documentation/Manuals	No	Refer to J2578	No	No	No	No
Labels/Signage	Yes; markings	Refer to J2578	No	Yes	No	Yes, markings
Training	No	No	No	No	No	No
Procedures/Procedure Requirements	Yes; test requirements	No	Yes; test requirements	Yes; test requirements	Yes; test requirements	Yes; test requirements
Cross Cutting Issues						
Materials	Yes	No	No	No	No	Yes
Fabrication Guidelines	Yes	No	Yes, limited	Yes, insulation & barriers	Yes	Yes
Operating Guidelines	No	Yes	Yes	Yes; limited	Yes	No
Operating Conditions	Yes	Yes; limited	No	Yes; failure conditions	Yes	No
Crashworthiness	No	Yes; refers to applicable standards	No	No	Yes (Not for Electrical Isolation)	Yes

Code	CSA HPRD1	ISO 23273-1:2006	ISO 23273-2:2006	ISO/DIS 23273-3	Japanese Standards	WP.29
Special Features						
Pertinent References	ANSI, CSA, CGA, ASTM, ISO, SAE	ISO 8713, 11451, 23273-2, 23273-3, SAE, CISPR	ISO 17268, 23273-1, SAE, UN ECE R13 & R79	ISO 23273-1, 23273-2, 6722, 14572, 60664-1	None	None
Schematics	No	No	No	No	No	Limited to tests
FMEA – Design, Production	Yes	Yes	Yes	Yes	No	No
FTA	No	Yes	Yes	Yes	No	No
Glossary/Definitions	Yes	Yes	Yes	Yes	Yes	Yes
Tests	Yes, design qualification; acceptance testing; batch testing	No	Yes, normal discharges, hydrogen emissions	Yes, high-voltage isolation; insulation resistance; barrier continuity	Yes, gas leak detection; live components; ventilation; gas/air tight housing/piping; collision; vibration; fill port integrity	Yes, endurance; H_2 compatibility; ageing; ozone; corrosion resistance; pressure cycle; leakage; environment; tensile; temperature; shear; etc.

Table 9. Summary of HFCV FMEA and Codes and Standards

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
A.	**Compressed-Hydrogen Fuel Storage System**									
A.1	**Compressed-Hydrogen Storage Subsystem**									
A.1.1	Compressed-hydrogen fuel container	• Leak, loss of hydrogen without a substantial drop in pressure. • Rupture – loss of fuel and fragmentation of container (mechanically, chemically or thermally induced damage).	• Design/Qualification/Manufacturing/QC/Installation reqs.	Design considerations; Tests: Design qualification; Process verification & QC; Installation and Integration requirements.	Design and performance requirements for fuel container; Location/Installation of components	Location and Installation	General design requirements; Design Qual. Tests; Approval Provisions; Location reqs; container test procedures	Container types, Service conditions; Material qualification tests and requirements; design qualification tests; Inspection; Manufacture; Production and Batch tests	Container qualification test requirements	There are several codes (in particular HGV2) that address the design, manufacture, installation, and integration for the safe use of compressed-hydrogen fuel containers. **Potential Gap:** Due to the potential severity of container failure, NHTSA may want to evaluate the sufficiency of proposed fire tests and standards. **Potential Gap:** Due to the potential severity of container rupture caused by fire, NHTSA may want to evaluate the sufficiency of proposed fire tests and standards. **Potential Gap:** Performance testing for leak sensors; enhanced requirements.
			• Hydrogen leak sensors	Process fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests	PRD and bonfire test required	Bonfire	
			• PRD	Thermally activated pressure-relief devices required	Design and performance requirements for fuel containers.		Overpressure protection requirements	PRD required		
A.1.2	Thermally activated PRD	• Fails to vent the contents in the event of a fire. • Vents contents inappropriately (in the absence of fire) • Venting of contents/blowdown,-- loss of fuel and pressure in the container without fragmentation of the container. (mechanically induced damage) • Rupture	• Design/Qualification/Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements.	Design and performance requirements for fuel container; Location/Installation of components	Thermally activated PRD required; location requirements	Overpressure protection requirements; Design qualification tests; Approval provisions; Location and Installation of components.	General design statement; must fully vent; design qualification, production batch testing; Inspection/acceptance;	Container qualification test requirements	HPRD1 addresses the design, manufacture, installation, and integration for the safe use of thermally activated PRDs for installation on fuel containers. Other codes specify that a PRD is required with testing of the PRD related to testing for the integrated fuel container system. **Potential Gap:** The system design for the thermally activated PRD and fuel container could result in a single-point failure of the container should the PRD fail to activate in a fire. System designs to minimize or eliminate this single-point failure mode should be considered.
			• Hydrogen leak sensors	Process fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests	PRD required	Bonfire	

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
A.1.3	Container shut-off selector valve	• Restrict or limit fuel flow. • Leak or rupture • Fail open • Fail closed	• Design/Qualification/Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff – staged warning and shutdown process.	Design and performance requirements; Location/Installation of components	Fail-safe design; no other specific requirements	Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements of the container shut-off selector valve are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component. Most codes also require a fail-safe design that gives provisions for shutting off the fuel supply in an emergency and provisions for control systems to alert the driver and/or shut-down the vehicle system in the event of low fuel cell voltage. **Potential Gap:** If only one fuel container is in use on the vehicle; a failure of the container shut-off selector valve will immediately stop the fuel supply to the fuel cell. If the vehicle is in operation it could stop in a place that is hazardous (i.e., highway) to the driver. Provisions may need to be considered to ensure that an immediate shut-down of the vehicle during operation is not possible (second fuel supply). **Potential Gap:** Fuel system valves and regulators that meet the requirements of applicable ISO and ANSI NGV standards may not be sufficient for hydrogen.
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests			
			• Downstream HP Safety Relief	Overpressure protection requirements	Overpressure protection requirements	PRD or pressure sensor and shutdown of HP H2.	Overpressure protection requirements			
			• Fuel cell voltage monitoring	Monitor critical control; low voltage	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Second container				Max of 4 containers per assembly			
A.1-a	Hydrogen fuel storage line	• Leak or rupture	• Design/Qualification/Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff – staged warning and shutdown process. Piping and associated component parts should be fabricated and tested to conform to all applicable specifications of ANSI/ASME B31.1.	Design and performance requirements; Location/Installation of components	Fail-safe design; Airtightness	Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements for the fuel storage lines and connections are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component. Piping and associated component parts must be fabricated and tested to conform to all applicable specifications of ANSI/ASME B31.1. **Potential Gap:** Japanese Standard requires a pressure gauge on the high-pressure side of the fuel system. **Potential Gap:** Ignition and flammability tests of releases of hydrogen and electrical arcs in the event tubing is severed.
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests			
			• Downstream HP Safety Relief	Overpressure protection requirements	Overpressure protection requirements	PRD or pressure sensor and shutdown of HP H2.	Overpressure protection requirements			
			• Hydrogen leak sensors	Process fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Hydrogen pressure sensor	Process fault monitoring	Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Pressure gage indicating HP side of fuel system				
			• Ventilation	PRDs should be vented to outside the vehicle; See J2578 for PRD discharge	Discharges; PRD shall vent to outside of vehicle	Shall be provided to discharge leaked H_2 & vent in a safe manner	PRD vent to outside of vehicle			

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
A.2 Hydrogen De-Fueling Sub-System										
A.2.4	Defueling manual valve	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Defueling design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			J2578 requires that there be a means to defuel and requires the system to be depressurized to a recommended level followed by a purge with an inert gas. J2579 provides general guidance for design and procedure. The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Hydrogen leak sensors	Process fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Hydrogen pressure sensor	Process fault monitoring	Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Pressure gage indicating HP side of fuel system				
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests			
			• Downstream HP Safety Relief (prevention)	Overpressure protection requirements	Overpressure protection requirements	PRD or pressure sensor and shutdown of HP H2.	Overpressure protection requirements			
			• Container shut-off valve	Fail-safe design to isolate fuel	Fail safe design; Main shut-off valve shall be closed when not operating	Main stop valve must be fail-safe	Container isolation valve; automatic valves must fail-safe			
A.2.5	Defueling port	• Restrict or limit fuel flow • Become bent or damaged	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Defueling design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
A.2-a	Hydrogen defueling line	• Leak or rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
A.3 Hydrogen Fueling Sub-System										
A.3.6	Fill stop/check valve	• Restrict or limit fuel flow • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Defueling design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
A.3.7	Fill port	• Restrict or limit flow • Become bent or damaged	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Defueling design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
A.3-a	Hydrogen fueling line	• Leak or rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
B. Hydrogen Flow Control System										
B.1 High-Pressure (HP) Flow Control Subsystem										
B.1.8	HP Safety Relief	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Downstream MP Safety Relief	Overpressure Protection	Overpressure Protection	PRD or pressure detector & shut-down of HP H_2	Pressure Relief			
			• Ventilation	PRDs should be vented to outside the vehicle; See J2578 for PRD discharge	Discharges; PRD shall vent to outside of vehicle	Shall be provided to discharge leaked H_2 & vent in a safe manner	PRD vent to outside of vehicle			
			• Hydrogen leak sensors	Process fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Hydrogen pressure sensor	Process fault monitoring	Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Pressure gage indicating HP side of fuel system				
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.	Front, side, rear (use Helium)	Container mounting calculation instead of test		Currently not applicable to Hydrogen	
			• Thermal protection & fire test requirements	Bonfire, localized fire; storage system thermal protection			Bonfire, pan fire tests			
			• Container Shut-off Valve	Fail-safe design to isolate fuel	Fail safe design; Main shut-off valve shall be closed when not operating	Main stop valve must be fail-safe	Container isolation valve; automatic valves must fail-safe			

System/Subsystem/Component	Failure Mode	Controls	Applicable Codes and Standards						Comments
			SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	
B.1.9 Main system manual valve	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
		• Upstream HP, downstream MP Safety Relief • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Thermal protection & fire test requirements • Container Shut-off Valve • Crash test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
		• Fuel cell voltage monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
		• Downstream solenoid valves	Fail-safe design, isolation, redundancy	Fail-safe design; means to close main H_2 shut-off valve; excess flow valve	Main-stop valve must operate electromagnetically without fail	Fail-safe design			
B.1.10 Main system solenoid valve	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
		• Downstream MP Safety Relief • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Thermal protection & fire test requirements • Crash test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
		• Main system manual valve, main system solenoid valve and container shut-off valve	Fail-safe design, isolation, redundancy; fail-safe fuel shutoff	Fail-safe design; means to close main H_2 shut-off valve; excess flow valve		Container isolation valve; automatic valves must fail-safe			
		• Fuel cell voltage monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
B.1.11 HP hydrogen filter	• Restrict or limit fuel flow (plugged/clogged) • Allow passage of contaminants (Leak or rupture)	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
		• Hydrogen pressure sensor	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
		• Fuel cell voltage monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			

System/Subsystem/Component	Failure Mode	Controls	Applicable Codes and Standards						Comments
			SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	
B.1.12 HP regulator	• Restrict or limit fuel flow • Seal leak or rupture • Fail to control pressure – fail open • Fails closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
		• Upstream HP, downstream MP Safety Relief • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements • Container Shut-off Valve	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
		• Fuel cell voltage monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
B.1-a HP Hydrogen Flow Control Line	• Leak/rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
B.2 Mid-Pressure (MP) Flow Control Sub-system									
B.2.13 MP safety relief	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
		• Downstream anode safety relief valve • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
		• Main system solenoid valves; Container Shut-off Valve	See B.1.10	See B.1.10	See B.1.10	See B.1.10			

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
B.2.14	LP hydrogen filter	• Restrict or limit fuel flow (plugged/clogged) • Allow passage of contaminants to downstream components (leak or rupture)	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Upstream MP, downstream anode safety relief valves • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
			• Main system solenoid valves; Container Shut-off Valve	See B.1.10	See B.1.10	See B.1.10	See B.1.10			
			• Fuel Cell Voltage Monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
			• Flow meter	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions					
B.2.15	Anode pressure regulator	• Restrict or limit fuel flow • Seal leak or rupture • Fail to control pressure – Fails open • Fails closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Upstream MP safety relief valve and anode safety relief valve • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
			• Main system solenoid valves; Container Shut-off Valve	See B.1.10	See B.1.10	See B.1.10	See B.1.10			
			• Fuel Cell Voltage Monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
			• Flow meter	See B.2.14	See B.2.14					
B.2-a	MP Hydrogen Flow Control Fuel Line	• Leak/rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
B.3 low-Pressure Flow Control Sub-system										
B.3.16	Anode safety relief	• Restrict or limit fuel flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
			• Main system solenoid valves; Container Shut-off Valve	See B.1.10	See B.1.10	See B.1.10	See B.1.10			
			• Fuel Cell Voltage Monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
			• Flow meter	See B.2.14	See B.2.14					
B.3.17	Hydrogen flow meter	• Fail to function properly • Leak or rupture	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
B.3.18	Hydrogen pressure sensor	• Fail to function properly • Leak or rupture	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Ventilation • Hydrogen leak sensors	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
			• Flow meter	See B.2.14	See B.2.14					

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards						Comments
				SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	
B.3.19	Final hydrogen solenoid valve	• Restrict or limit fuel flow • Leak or rupture	• Design/Qualification/ Manufacturing/QC/Installation reqs.	Design considerations; Over-protection requirement; Tests: Design qualification; Process verification & QC; Installation and Integration requirements. Fail-safe fuel shutoff.	Design and Performance requirements		Design statement; specifications for hydrogen components; fail-safe design; Design qualification tests; Conformity of Production; Location and Installation of Components			The design, manufacture, and installation requirements are only generally addressed in SAE J2579 as part of testing requirements for any hydrogen component.
			• Upstream anode safety relief • Ventilation • Hydrogen leak sensors • Hydrogen pressure sensor • Crash test requirements • Thermal protection & fire test requirements • Main system solenoid valves; Container Shut-off Valve	See B.1.8	See B.1.8	See B.1.8	See B.1.8			
			• Fuel Cell Voltage Monitoring	See B.1.9	See B.1.9	See B.1.9	See B.1.9			
B.3-a	LP Hydrogen Flow Control Fuel Line	Leak/rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
C. Fuel Cell System										Limited standards exist for the fuel cell and auxiliary components. Standards that address the fuel cell system primarily do so in relation to minimizing electrical hazards leading to electric shock or ignition of released vapors.
C.1 Fuel Cell Stack Sub-system										Standards related to fuel cell design, qualification, manufacture, installation, and hazards during operation (seal leakage; membrane holes; over-temperature) may require more detail.
C.1.20	Fuel cell stack	• Membrane rupture (or small holes) • Seal leakage • Short circuit	• Design/Qualification/Manufacturing/QC/Installation reqs.	General design principles; Ref. SAE J2344; High-voltage dielectric withstand capability	High-voltage isolation test					J2578 generally addresses fuel cell system safety without specific performance tests or prescriptive requirements. J2578 states that the fuel cell system shall be designed using standard engineering practice until relevant SAE documents are available and SAE J2344 should be used for subsystems using electrical components. J2578 further states that the fuel cell stack shall be designed to prevent hazardous operating conditions (fluid leakage, overpressure, fire and shock). Section 4.3.5 addresses potential faults to monitor including cell stack or process fault (out-of-limit thermal, pressure, flow, or composition), ground fault, low-voltage fault, and overcurrent fault; resolved by having a fail-safe design and procedures that isolate fuel sources through staged warnings and safety shut-downs.
			• Hydrogen sensor on cathode							
			• Oxygen sensor on anode							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
C.1.21	Anode recirculation pump	• Fails to function • Leak	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions					
			• Thermal protection & fire test requirements							
			• Hydrogen leak sensors	Fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
C.1.22	Anode purge valve	• Restrict or limit flow • Leak or rupture • Fail open • Fail closed	• Design/Qualification/Manufacturing/QC/Installation reqs.				Fail-safe design			
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Thermal protection & fire test requirements							
			• Hydrogen leak sensors	Fault monitoring	Hydrogen-related fault conditions	At least one detector at appropriate position; warning and shutdown	Required test procedures			
			• Crash test requirements	Ref. FMVSS with mod. for H2.	Must meet applicable national/international stds.					
C.1.23	Cathode humidifier	• Not functional • Leak from inlet to exit	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
C.2 Cooling Sub-system										
C.2.24	Radiator	• Restrict or limit coolant flow • Fails to function	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Temperature sensors	Process fault monitoring						
C.2.25	Stack coolant pump	• Fails to function • Leak or rupture	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Temperature sensors	Process fault monitoring						
C.2.25-c	Coolant line	• Leak or rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
C.3 Air Supply Sub-system										
C.3.26	Cathode air filter	• Restrict or limit air flow (partially plugged/clogged) • Hole in filter media • Plugged	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Temperature sensors	Process fault monitoring						

System/Subsystem/Component		Failure Mode	Controls	Applicable Codes and Standards: SAE (J2578, J2579)	ISO (23273-1, -2, -3)	Japanese (HFCV Standards)	European (WP.29 Draft)	CSA (HGV2&HPRD1)	FMVSS (303, 304, 305)	Comments
C.3.27	Cathode air blower	• Fails to function	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Temperature sensors	Process fault monitoring						
C.3.28	Air flow meter	• Fails to function properly	• Design/Qualification/Manufacturing/QC/Installation reqs.							
			• Voltage Monitoring	Fuel cell system and stack monitoring – general requirements; Ref. to IEC 61508-3 and UL 1998.	Notify driver of FC power reductions	Test for function of switch to shut off power due to electrical leak	Electronic control syst must be tested			
			• Temperature sensors	Process fault monitoring						
C.3-a	Air line	• Leak, rupture	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	See A.1-a	
D.	**Vehicle Control System (Electronic)**	• Fails to function properly								Under fault monitoring J2579 says that faults that cannot be managed by the fuel system should be communicated to the vehicle integrator, however there is little mention of the vehicle integrator. **Potential Gap:** General requirements exist for the Vehicle Control System, including process fault monitoring is addressed with fail-safe design. Specific performance criteria for the control system are not currently addressed.
E.	**Vehicle**	• Fails to function properly following a crash or external fire	• Crash test requirements							**Potential Gap:** Full vehicle fire tests of the fuel system (including the container) may need to be considered to ensure that the integrated fuel system does not pose any hazards above and beyond those of the individual component fire tests.

6.3 POTENTIAL GAPS IN STANDARDS

Following is a list of topics that may need to be considered for further evaluation, based on the comparison of results of the FMEA to applicable codes and standards.

Hydrogen Components

- Standards currently exist that address the design, manufacture, installation, and integration for the safe use of compressed-hydrogen fuel containers. A standard is also being prepared for pressure relief devices for compressed-hydrogen vehicle fuel containers. The design, manufacture, and installation requirements for other hydrogen components are generally addressed in SAE J2579 but only briefly in terms of testing. References are made to applicable ISO and ANSI NGV standards but it states that they may not be acceptable for hydrogen and that care should be taken to ensure that the unique concerns related to compressed hydrogen are considered in the design, manufacture, and testing of the individual components.

- The NGV3 committee is expanding the scope of ANSI/CGA America NGV 3.1-1995 to address hydrogen system components, other than containers and PRDs, for hydrogen-gas-powered vehicles. The plan is to start this activity in the May-June 2007 time period, with the first draft completed in March 2008. NHTSA may want to review the guidelines provided to ensure that the components will be designed for safe use with hydrogen fuel cell vehicles.

- ISO 15500 standards address CNG fuel system components for road vehicles. There are currently no similar ISO standards for hydrogen vehicle components, although plans may be underway.

Compressed-Hydrogen Fuel Containers

- As mentioned above, codes currently exist that address the design, manufacture, installation, and integration for the safe use of compressed-hydrogen fuel containers. However there is currently no FMVSS specific to the unique concerns related to compressed-hydrogen fuel containers and the integrated fuel cell systems during a crash. Due to the potential severity of container failure, NHTSA may want to evaluate the sufficiency of proposed tests and standards.

Fire Testing

- Vehicle fires are not a well characterized hazard and, consequently, present a significant design challenge. Fire can be caused by many factors, can originate inside or outside the vehicle, and can travel different paths and speeds depending upon many factors. Currently the “design” fire for gaseous fuel vehicles is embodied in the fuel container bonfire tests such as in FMVSS 304. The containers are protected by thermally activated pressure relief devices typically located at a port at each end of the container that activate when their immediate surroundings are heated, but cannot detect localized heat sources elsewhere. They protect containers from large, distributed fires, but not highly localized fires. Technology and standards to address localized fire is under investigation and consideration by the hydrogen and natural gas vehicle industry. NHTSA may want to consider better characterizing the risk from potential vehicle fire scenarios and to develop improved fire test methods.

- Consider issues of ignition, flammability of releases of hydrogen, and electrical arcs, in the event tubing is severed.

- Current material flammability tests are not conducted with a hydrogen flame. Consider requiring that the tests be conducted with a hydrogen flame to more accurately assess the impacts.

- Consider self-ignition tests to determine conditions under which external debris or particulate matter can cause ignition of venting hydrogen.

Leak Detection

- Hydrogen leak detection is only generally addressed with respect to fault monitoring. Additional requirements may need to be considered, including performance testing to measure hydrogen leakage and concentrations in and around the fuel system over time in conjunction with passive and active ventilation systems.

High-Consequence Failure Modes

- The system design for the thermally activated PRD and fuel container could result in a single-point failure of the container should the PRD fail to activate in a fire. System designs to minimize or eliminate this single-point failure mode should be investigated.

- If only one fuel container is in use on the vehicle; a failure of the container shut-off selector valve will immediately stop the fuel supply to the fuel cell. If the vehicle is in operation it could stop in a place that is hazardous (i.e., highway) to the driver. Provisions may need to be added to ensure that an immediate shut-down of the vehicle during operation is not possible (second fuel supply).

- The conceptual model used in this analysis included a single pressure gauge in the low-pressure section of the fuel deliver line. The Japanese HFCV Standard requires an additional pressure gauge on the high-pressure side of the fuel system. Investigators may want to consider evaluating the potential impact this would have on system safety.

Fuel Cell and Auxiliary Components

- Limited standards exist for the fuel cell and auxiliary components. Standards that address the fuel cell system primarily do so in relation to minimizing electrical hazards leading to electric shock or ignition of released vapors. J2578 generally addresses fuel cell system safety without specific performance tests or prescriptive requirements. J2578 states that the fuel cell system shall be designed using standard engineering practice until relevant SAE documents are available, and SAE J2344, Guidelines for Electric Vehicle Safety should be used for subsystems using electrical components. J2578 further states that the fuel cell stack shall be designed to prevent hazardous operating conditions (fluid leakage, overpressure, fire, and shock). It addresses potential faults to monitor including cell stack or process fault (out-of-limit thermal, pressure, flow, or composition), ground fault, low-voltage fault, and overcurrent fault. It is resolved by having a fail-safe design and procedures that isolate fuel sources through staged warnings and safety shut-downs.

Voluntary standards related to fuel cell design, qualification, manufacture, installation, and hazards during operation (seal leakage, membrane holes, over-temperature) may require more detail.

- SAE is currently developing procedures for testing PEM fuel cell systems and their major subsystems for automotive applications:

    - SAE J2615, "Performance Test Procedures for Fuel Cell Systems for Automotive Applications," has been published, will be reviewed, and terms will be harmonized with J2617.
    - SAE J2616, "Performance Test Procedures for the Fuel Processor Subsystem of Automotive Fuel Cell System," is being reviewed.
    - SAE J2617, "Performance Test Procedure of PEM Fuel Cell Stack Subsystem for Automotive Application," has passed balloting and was published in 2007.
    - SAE J2722, "Recommended Practice for the Durability Testing of PEM Fuel Cell Stacks," is in draft form.

Vehicle Control System

- General requirements exist for the vehicle control system including process fault monitoring that is addressed with fail-safe design in SAE J2578 and J2579 standards. Specific performance criteria for the control system are not currently addressed.

7.0 RESULTING ASSESSMENT OF SAFETY ISSUES

NHTSA requested that Battelle perform a failure modes and effects analysis to characterize potential hazards from compressed-hydrogen fuel cell vehicles and identify potential safety issues that NHTSA may want to consider addressing to help ensure the safety of passengers and the public.

Battelle focused this assessment on two fundamental questions:

- In its regulatory function, what safety issues should NHTSA consider prioritizing for compressed-hydrogen vehicles?
- Are there gaps in the coverage of safety standards for compressed-hydrogen vehicles that merit NHTSA's consideration?

To address these very challenging questions, Battelle adopted a structured and systematic approach that included the following activities:

- Review of NHTSA's safety objectives and the general topics addressed by the FMVSS to characterize NHTSA's potential roles in hydrogen safety.
- Review of the unique elements of compressed-hydrogen vehicles in an effort to narrow the scope of the assessment to those elements that are unique to hydrogen vehicles.
- Review of the unique hazards of compressed-hydrogen vehicles.
- Failure modes and effects analysis of a conceptual compressed-hydrogen fuel cell vehicle to characterize potential hazards and potential controls to mitigate these hazards.
- Compare the results of the FMEA with fuel cell vehicle codes and standards to identify potential gaps in safety coverage that may need to be considered.

Battelle has focused this investigation on compressed hydrogen, polymer electrolyte membrane fuel cell vehicles. While other fuel storage and fuel cell options are under development, compressed hydrogen is believed to be the most likely near-term solution and the best focus. Secondly, electrical shock hazards are investigated in a complementary Subtask under this contract[1] and, for completeness, are addressed, but only at a high level in this report. Last, this task has drawn liberally from a complementary contract for NHTSA being conducted in parallel that is focused on collecting and summarizing current codes and standards efforts for compressed-hydrogen fuel cell vehicles.

This section presents a summary of the assessment, highlighting high-consequence failure modes, root causes, design controls, and potential gaps in the current codes and standards.

7.1 HIGH-CONSEQUENCE FAILURE MODES

Overall, the unique failure modes that appear to have the greatest hazard in hydrogen vehicles are large releases of hydrogen and rupture of the fuel container. The FMEA results show that high-pressure components in compressed-hydrogen fuel systems lack redundancy such that single-point failure of the container, PRD or first valve can result in a large scale release or venting of hydrogen and, for containers, release of mechanical energy. Small releases of hydrogen and rupture of other components may also be hazardous, but do not have the potential destructive force of large releases and fuel container rupture.

Potential consequences of a hydrogen release in the storage area can vary depending on the circumstances under which the release occurs. Since the compressed-hydrogen fueling and fuel storage system contains a large amount of fuel at high pressures, the main consequences of a hydrogen release may include:

- Immediate ignition of released fuel resulting in a high-pressure hydrogen jet flame hazard;
- Collection of a combustible mixture in a closed environment leading to a fire hazard;
- Collection of hydrogen in a closed environment leading to an asphyxiation hazard; and
- Delayed ignition of collected vapors leading to a potential explosion or detonation hazard.

The primary failure modes considered in the FMEA for the compressed-hydrogen fueling and fuel storage system include leak or rupture of the fuel container, fuel delivery lines and associated components. Secondary failure modes considered include failure of PRDs or valves to open or close when required. As detailed in the FMEA there are a number of potential causes for these component failure modes that can be grouped as follows:

- Inadequate design, testing, manufacturing, installation, or maintenance of equipment;
- Damage caused by external fire; and
- Damage caused by external impact (including crashes and road debris).

Potential consequences of a compressed-hydrogen container rupture can also vary depending on the circumstances. The main consequences of a container rupture may include:

- Immediate ignition of released fuel resulting in a high-pressure hydrogen jet flame hazard;
- Collection of a combustible mixture in a closed environment leading to a fire hazard;
- Collection of hydrogen in a closed environment leading to an asphyxiation hazard;
- Delayed ignition of collected vapors leading to a potential explosion or detonation hazard;
- Explosive release of mechanical energy and of the container/component materials; or
- Dislodging/ejection of components due to an inertial release of the compressed-hydrogen gas.

Potential causes for a container rupture can be grouped as follows:

- Inadequate design, testing, manufacturing, installation, or maintenance of equipment;

- Damage caused by external fire or localized fire; and
- Damage caused by external impact (including crashes and road debris).

As noted above, industry codes and standards currently exist or are in development; these address the design, manufacture, installation, and integration for the safe use of compressed-hydrogen fuel containers. However there is currently no FMVSS specific to the concerns related to compressed-hydrogen fuel containers and the integrated fuel cell systems during a crash. Due to the potential severity of container failure, NHTSA may want to evaluate the sufficiency of proposed tests and standards for compressed-hydrogen fuel containers.

7.2 Root Causes and Design Controls

As part of the FMEA process, the analysts identified typical HFCV safety features designed to prevent a failure or help to mitigate potential consequences. These basic features are listed in Table 10 below.

Table 10. Controls Designed to Address Root Causes and Failure Modes

Root Causes/Failure Modes	Controls
• External impact	• Crash test requirements – to provide a systems approach to help ensure fuel system integrity to prevent or minimize the release of hydrogen in the event of a crash. • Impact sensors – to provide a means to detect a crash and send a signal to activate the automatic fuel shutoff(s) and electrical disconnect(s).
• Inadequate design, testing, manufacturing, installation, or maintenance of equipment • Degradation • Mechanical, electrical, electronic failures • Wrong material • Poor quality hydrogen	• Design/Qualification/Manufacturing/QC/Installation/Maintenance requirements – to ensure that all components used within the fuel storage, supply, and fuel cell systems are designed, appropriately tested, installed, and maintained for the service environment in which they will operate.
• Line or component failure	• Fail-safe design – to prevent the unwanted discharge of fuel resulting from a single-point failure of the shutoff function.
• Flow restriction • Leak or rupture of line or component	• Flow meter – to provide an indication to the vehicle control system to help manage the flow of hydrogen to the fuel cell.
• Degradation • Seal failure	• Leak detection: Hydrogen leak sensors – to provide a means to detect hydrogen leakage and provide a warning and shut off of hydrogen fuel flow.
• Overpressure	• Pressure relief – to provide a means to relieve excess pressure in a safe manner away from the vehicle and prevent a line or component rupture.
• Leak or rupture of line or component • Flow restriction • Regulator failure	• Pressure sensor – to provide an indication to the vehicle control system to help manage the hydrogen fuel pressure in the fuel supply system.

Root Causes/Failure Modes	Controls
• Failure of the cooling system	• Temperature sensors – to monitor the temperature of the fuel stack.
• External fire or localized fire	• Thermal protection and fire test requirements – to demonstrate that fire protection systems in the hydrogen storage systems will prevent the rupture of the containment vessel when exposed to fire.
• Leak • PRD fails open	• Ventilation – to provide a means to discharge leaked hydrogen away from the vehicle.
• Reduced flow of hydrogen to the anode • Overpressuring the anode	• Voltage monitoring – to monitor fuel cell stack performance and provide a means to detect low voltage or overcurrent that could lead to internal or external component failures and subsequent exposure of personnel to hazards.

7.3 Highly Variable Hazards

To achieve safety and performance objectives, most systems are designed to prevent worst-case failures, where "worst case" is a maximum stress from the service environment, such as maximum temperature or maximum number of stress cycles. Vehicle engineering is more problematic in that vehicles are used in such a wide variety of applications and environments that worst-case conditions cannot be readily defined or measured. Two examples of such hazards are vehicle crash and fire. Both are difficult to characterize because their severity depends upon multiple random variables. Nevertheless, each of these is critically important for hydrogen vehicles, because they have the potential to contribute to or cause serious failure modes of container rupture and/or large hydrogen release.

Crash

Vehicle crashes are highly variable events in which key variables of mass, speed, and direction of impact of vehicles involved are not limited or controlled. Despite this challenge, NHTSA has successfully improved crash safety by defining minimum crash safety requirements and crash safety ratings for vehicles. Automotive engineers have responded with crash management structures and systems that protect the occupants in these "design crash scenarios."

In the 300 series of the FMVSS, NHTSA has similarly established minimum crash safety requirements for fuel systems. FMVSS 303 specifically addresses CNG vehicle fuel systems, which are similar to compressed-hydrogen fuel systems. This standard specifies a maximum allowable pressure drop in the fuel system following front, rear, and side impacts prescribed in the standard.

Hydrogen fuel containers are designed to operate at pressures over 10,000 psi (70 MPa) during routine service for up to 15 to 25 years and, consequently, are structurally strong and durable. The walls of these pressure vessels are thicker and stronger than the adjacent structural components of the vehicle and any protective cages. Currently, there is no experience to suggest that the damage in a collision would be great enough to cause immediate destructive rupture of a hydrogen fuel container. However, the attached high-pressure lines and cylinder appurtenances may be deformed or sheared, resulting in leakage or loss of fuel. In reported vehicle accidents with similar natural gas vehicles, fuel containers have not ruptured and, in most cases, the container continued to maintain pressure.

Results of this investigation confirm that existing crash testing requirements could be enhanced to include compressed hydrogen to achieve the same level of safety as other fuel systems. No evidence was found in this investigation to suggest that additional or different crash scenarios were needed for hydrogen vehicles or fuel systems. One element that does require further consideration and analysis, however, is the allowable leakage rate following a crash. As indicated earlier, because of its inherently low electrical conductivity, compared to natural gas or gasoline vapor, when flowing, hydrogen has a propensity to generate electrostatic charges to levels that exceed its lower minimum-ignition energy. In other words, hydrogen has a propensity to self-ignite when being vented, a property that makes it rather unusual with regard to fire hazards. NHTSA may want to consider the potential for self-ignition in its evaluation of allowable leakage.

Fire

Fire is a hazard for hydrogen vehicles because it can cause catastrophic rupture of the hydrogen fuel container and fuel system if they are not properly vented. Fire is highly variable, like crash events. There is a range of fire scenarios to which a vehicle, fuel system, and fuel container may be exposed, and they are not well defined in an engineering design sense. Examples of vehicle fire scenarios include

- Liquid fuel spill fire under vehicle (from crash with gasoline or diesel fueled vehicle);
- Brake and tire fire (common on buses);
- Passenger compartment fire resulting from electrical short or payload fire;
- Vandalism; and
- Payload fire in the trunk.

Once initiated, the progression of fire depends upon availability of flammable materials and the surrounding environment. Hence the exposure of the fuel container and fuel system is difficult to define.

High temperature in a fire will raise the internal pressure of the container and degrade the strength of metal, thermoplastic, and composite container materials, potentially causing rupture. They are protected by thermally activated pressure relief devices that open when heated and rapidly blow down or vent the full contents of a fuel container.

The “design” fire for hydrogen and natural-gas-fueled vehicles is a “pool or engulfing fire” scenario embodied in the fuel container bonfire tests such as in FMVSS 304. In this test a full or partially full container is suspended 4 inches over a “uniform fire source” 1.65 meters (65 inches) in length and required either to vent its contents through a PRD or to not burst within 20 minutes. The containers are protected by thermally activated pressure relief devices typically located at a port at each end of the container. Long tanks, such as those used on buses, may have piping exterior to the container to locate another PRD midway along its length.

Current thermally activated PRDs are local heat detectors only. Hence, they activate when their immediate surroundings are heated, but cannot detect localized heat sources elsewhere on the container. They protect containers from large, distributed fires such as pool fires, but not highly localized fires. Ruptures have occurred on natural gas fuel containers recently due to localized fire impingement.[15]. Technology and standards to address localized fire are under investigation and consideration by the hydrogen and natural gas vehicle industry.

Although there are multiple scenarios for vehicles fires that could impinge upon a hydrogen fuel system, the only test found in available codes and standards is the bonfire test described above. Recognizing the potentially catastrophic nature of container burst due to fire, suggests the need for an analysis that defines typical and atypical vehicle fire scenarios, their likelihood and the likelihood they will affect fuel containers. It suggests this analysis should include a comprehensive assessment of fires that H2 containers may be exposed to as well as ranking and categorization based on their likely impact on fuel systems. From this, government and industry can develop a more comprehensive and representative approach to fire qualification testing, thus improving safety and reducing the likelihood of container rupture. This characterization should lead to a more clear definition of the fuel system and vehicle elements that may need to be included in a fire test that truly captures the entire fire protection system.

8.0 REFERENCES

1. Battelle, 2007a. Electrical Isolation Test Procedure for Hydrogen Fuel Cell Vehicles, Final Report. NHTSA Contract Number DTNH22-02-D-02104, Task Order 014, Subtask 2, Final Report, September 2007. Washington, DC: National Highway Traffic Safety Administration.
2. Battelle, 2007b. Evaluation and Comparative Analysis of Existing and Draft Hydrogen Fuel Cell Vehicle (HFCV) and Related Component Regulations and Standards, Final Report. NHTSA Contract Number DTNH22-02-D-02104, Subtask 12, September 2007. Washington, DC: National Highway Traffic Safety Administration.
3. Hennessey, B., Hammel-Smith, C., & Koubek, M., 2005. NHTSA's Four-Year Plan for Hydrogen, Fuel Cell and Alternative Fuel Vehicle Safety Research. Proceedings of the 19th International Technical Conference on the Enhanced Safety of Vehicles (ESV) - Washington D.C. June 6-9, 2005. Paper Number 05-0034. Southfield, MI: United States Council for Automotive Research, LLC.
4. Battelle, 2004. Survey of Potential Safety Issues With Hydrogen-Powered Vehicles. Final Report, prepared by Stephens, D. R., Gifford, M. T., & George, P. E., for USCAR Safety Working Group of USCAR, August 2004. Southfield, MI: United States Council for Automotive Research, LLC.
5. Stephens, D. R., Herridge, J. T., & Gifford, M. T., 2002. Reference Guide for Integration of Natural Gas Vehicle Fuel Systems. GRI 02/0013, Battelle Final Report for the Gas Research Institute, January 2002. Des Plaines, IL: Gas Research Institute.
6. Drell,, I. and Belles, F., 1958. Survey of Hydrogen Combustion Properties. Report 1382. Washington, DC: National Advisory Committee for Aeronautics (now National Aeronautics and Space Administration).
7. AGA, 1965. *Gas Engineers Handbook*, Chapter 5.2 Combustion of Gas. Washington, DC: American Gas Association.
8. Reed, R. J., 1978. North American Combustion Handbook, Second Edition. Cleveland, OH: North American Manufacturing Co.
9. Kuchta, J. M., 1985. Investigation of Fire and Explosion Accidents in the Chemical, Mining, and Fuel-Related Industries. Bulletin 680. Pittsburgh, PA: U. S. Bureau of Mines.
10. Xu, B. P., El Hima, L., Wen, J. X., Dembele, S., & Tam, V. H. Y. Numerical Study of Spontaneous Ignition of Pressurized Hydrogen Release into Air. International Conference on Hydrogen Safety, S. Sebastian Spain, September, 2007. London, England: Fire and Explosion Research Centre, Kingston University.
11. Astbury, G. R., & Hawksworth, S. J. Spontaneous Ignition of Hydrogen Leaks: A Review of Postulated Mechanisms. International Conference on Hydrogen Safety, Pisa, Italy, September 2005. Buxton, U.K.: Health & Safety Laboratory.
12. Edgar, J., 1999. "Goodbye 12 volts… hello 42 volts." AutoSpeed, Issue 50 (October 5, 1999). Victoria, AU: Web Publications PTY, Limited. Available online at http://autospeed.drive.com.au/cms/A_0319/article.html. Accessed May 8, 2007.
13. Kassakian, J. G., et al., 2000. "Automotive Electronics Power Up." IEEE Spectrum, May.
14. Weiss, M. A., Heywood, J. B., Drake, E. M., Schafer, A., & AuYeung, F. F., 2000. On the Road in 2020: A Life-Cycle Analysis of New Automobile Technologies. Energy Laboratory Report # MIT EL 00-003, 161 pp. Cambridge, MA: Massachusetts Institute

of Technology. Available on the Web at http://www.e-mobile.ch/pdf/2004/Massachusetts2020.pdf. Accessed May 8, 2007.

15. Seattle Fire Department, 2007, Operations Division, Firefighter Near Miss, Auto Fire With Compressed Natural Gas (CNG) Fuel Tank Explosion, PowerPoint Presentation, Revised Version November 24, 2007, www.seattle.gov/fire/publications/cng/CNGAutoFire.ppt.

Standards

International Electrotechnical Commission

- IEC 60479-1, Technical Specification, Effects of current on human beings and live stock

CSA America

- CSA HGV2 (Hydrogen Gas Vehicle) Fuel Containers, Basic Requirements for Compressed Hydrogen Gas Vehicle (HGV) Fuel Containers, Draft Working Document, 10/13/2006
- CSA HPRD1, Pressure Relief Devices for Compressed Hydrogen Vehicle Fuel Containers, Draft Working Document, 3/28/2007

Federal Motor Vehicle Safety Standards

- FMVSS 303: Fuel System Integrity of Compressed Natural Gas (CNG) Vehicles
- FMVSS 304: Compressed Natural Gas Fuel Container Integrity
- FMVSS 305: Electric Powered Vehicles: Electrolyte Spillage And Electrical Shock Protection

International Organization for Standardization

- ISO 23273-1:2006(E): Fuel Cell Road Vehicles -- Safety Specifications -- Part 1: Vehicle Functional Safety, First Edition, 4/1/2006
- ISO 23273-2:2006: Fuel Cell Road Vehicles -- Safety Specifications -- Part 2: Protection Against Hydrogen Hazards For Vehicles Fueled With Compressed Hydrogen, First Edition, 5/15/2006
- ISO/DIS 23273-3: Fuel Cell Road Vehicles -- Safety Specifications -- Part 3: Protection Of Persons Against Electric Shock, 6/2006

Japanese HFCV Standards

- Attachment 17: Technical Standard for Fuel Leakage in Collisions
- Attachment 100: Technical Standard for Fuel Systems of Motor Vehicles Fueled by Compressed Hydrogen Gas
- Attachment 101: Technical Standard for Protection of Occupants Against High Voltage in Fuel Cell Vehicles

Society of Automotive Engineers SAE J2578: Recommended Practice for General Fuel Cell Vehicle Safety (12/2002)

- SAE J2579 Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles, Draft Working Document, 2006

United Nations Economic Commission for Europe

- WP.29 Draft Standard for Compressed Gaseous Hydrogen, Proposal for a New Draft Regulation for Vehicles Using Compressed Gaseous Hydrogen, 12/10/03

APPENDIX A
SUMMARY OF HYDROGEN VEHICLE CODES AND STANDARDS

SAE Recommended Practices

SAE International, through the voluntary work of more than 7,000 committee members and participants, maintains over 8,300 technical standards and related documents. Through its Fuel Cell Standards Committee, SAE has developed or is currently developing recommended practices to address emerging fuel cell vehicle technologies. The SAE Fuel Cell Standards Committee is comprised of several Working Groups (WGs), each with its own area of expertise, including safety, interface, emissions, performance, and terminology.

This report highlights the two main standards developed by the SAE Safety Working Group for fuel cell vehicle safety, one published (SAE J2578) that focuses on vehicle safety, and one still in the developmental stages (SAE J2579) that focuses on safety of integrated systems and components. As of August 2006, the Safety Working Group was progressing with revisions to SAE J2578, General Fuel Cell Vehicle Safety, first published as a Recommended Practice in December 2002. At the same time, the draft of SAE J2579, Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles, is being developed. Each document is discussed below.

SAE J2578 - Recommended Practice for General Fuel Cell Vehicle Safety

The SAE Recommended Practice J2578 is a performance standard that provides technical guidance on general FCV safety as well as the safety and safe integration of the fuel cell system, fuel storage system, and electrical systems for overall FCV safety. The purpose of this document is to provide introductory mechanical and electrical system safety guidelines that should be considered when designing fuel cell vehicles for use on public roads.

The fundamental hierarchy of vehicle system safety design as described in SAE J2578 is:

- Protection of vehicle occupants and the public from injuries that could result from failure of vehicle components in operation or from external impacts (collisions);
- Protection of vehicle occupants, general public, and service personnel from hazards associated with operating or servicing of the fuel cell vehicle; and
- Minimization of vehicle system damage caused by subsystem or component failures.

SAE J2578 provides guidance in developing vehicle designs so that any single-point hardware or software failure will not result in an unreasonable risk to people or uncontrolled behavior of the vehicle through implementation of appropriate means (FMEA, isolation, separation, redundancy, supervision, and automatic disconnects). Specifically, the standard sets forth provisions for general vehicle safety in which recommendations are provided for safe vehicle designs, electromagnetic compatibility and tolerance to electrical transients, and FCV crashworthiness. Table A-1 provides an overview of the tests or requirements for each system and subsystem covered in the FMEA.

Table A-1. Overview of SAE J2578

System	Tests or Requirements
Vehicle	• **Crashworthiness:** Meet government requirements for fuel system integrity (FMVSS 301 & 303) and electrical integrity (FMVSS 305); with modifications for hydrogen gas (test pressures; helium test gas; electrical isolation criteria). • **Safety Design:** Single point hardware or software failure should not result in an unreasonable risk to persons or uncontrolled behavior of the vehicle through implementation of appropriate means (FMEA, isolation, separation, redundancy, supervision, and automatic disconnects). • **Vehicle Operation:** A single main switch function should be provided so that the operator can disconnect traction power sources, shutdown the fuel cell system, and shutoff fuel supply. The main switch shall be activated by and accessible to the operator, similar to a conventional ignition switch; SAE J2344 for guidance on preventing unintended motion when parked. • **Fail-Safe Design:** FCV should have a failsafe design and have the ability to perform staged warnings and/or safety shutdowns when faults that could lead to hazardous conditions are detected (isolate fuel and electrical supplies); use main switch to shutdown, crash sensors, and/or warnings to the operator. • **Electromagnetic Tolerance:** All assemblies should be functionally tolerant (including no false shutdowns) of the electromagnetic environment to which the vehicle will be subject. • **Normal Discharge Tests:** Vehicle should be designed to minimize discharges (>25% LFL) during normal operation by accounting for operating variations, component wear, and ageing effects; fuel constituents in purges, vents, and exhausts that occur during normal operation, start-up, and shut-down should be non-hazardous (<25% LFL – can use barriers, natural/forced ventilation, catalytic reactors, or other). • **Ignition Sources:** Minimize potential ignition sources through design and control of external temperatures, electrical equipment, static discharge, and catalytic materials. • **Labels, Manuals, and Safety Info:** Provisions for warning labels, service manuals, and information to warn of potential hazards with vehicle operation, service, and emergency response. • **Water Immersion:** Immersion of FCV in water should not result in electrical potential, emissions, or flame/explosion hazardous to nearby people.
Hydrogen Fuel System	• **Engineering Design:** The fuel system should be designed to standard engineering practices until relevant SAE documents are available. • **Failsafe Design:** Means should be provided to prevent unwanted discharge of fuel from single-point failures of the shut-off system. • **Fault Monitoring:** Fuel system faults that may require monitoring include: fuel discharge fault; fuel shutoff fault; process fault; or ventilation fault.
Hydrogen Storage Sub-System	• See Hydrogen Fuel System
Hydrogen De-Fueling Sub-System	• **De-fueling:** Vehicle manufacturer should provide a means of removing fuel from FCVs; including depressurizing and purging the onboard storage and fuel systems.
Hydrogen Fueling Sub-System	• **Safe Fueling:** During fueling automatic systems that ensure the vehicle traction system is de-energized and ready for fueling should be used. • **Gas Accumulation:** Fueling location should be designed to prevent accumulation of flammable gas and ingress of foreign material. • **Grounding to Fill Station During Refueling**: A means needs to be provided to have the vehicle ground plane at the same potential as the fueling station prior to fill nozzle connection.
Hydrogen Flow Control System	• **Engineering Design:** The fuel system should be designed to standard engineering practices until relevant SAE documents are available. • **Fail-Safe Design:** Means should be provided to prevent unwanted discharge of fuel from single-point failures of the shut-off system. • **Fault Monitoring:** Fuel system faults that may require monitoring include: fuel discharge fault; fuel shutoff fault; process fault; or ventilation fault.

System	Tests or Requirements
HP Flow Control Sub-System	• See Hydrogen Flow Control System
MP Flow Control Sub-System	• See Hydrogen Flow Control System
LP Flow Control Sub-System	• See Hydrogen Flow Control System
Fuel Cell System	• **High-Voltage Isolation Test -** System - Fuel cell system and all other high-and intermediate voltage circuits should have adequate isolation between its DC buss and other electrical circuits and the vehicle conductive structure (resistance >=125 ohms/V over range of environmental conditions; measure isolation resistance) • **High-Voltage Dielectric Withstand Capability** - System – High-voltage systems should demonstrate adequate dielectric strength so that there is not indication of a dielectric break-down or flashover after the application of a voltage. • **Engineering Design:** Standard engineering practice should be used for the design of subsystems or components containing hydrogen or hazardous fluids until relevant SAE standards are developed.
Fuel Cell Stack Sub-System	• **Safety Design:** Fuel cell stacks should be designed to prevent hazardous operating conditions including hazardous fluid leakage, overpressure, fire, and shock hazard. • **Isolation:** The fuel cell should have adequate isolation resistance between its DC buss and other electrical circuits and the vehicle conductive structure. • **Dielectric Withstand Capability:** For design validation, each high-voltage system should demonstrate adequate dielectric strength such that there is no indication of a dielectric breakdown or flashover. • **Fault Monitoring:** Some faults that may require monitoring to address potentially hazardous conditions include: Cell Stack or Process Fault, Ground Fault ; Low-Voltage Fault; Overcurrent Fault
Fuel Cell Cooling Sub-System	• See Fuel Cell System
Fuel Cell Air Supply Sub-System	• See Fuel Cell System
Electric Power Management, Control, & Propulsion System	• **Electrical Hazards Control:** The objective is to prevent inadvertent contact with hazardous voltages (if present in the FCV) or to prevent the development of an ignition source, or damage or injury from the uncontrolled release of electrical energy. • **Engineering Design:** Refer to SAE J2344; SAE J1742; SAE J1645; UL 2251; SAE J1772; SAE J1773 for guidance on the high-voltage components, wiring, and fusing. • **Electrical Safety:** The installation of electrical systems and equipment should follow safety guidelines in Section 4.4 of SAE J2578. • **Fault Monitoring:** Some electrical system faults that may require monitoring are: Ground Fault; Overcurrent • **High-Voltage Isolation:** Any high- or intermediate-voltage circuits of the completed vehicle not addressed within the fuel cell module should have adequate isolation resistance between it and the electrical chassis and between it and other electrical circuits. • **Dielectric Withstand Capacity:** For design validation, each high-voltage system should demonstrate adequate dielectric between the electrical circuits and the vehicle conductive structure such that there is no indication of a dielectric breakdown or flashover. • **Access to Live Parts:** An interlock, special fasteners, or other means should be provided on any cover whose removal provides access to live parts with hazardous voltage. If a Hazardous Voltage Interlock Loop is used for safety, such interlocks may be part of this monitoring loop. • **Bonding and Grounding:** If hazardous voltages are contained within a conductive exterior case or enclosure that may be exposed to human contact as installed in the vehicle, this case should be provided with a conductive connection to the vehicle chassis. - **Vehicle Bonding**: All body panels and components that part of the fill process should have an electrical connection to the vehicle conductive structure

System	Tests or Requirements
	- **Vehicle Interior Bonding:** Interior component materials should be selected that do no promote static discharges. - **Electrical Components Bonding**: Energy storage compartments (e.g., stack module, batteries) and major power electronics components should have their external conductive cases connected directly to the vehicle conductive structure (chassis) by a ground strap, wire, welded connection, or other suitable low-resistance mechanical connections. • **Hybrid Fuel Cell Vehicle:** Vehicles with fuel cells and batteries and/or capacitors should meet the following requirements: - A conductive connector mounted on the vehicle (inlet connector) should have safety features to prevent inadvertent contact with hazardous voltages - The vehicle manufacturer should provide the capability to monitor any circuits energized from premise wiring during charging, and, if the electrical isolation falls below operating limit in 4.4.3.2, the circuit should be de-energized. • **Back-Feed to Fuel Cell:** The fuel cell stack module should be protected from unintended back-feed of power from energy sources such as the traction battery pack and/or the regenerative system. • **Traction Battery Pack**: If the vehicle is equipped with a traction battery pack or other high-voltage batteries, the isolation of the battery from the vehicle conductive structure should comply with SAE J1766, Appendix A. • **Automatic Disconnects:** An automatic disconnect function should provide a means of electrically isolating both poles of a fuel cell stack module, traction battery, and other high-voltage sources from external circuitry or components. This function would be activated by either the main switch or as an automatic triggering protection. Refer to SAE J2344. • **Manual Disconnects:** A means should be provided to disconnect both poles or de-energize the fuel cell module, a traction battery, and other high-voltage sources from external circuitry or components. This function would be used for vehicle assembly, service, and maintenance operations. Refer to SAE J2344. • **Labeling:** Hazardous voltage equipment or compartments containing hazardous voltage equipment should be identified using the high-voltage symbol from IEC 60417.

According to the fuel cell standards Web site,* revisions to SAE J2578 are under consideration for re-issuing that include reviewing how hazardous discharges are addressed, determining if fuel is needed onboard for crash test to meet J1766 electrical standards, and harmonizing J2578 with J2579 that is still in draft form.

SAE J2579 (DRAFT) – Recommended Practice for Fuel Systems in Fuel Cell and Other Hydrogen Vehicles

Recommended Practice SAE J2579 is a draft performance standard that addresses systems for the storage and handling of hydrogen on-board vehicles. Handling includes processing (producing and chemically conditioning) and delivering (conditioning and conveying) hydrogen (or hydrogen-rich gas) to a fuel cell stack, internal combustion engine or other power-generation system. The fuel, associated process streams, and byproducts within these systems may present potential hazards. The purpose of this document is to provide guidance to minimize those hazards.

* http://www.fuelcellstandards.com/2.1.7.5.htm

This document identifies safety considerations to be used in the design and construction of these systems to minimize hazards in their operation and maintenance. This document also identifies performance criteria for hydrogen storage systems and the associated test protocols to verify that production hydrogen storage systems and design prototypes satisfy these performance criteria. Although RP J2579 covers all types of processing and delivery methods for FCVs, Table A-2 provides an overview of only those tests/requirements for systems associated with compressed-hydrogen FCVs.

The fuel cell standards Web site indicates that the first issue of this document will be as a Technical Information Report to validate test methods.

Table A-2. Overview of SAE J2579

System	Tests or Requirements
Vehicle	• **Safety Design:** Single point hardware or software failure should not result in an unreasonable risk to persons or uncontrolled behavior of the vehicle. The requirements are intended to minimize the likelihood of single point failures through design considerations, detection and management of faults, and identify and communicate faults that are to be managed by vehicle control systems. (use FMEA to recognize failure modes) • **Crashworthiness:** Vehicle-level requirements such as hydrogen permeation and post-crash leakage limits are specified in SAE J2578.
Hydrogen Fuel System	• **Hazard Management:** Manage exposure of humans to potentially hazardous materials; • **Fail-Safe Design:** An automatic means should be provided to prevent the unwanted discharge of fuel arising from single-point failures of the shutoff function. • **Management of Flammable Conditions:** The following items should be addressed: Purging when appropriate before the initiation of reaction; Air-to-fuel regulation as necessary during operation; Reactant shutoff, purging or passivation as necessary after shutdown; fault monitoring to ensure that the reaction remains within prescribed process limits throughout all operating modes; Possible formation of flammable mixtures due to failures in fuel containing systems; Potential formation of flammables outside the fuel system. • **Over-Pressure Protection:** The system should have adequate protection to prevent rupture in case of over-pressure due to system faults and externalities, e.g., fire. • **Thermal (Over-Temperature) Protection:** The design of fuel systems should consider over-temperature protection to prevent the unintended release of hazardous materials and the creation of unintended ignition sources. In event of fire, a hydrogen release should occur in a controlled manner. • **Fault Monitoring:** The fault monitoring should include any failure modes related to critical functionality and safety such as over-pressurization, over-temperature, and high leakage. The fuel system may include sensors and/or switches to provide fault detection to the customer. See SAE J2578 for guidance in implementing a staged warnings and shutdowns. • **Crashworthiness:** The system, mounting and installation should be designed to minimize the potential releases of hazardous materials resulting from a crash. • **Design - Service Life Conditions:** Must address pressure, temperature, fuel quality, shock and vibration, fatigue and wear-out. • **Design - Material Selection:** Components should be made of materials that are suitable for the vehicle service life with the range of process fluids and conditions expected during both normal operation and fault management. • **Design Qualification:** Components and systems should be designed and built to contain hydrogen under expected service conditions and perform safety-critical control functions over the projected life of the product. • **Code Compliance:** Pressurized components or systems may comply with applicable national or regional codes, standards, or directives for the design, fabrication, and verification of equipment as long as requirements are consistent with the general service defined in this recommended practice.

System	Tests or Requirements
	• **Performance Requirements for Hydrogen Systems:** To qualify the design and construction, systems should be fabricated and assembled in a manner representative of normal production and undergo the series of verification tests specified that simulate the condition of the system throughout its life, including both normal operation and some service-terminating events. - **Verification of Performance over Service Life:** Mechanical Damage, Chemical Exposure, Exposure to Thermal and Pressure Ranges, Exposure to Cycle Fatigue and Wear-Out , Compliance with SAE J2578 - **Service-Terminating Exposures** • **Production Validation - Process and Quality:** Must address Quality Control Systems, Process Verification, Routine Production Tests (per unit), Production Lot Tests (Batch Tests) • **System and Vehicle Integration:** SAE J2578 Specifications, Labels, Installation and Mounting, Fill and Discharge Systems, Owner Guide or Manual, Emergency Response, Maintenance, Service Life Limitations • **Regulatory Approval:** Approval should be obtained in accordance with the relevant regulations of the government entity with jurisdiction where the systems and vehicles are to be used. In the USA, see 49 CFR 571 for Federal Motor Vehicle Safety Standards.
Hydrogen Storage Sub-System	• **Fail-Safe Design:** Must have automatic hydrogen shut-off via fail-safe devices when signaled by the vehicle safety system and when the propulsion system is not active. This device should be as close to the outlet point of the container as possible; operation is verified by SAE J2578. • **Over-pressure Protection:** Must have over-pressure protection from an extreme temperature increase (in the presence of fire), and over-pressurization from a fueling station malfunction. With regard to fire, containers should be protected by thermally activated pressure-relief devices. • **Design Qualification & Verification Tests:** Should be performed on the complete storage system: Chemical Exposure and Surface Damage; Extended Pressure Exposure (Accelerated Stress Rupture); Pressure Cycling – Ambient and Extreme Temperature; Extreme Pressure Exposure; Penetration; End of Life Permeation; Engulfing Fire (Bonfire Test); Localized Fire; Burst Test; Design Re-Qualification Process; Compliance to J2578; Production QC Tests (leak, proof pressure, dimension check, NDE). • **Production Quality Control Tests:** TBD; Equipment not covered by container production test requirements should be validated for the performance requirements with the following modifications: Routine leak test at NWP; Routine proof pressure tests to 1.5 times NWP; Dimension checks during the proof pressure test; and NDE examination to verify that flaw sizes are below the manufacturer's specifications. • **Installation:** Hydrogen storage systems must be installed in accordance with SAE J2578 or equivalent. • **Inspection after Damage:** Containers involved in collisions, accidents, fires or other events that cause damage should be subjected to inspection procedures provided in CGA pamphlet C-6.4. • **Service & Repair:** Service and repair should follow manufacturer guidelines; no storage system at the end of its useful life (number of refuelings) or with impact/other damage should be returned to service. • **Labels:** Labels indicating the date of manufacture, manufacturer and parameters of storage characterization (i.e., compressed pressure ratings) should be affixed. • **Handling:** Hydrogen storage systems installed during retail service should have been qualified for survival of harsh handling or else meet the manufacturer requirements for monitoring all handling conditions (such as a brittle coating or shock sensor) to indicate when the system has been handled harshly and is not qualified for installation in a vehicle.
Hydrogen De-Fueling Sub-System	• **Fueling/De-Fueling:** The ability to de-fuel as well as fuel the vehicle should be provided following guidance in SAE J2578. • **De-Fueling Procedures:** The supplier of the compressed gas fuel system should also provide for the ability to properly de-fuel including procedures per SAE J2578 (depressurization and purging). De-fueling is limited to safe disposal of the contents of the system, either to atmosphere, to absorbents, or to a container. • **Safety Design:** Considerations must be given in the design to allow safe and effective fueling and de-fueling.

System	Tests or Requirements
Hydrogen Fueling Sub-System	• **Fueling/De-Fueling:** The ability to de-fuel as well as fuel the vehicle should be provided following guidance in SAE J2578. • **Safety Design:** Considerations must be given in the design to allow safe and effective fueling and de-fueling. • **Fueling Procedure:** The system (including all equipment used for filling: connectors, hoses, etc.) must always be purged with an inert gas prior to filling. Specific care is required to ensure that containers and high-pressure systems are properly purged with an inert gas prior to fill with hydrogen (or any other compressed fuel) to preclude the formation of flammable mixtures within the system. • **Unique Fueling Connection:** A unique connection configuration is required to prevent products other than hydrogen from being filled into the system. • **Receptacle:** The receptacle for the compressed gas hydrogen fuel system on the vehicle should comply with SAE J2600. • **Check Valve:** The fuel system should utilize a check valve or other feature to prevent back-flow of hydrogen, resulting in an unwanted discharge to ambient. (6.2.9) • **Service Life Design:** The system must be designed to withstand at least twice the anticipated filling cycles
Hydrogen Flow Control System	• See Hydrogen Fuel System
HP Flow Control Sub-System	• See Hydrogen Fuel System
MP Flow Control Sub-System	• See Hydrogen Fuel System
LP Flow Control Sub-System	• See Hydrogen Fuel System
Fuel Cell System	• Not Addressed
Fuel Cell Stack Sub-System	• Not Addressed
Fuel Cell Cooling Sub-System	• Not Addressed
Fuel Cell Air Supply Sub-System	• Not Addressed
Electric Power Management, Control, & Propulsion System	• **Electrical System Safety:** The installation of electrical systems and equipment should follow safety guidelines in SAE J2578.

ISO SAFETY SPECIFICATIONS

The International Organization for Standardization is the world's largest developer of standards. ISO standards are developed by technical committees comprised of experts from the industrial, technical and business sectors that have asked for the standards, and that subsequently put them to use. The ISO standards for fuel cell vehicles are developed under the Road Vehicles Technical Committee (TC 22) by the Electrically Propelled Road Vehicles Sub-Committee (SC 21). In particular, this subcommittee has developed the safety specifications for fuel cell road vehicles in Parts 1, 2, and 3 of ISO 23273. Part 1 is related to vehicle functional safety, Part 2 is related to protection against hydrogen hazards for vehicles fueled with compressed hydrogen, and Part 3 is related to protection of persons against electric shock. Each standard is discussed in more detail below.

ISO 23273-1:2006(E) – Fuel Cell Road Vehicles -- Safety Specifications -- Part 1: Vehicle Functional Safety

Part 1 of ISO 23273 was published in May 2006 and specifies the essential requirements for the functional safety of fuel cells with respect to hazards to persons and the environment inside and outside of the vehicle caused by the operational characteristics of the fuel cell power systems. ISO 23273-1:2006 does not apply to manufacturing, maintenance or repair of the vehicles.

The requirements in ISO 23273-1:2006 address both normal operating (fault-free) condition and single fault conditions of systems and components over the range of environmental and operational conditions for which the vehicle is designed to operate, as identified by using appropriate hazard analysis tools.

ISO 23273-1:2006 applies only when the maximum working voltage of the on-board electrical circuits is lower than 1,000 V a.c. or 1,500 V d.c. according to national or international standards and/or legal requirements. Table A-3 provides an overview of the tests or requirements for general vehicle safety.

Table A-3. Overview of ISO 23273-1:2006

System	Tests or Requirements
Vehicle	• **Crashworthiness:** Crashworthiness requirements for the FCV shall meet applicable national or International Standards and legal requirements. • **Safety Design:** Safety measures shall be provided to reduce hazards for persons caused by single-point hardware or software failures in systems and components as identified in appropriate hazard analyses (FMEA, FTA, or other). • **Vehicle Operation:** A main switch function should be provided so that the operator can disconnect traction power sources and shut off the fuel supply, similar to a conventional ignition switch. For the power on procedure at least two distinctive and deliberate actions must be performed to go from power off to driving enabled while only one is necessary to go from driving enabled to power off. • **Fail-Safe Design:** The design of systems and components specific to the FCV shall consider fail-safe design for electric and hazardous fluid system controls. Electric circuits shall open and fuel shutoffs shall close to isolate electrical and fuel sources of the fuel cell power system. • **Electromagnetic Tolerance:** All electric assemblies on the FCV, which could affect safe operation of the vehicle, shall be functionally tolerant of the electromagnetic environment to which the vehicle will normally be exposed.

System	Tests or Requirements
	• **Design Requirements:** The requirements shall be met over the range of environmental and operating conditions for which the vehicle is designed to operate. • **Driver Notifications:** The driver should be notified when the fuel cell is ready for driving as well as in the event of significant reductions in power if the fuel cell is equipped to automatically reduce propulsion power. • **Safe Shutdown:** The safety measures shall include the ability to perform shutdowns safely when faults are detected that could lead to hazardous conditions. • **Reverse Driving:** If driving backward is achieved by reversing the rotational direction of the electric motor the following requirements shall be met - switching direction shall require two separate actions by the driver or, if only one action is required, the usage of a safety device that allows the transition only when the vehicle does not move or moves slowly. • **Labels, Manuals, and Safety Info:** - Refer to SAE J2578 for owner's manual, marking, and emergency response.
Hydrogen Fuel System	• Refer to ISO 23273-2:2006
Hydrogen Storage Sub-System	• Refer to ISO 23273-2:2006
Hydrogen De-Fueling Sub-System	• Refer to ISO 23273-2:2006
Hydrogen Fueling Sub-System	• Refer to ISO 23273-2:2006
Hydrogen Flow Control System	• Refer to ISO 23273-2:2006
HP Flow Control Sub-System	• Refer to ISO 23273-2:2006
MP Flow Control Sub-System	• Refer to ISO 23273-2:2006
LP Flow Control Sub-System	• Refer to ISO 23273-2:2006
Fuel Cell System	• Not Addressed
Fuel Cell Stack Sub-System	• Not Addressed
Fuel Cell Cooling Sub-System	• Not Addressed
Fuel Cell Air Supply Sub-System	• Not Addressed
Electric Power Management, Control, & Propulsion System	• Refer to ISO/DIS 23273-3

ISO 23273-2:2006 - Fuel Cell Road Vehicles -- Safety Specifications -- Part 2: Protection Against Hydrogen Hazards For Vehicles Fueled With Compressed Hydrogen

ISO 23273-2:2006, published in May 2006, specifies the essential requirements for fuel cell vehicles (FCV) with respect to the protection of persons and the environment inside and outside the vehicle against hydrogen related hazards. ISO 23273-2 applies only to FCVs where compressed hydrogen is used as the fuel and does not apply to manufacturing, maintenance, and repair.

ISO 23273-2:2006 requires that components are designed, installed, and serviced so that they can operate safely under the environmental and operating conditions specified by the manufacturer. In addition, the high, medium, and low-pressure components are to have adequate pressure ratings and are to be electrically grounded if exposed to potential flammable areas to prevent inadvertent ignition of hydrogen discharges. Table A-4 provides an overview of the tests or requirements for the hydrogen storage and supply systems covered in the FMEA.

Table A-4. Overview of ISO 23273-2:2006

System	Tests or Requirements
Vehicle	• **Normal Discharge Tests**: - Vehicle - Tests shall be performed according to applicable national or international standards or legal requirements. If none exist, test methods shall be specified by the vehicle manufacturer. Tests shall be run over all normal operating modes and in all normal areas of vehicle use (start, run, stop, and off [parked]). - Passenger Compartment, Other Compartments, Parking in Non-mechanically Ventilated Enclosures, and Operation in Ventilated Structures: Test Methods for Determining Flammability Around the Vehicle from Fuel Discharges • **Hydrogen Hazards Tests**: - Vehicle - A combination of analyses and tests can be used to prove that any hydrogen emissions under all normal and applicable first-failure modes are below hazardous levels for persons. • **Design Requirements:** The requirements shall be met across the range of environmental and operational conditions for which the vehicle is designed to operate. • **Safety Design:** A hydrogen hazard analysis shall be performed considering primarily the interface between the components and systems, as established during assembly into the vehicle. An FMEA, an FTA, or another appropriate method may be used, and shall determine potential single hardware and software failures or conditions that could form a hazard for persons in or around the vehicle. Based on this analysis, a description shall be provided of the hardware and software measures enacted to prevent or limit failures or conditions to non-hazardous levels for persons. • **Alternative Designs:** The vehicle manufacturer shall define and perform an appropriate combination of necessary analyses and tests to sufficiently demonstrate that the alternative concept provides protection against potential hazards that is equivalent to this standard. • Refer to ISO 23273-1:2006
Hydrogen Fuel System	• **Fail-Safe Design:** Fuel system should be equipped with a fire protection system with one or more temperature-triggered PRDs, a main hydrogen shut-off valve that shall be closed when energizing power to the valve is lost and when the fuel cell system is not operating, a hydrogen shut-off system, and an excess flow valve or system with the same function.
Hydrogen Storage Sub-System	• **Over-Pressure Protection:** The fuel container system shall be equipped with one or more temperature-triggered PRDs. • **PRD Discharge:** Discharges from the PRD shall be vented to the outside of the vehicle and shall be protected as well as all associated piping and outlet, such that functionality is not compromised due to flow restrictions.
Hydrogen De-Fueling Sub-System	• See Hydrogen Fuel System
Hydrogen Fueling Sub-System	• **Electrostatic Discharge**: Measures against electrostatic discharges of the vehicle at the receptacle should be taken. • **Fueling Safety:** Vehicle movement by its own propulsion system should be prevented when the vehicle is being refueled. (See also J2578) • **Nozzle & Receptacle:** See ISO 17268 for nozzle and receptacle requirements. Nozzle and receptacle shall be provided with a cap to prevent invasion of dust, liquid, contaminants, etc. • **Fueling Location:** The fueling location on the vehicle shall be designed so as to prevent the accumulation of flammable gases and the ingress of foreign material. It shall be placed in an appropriate position to ensure safe operation. The side of the vehicle is preferable.
Hydrogen Flow Control System	• **PRD Discharge:** Discharges from the PRD shall be vented to the outside of the vehicle and shall be protected as well as all associated piping and outlet, such that functionality is not compromised due to flow restrictions.
HP Flow Control Sub-System	• See Hydrogen Flow Control System
MP Flow Control Sub-System	• See Hydrogen Flow Control System
LP Flow Control Sub-System	• See Hydrogen Flow Control System

System	Tests or Requirements
Fuel Cell System	• Not Addressed
Fuel Cell Stack Sub-System	• Not Addressed
Fuel Cell Cooling Sub-System	• Not Addressed
Fuel Cell Air Supply Sub-System	• Not Addressed
Electric Power Management, Control, & Propulsion System	• Refer to ISO/DIS 23273-3

ISO/DIS 23273-3 – Fuel Cell Road Vehicles -- Safety Specifications -- Part 3: Protection of Persons Against Electric Shock

Part 3 of ISO 23273 specifies the requirements of FCV for the protection of persons and the environment inside and outside the vehicle against electric shock. This part applies only to on-board electric circuits with working voltages between 25 V a.c. and 1,000 V a.c., or 60 V d.c. and 1,500 V d.c. respectively. This standard does not apply to FCV connected to an external electric power supply; component protection; or manufacturing, maintenance and repair.

Although this is currently a Draft International Standard (DIS), a recent vote on the DIS received only editorial comments and therefore will proceed to publication (according to the fuel cell standards Web site). Table A-5 provides an overview of the tests or requirements for the protection of people against electric shock.

Table A-5. Overview of ISO/DIS 23273-3

System	Tests or Requirements
Vehicle	• **Insulation Resistance Test**: - System/Vehicle - Measure resistance between electrical system and chassis. System/Vehicle is pre-conditioned at one ambient and tested at a 2nd ambient, such that the test covers a time in which condensation is likely to occur. • **Barrier/Enclosure Continuity Test** - Component/Vehicle - Test for minimal resistance between barrier/enclosure and chassis.
Hydrogen Fuel System	• Refer to ISO 23273-2:2006
Hydrogen Storage Sub-System	• Refer to ISO 23273-2:2006
Hydrogen De-Fueling Sub-System	• Refer to ISO 23273-2:2006
Hydrogen Fueling Sub-System	• Refer to ISO 23273-2:2006
Hydrogen Flow Control System	• Refer to ISO 23273-2:2006
HP Flow Control Sub-System	• Refer to ISO 23273-2:2006
MP Flow Control Sub-System	• Refer to ISO 23273-2:2006
LP Flow Control Sub-System	• Refer to ISO 23273-2:2006

System	Tests or Requirements
Fuel Cell System	• **High-Voltage Isolation Test** - Component (harnesses, bus bars, connectors) - Test for dielectric breakdown or flashover between the component under test and the chassis.
Fuel Cell Stack Sub-System	• See Electric Power Management, Control, & Propulsion System
Fuel Cell Cooling Sub-System	• See Electric Power Management, Control, & Propulsion System
Fuel Cell Air Supply Sub-System	• See Electric Power Management, Control, & Propulsion System
Electric Power Management, Control, & Propulsion System	• **Basic Protection Measures:** General/Test Methods and Requirements for the Protection Measures Against Electric Shock; shall be performed on each voltage class B electrical circuit of the vehicle. • **Protection Against Direct Contact:** Persons shall be protected against direct contact with the live parts of any Class B electrical circuit through basic insulation of live parts and/or barriers/enclosures preventing access to the live parts. • **Wire Marking:** Identification of Class B Wiring • **Electrical Hazards:** The vehicle manufacturer shall conduct an appropriate hazard analysis in respect to electric shock and establish a minimum set of measures that give sufficient protection against electric shock (FMEA, FTA, or other) and shall consider normal (fault free) and first failure conditions. The analysis should consider both normal operational and environmental conditions as well as specific conditions such as exposure to water. • **Bonding and Grounding:** Exposed conductive parts including exposed conductive barriers/enclosures shall be connected to the electric chassis (for potential equalization). • **Insulation General:** If protection is provided by insulation, the live parts of the electrical system shall be totally encapsulated by insulation that can be removed only by destruction; suitable to the maximum working voltage and temperature ratings of the FCV and its systems; and sufficient insulation resistance, if required, and withstand a voltage test. • **Voltage Withstand Capability:** The voltage class B systems shall be designed according to IEC 60664 or a voltage withstand test shall be performed to demonstrate the adequacy of the protection measures to isolate live parts under normal conditions for harness, bus bars, and connectors. • **Electric Equipment Marking**: A symbol according to IEC 60417 and ISO 3864 shall appear near class B voltage sources and shall be visible on barriers, enclosures, and insulation that provide protection against direct contact under normal fault-free conditions.

CSA Draft Standards

Two draft CSA standards were reviewed for this project; the first standard relates to design requirements and tests for compressed-hydrogen gas vehicle fuel containers (HGV2) and the second standard relates to design requirements and tests for PRDs used on the fuel containers (HPRD1).

CSA HGV2 Fuel Containers (DRAFT) Compressed-Hydrogen Gas Vehicle (HGV) Fuel Containers

This draft standard contains requirements for the material, design, manufacture, and testing of serially produced, refillable Type HGV2 containers intended only for the storage of compressed hydrogen for vehicle operation. These containers are to be permanently attached to the vehicle. Type HGV2 containers shall not be over 1,000 liters (35.4 cu ft) water capacity.

The committee is currently working with OEM's and tank manufacturers, reviewing ISO requirements on compressed-hydrogen fuel containers, and working with an ASME Steering Committee on issues of possible hydrogen embrittlement. Issue of the HGV2 is targeted for July 2007. Table A-6 provides an overview of the tests or requirements for the compressed-hydrogen fuel container.

Table A-6. Overview of CSA HGV2

System	Tests or Requirements
Vehicle	• Not addressed
Hydrogen Fuel System	• See Hydrogen Storage Sub-system
Hydrogen Storage Sub-System	• **Container Design Qualification Tests**: Component - Bonfire test; environmental test (type 2, 3, & 4); Charpy impact test for steel; tensile test for metal; sustained load cracking (SLC) and corrosion tests for aluminum; shear strength for composites; UV for composites; ambient cycling; hydrostatic burst; hydrostatic pressure test; hydraulic pressure cycle; pressure hold; gas pressure cycle (type 4); temperature cycling; leak before break (type 1 & 2); leak test (type 4); permeation test (type 4); composite flaw tolerance (type 2, 3, & 4); penetration test (type 2, 3, & 4); drop test (type 2, 3, & 4). • **QA Verification:** Component - shall pass all relevant qualification tests prior to shipping; NDE verification flaws in metallic containers within limits; Visual/NDE verification non-metallic liners are free of flaws exceeding limits; Verification that the critical dimensions and parameters are within design tolerances; Verification of compliance with specified surface finish; Verification of coating quality (if required); Verification of markings; and Verification of strength (heat treatment) of metal containers, liners and bosses; for Type 1 containers, a hardness test or equivalent is required. • **Container Protection:** The installer shall be responsible for the protection of container valves, pressure relief devices, and connections as required by SAE J2578; factors to consider include the ability of the container to support the transferred impact loads and the effect of local stiffening on container stresses and fatigue life; Containers shall be protected from accidental cargo spillage and from mechanical damage. This standard contains no requirements for container integrity in a vehicle collision. Container locations and mountings should be designed to provide adequate impact protection to prevent container failure in a collision. • **Container Design:** Containers must meet the appropriate design standards for the type of container, service pressure, and compatibility; container must be equipped with a PRD. • **Quality Assurance:** QA of the container must be performed.
Hydrogen De-Fueling Sub-System	• Not addressed
Hydrogen Fueling Sub-System	• Not addressed

System	Tests or Requirements
Hydrogen Flow Control System	• Not addressed
HP Flow Control Sub-System	• Not addressed
MP Flow Control Sub-System	• Not addressed
LP Flow Control Sub-System	• Not addressed
Fuel Cell System	• Not addressed
Fuel Cell Stack Sub-System	• Not addressed
Fuel Cell Cooling Sub-System	• Not addressed
Fuel Cell Air Supply Sub-System	• Not addressed
Electric Power Management, Control, & Propulsion System	• Not addressed

CSA HPRD1 Pressure Relief Devices for Compressed-Hydrogen Vehicle Fuel Containers (DRAFT)

This draft standard contains requirements for the material, design, manufacture and testing of PRDs for use with the fuel containers described in CSA HGV2. This standard only applies to thermally activated pressure relief devices and does not apply to pressure relief valves that reseat or reseal themselves after activation due to overpressure.

The PRD1/HPRD1 Technical Advisory Group has developed a draft standard based on the existing PRD1 standard. Revisions to the document have been approved by both the Automotive Technical Committee and ANSI. The draft document will be printed by the end of April 2007 and will be available to participants through the committee forums. Issue of the standard is targeted for July 2007. Table A-7 provides an overview of the tests or requirements for the thermally activated PRD.

Table A-7. Overview of CSA HPRD1

System	Tests or Requirements
Vehicle	• Not addressed
Hydrogen Fuel System	• Not addressed
Hydrogen Storage Sub-System	• **PRD Construction Requirements:** Shall be in accordance with concepts of safety, performance, and durability. • **PRD Service Conditions (4.0):** Service life (4.2), pressure (4.4), specified by manufacturer; meet or exceed life of container it's protecting. Minimum design cycle life shall be 20,000 pressure cycles to 125% of service pressure (4.5). Maintain pressure integrity from -40°F to 185°F. PRD designed to comply with fuel meeting SAE J2719 and/or ISO 14687 (4.7) and external environmental factors (4.8). • **PRD Quality Assurance (5.0):** Quality systems shall be in accordance with Approved Quality System (AQS) like ISO 9001 and 9002 (5.2). Manufacturer shall use a nationally recognized

System	Tests or Requirements
	independent inspector to inspect, review, and sign-off on quality system (5.3). • **PRD Materials:** PRD materials in contact with H2 shall be acceptable for this type of service (focus on embrittlement & contamination of the fuel) without change in function and no harmful deformation or deterioration when exposed (6.1). • **PRD Design Requirements:** Once activated the device will fully vent contents of container and minimize potential external hazards from activation (projectiles) (6.2) • **PRD Rework & Repair:** non-compliant PRDs can be reworked/repaired as long as retested to demonstrate comply with requirements. • **PRD FMEA:** Shall perform an FMEA and make documents available to manufacturer. • **PRD Design Qualification Testing:** Conducted on finished PRD (7.1); pressure cycling (7.4); long term creep (7.5); thermal cycling (7.6); salt corrosion resistance (7.7); H2 compatibility (7.8); SCC resistance (7.9); impact due to drop & vibration (7.10); leakage (7.11); bench top activation (7.12); flow capacity (7.13); • **PRD Inspection & Acceptance Testing:** Must inspect all system critical components identified in the FMEA before assembly or shipping (7.3); leak testing (7.4). • **PRD Production Batch Testing:** Must batch test all system critical components identified in FMEA (9.1); fusible material yield temperature (9.3); rupture disk device rupture pressure (9.4); pressure relief device components (9.5); thermally activated pressure relief devices & parallel combination relief devices (9.6); series combination relief devices (9.7) • **PRD Marking (10):** Shall have permanent markings with name, year of this standard, manuf. service pressure, ID, part number, & traceability code; include arrows to show direction of flow if ambiguous. • **PRD Reuse (6.5):** PRDs that have been in service can not be reused in another container.
Hydrogen De-Fueling Sub-System	• Not addressed
Hydrogen Fueling Sub-System	• Not addressed
Hydrogen Flow Control System	• Not addressed
HP Flow Control Sub-System	• Not addressed
MP Flow Control Sub-System	• Not addressed
LP Flow Control Sub-System	• Not addressed
Fuel Cell System	• Not addressed
Fuel Cell Stack Sub-System	• Not addressed
Fuel Cell Cooling Sub-System	• Not addressed
Fuel Cell Air Supply Sub-System	• Not addressed
Electric Power Management, Control, & Propulsion System	• Not addressed

JAPANESE HFCV STANDARD

The Japanese HFCV technical standards are more prescriptive in nature and apply to the fuel tanks and fuel lines (gas containers, piping, and other devices fueled by compressed hydrogen gas) of ordinary-sized passenger vehicles. Specifically excluded are vehicles with a passenger capacity of 11 or more, vehicles with a gross weight of more than 2.8 tons, motorcycles, and mini-sized vehicles with caterpillar tracks and sleds. Three main Japanese Safety Standards were reviewed for this project including:

- Attachment 17: Technical Standard for Fuel Leakage in Collisions, etc.
- Attachment 100: Technical Standard for Fuel Systems of Motor Vehicles Fueled by Compressed Hydrogen Gas
- Attachment 101: Technical Standard for Protection of Occupants Against High Voltage in Fuel Cell Vehicles

Table A-8 provides an overview of the tests or requirements for each system and sub-system covered in the FMEA.

Table A-8. Overview of Japanese HFCV Standards

System	Tests or Requirements

Vehicle	• **Hydrogen Gas Leakage Detection Test**: Component/Vehicle - Test to ensure that the sensor actuates a warning and shuts off the supply of gas upon detection of hydrogen gas.
	• **Protection Against Direct Contact Test:** Vehicle - Test to ensure any live components can not be contacted (through insulation, barriers, enclosures, etc.) using a specified probe.
	• **Protection Against Indirect Contact Test:** Vehicle - Test to ensure continuity between barriers and enclosures and chassis.
	• **Vehicle Marking:** Barriers and enclosures installed for protection against direct contact shall be marked according to this standard. This provision shall not apply to barriers and enclosures that are not accessible, unless the parts are removed by means of tools or the motor vehicle is lifted by means of a jack.
	• **Ventilation of Hydrogen:** Vehicle - Ventilation shall be provided to discharge leaked hydrogen and not directly emit into passenger or luggage compartments, tire housing, exposed electrical terminals or switches, or other ignition sources.
	• **Gas Tight Housing**: Vehicle - No gas leakage shall be present (helium or carbon dioxide as test gases).
	• **Fuel Releases during Normal Operation:** Purged gas in excess of 4% hydrogen shall not be discharged or leak to the atmosphere.
	• **Hydrogen Leak Detection:** At least one detector of hydrogen gas leakage shall be installed at an appropriate position; does not apply when components are installed in a space that is sufficiently upward or when the gas leaked from components will be led to the atmosphere and with a leakage detector installed on an appropriate position of its passage.
	  - A device shall be installed that shuts off the supply of hydrogen gas when the leakage detector detects hydrogen leakage.
	  - A warning device shall be located at a position readily recognizable by the driver. Additionally a device shall give a warning to the driver at the driver's seat when an open wire or short circuit takes place in the leakage detector.
	  - The gas leakage detector shall be subjected "Test for Hydrogen Gas Leakage Detector"

Hydrogen Fuel System	• **Pressure Indicator:** The driver's seat shall be provided with a pressure gauge indicating the pressure at the primary side of the first pressure-reducing valve, or a residual amount meter indicating the residual amount of hydrogen gas. • **Fuel Leakage in Collision:** System - Frontal-collision and rear-end collision tests for fuel leakage after a collision. Fuel leakage in a lateral collision; fuel used in tests should be helium.

System	Tests or Requirements
	• **Vibration Resistance:** System/Component - Gas container and piping shall have proven resistance to vibration as specified. • **Installation:** Gas containers, piping, etc. shall not be such that they are removed for filling; shall not be located in the passenger or luggage compartments, or other places with insufficient ventilation unless housed in gas tight housing; shall be securely installed to prevent shifting or damage while traveling - sections liable to damage shall be protected by covering; if affected by the exhaust shall be protected by appropriate heat insulating measures; components exposed to direct sunlight shall be provided with adequate cover. • **Overpressure Protection:** A safety device that can prevent a significant pressure rise shall be provided at the secondary side of the pressure-reducing valve (not required if all secondary side components have pressure-resistant performance at the primary side) 1) a pressure relief device 2) pressure detector and shut-down of primary side hydrogen; PRD shall not vent directly into the passenger or luggage compartment, tire housing, exposed electrical terminals, exposed electrical switches, other ignition sources, other gas containers, or the front of the vehicle.
Hydrogen Storage Sub-System	• **Container Attachments:** The part attaching the gas container where it is filled must not be torn by acceleration toward the moving direction. All other container attachments must not be torn from the container when it is filled with hydrogen at the general use pressure and subjected to the prescribed accelerations toward the horizontal direction perpendicular to the direction of motion; compliance may be proven by calculation. • **Overfill Prevention:** Shall provide any of these devices to prevent overfill (overfill protection device, system to measure container pressure and a main stop valve that detects abnormal pressure drop, system to measure flow rate and a main stop valve that detects abnormal rise in flow rate). • **Container Removal:** Container shall not be such that it is removed for filling the hydrogen gas. • **Container Location:** Container shall be installed so that the horizontal distance from the front end is not < 420mm and 300mm from the rear; container attachments shall not be installed at a distance < 200 mm from the vehicle's external end in proximity (excluding rear).
Hydrogen De-Fueling Sub-System	• See Hydrogen Fuel System
Hydrogen Fueling Sub-System	• **Filling Port Integrity**: System/Component - Gas filling port must not be torn from the container under the specified accelerations (both longitudinal and lateral). May be proven through calculation. • **Check Valve:** A check valve shall be capable of preventing reverse flow at pressures ranging from the general-use pressure to the minimum pressure normally used. • **Overflow Prevention:** Shall be provided with a gas filling valve having an overflow prevention device. • **Installation:** Shall be installed where filling can be easily performed (not in the passenger or luggage compartments or location with insufficient ventilation); 200 mm away from exposed electric terminals, switches, or other ignition sources.
Hydrogen Flow Control System	• **Fuel Leakage in Collision:** System - Frontal-collision and rear-end collision tests for fuel leakage after a collision. Fuel leakage in a lateral collision; fuel used in tests should be helium. • **Vibration Resistance:** System/Component - Gas container and piping shall have proven resistance to vibration as specified. • **Installation:** Gas containers, piping, etc. shall not be such that they are removed for filling; shall not be located in the passenger or luggage compartments, or other places with insufficient ventilation unless housed in gas tight housing; shall be securely installed to prevent shifting or damage while traveling - sections liable to damage shall be protected by covering; if affected by the exhaust shall be protected by appropriate heat insulating measures; components exposed to direct sunlight shall be provided with adequate cover. • **Overpressure Protection:** A safety device that can prevent a significant pressure rise shall be provided at the secondary side of the pressure-reducing valve (not required if all secondary side components have pressure-resistant performance at the primary side) 1) a pressure relief device 2) pressure detector and shut-down of primary side hydrogen; PRD shall not vent directly into the passenger or luggage compartment, tire housing, exposed electrical terminals, exposed electrical switches, other ignition sources, other gas containers, or the front of the vehicle. • **Main Stop Valve:** The main stop valve shall be operable at the driver's seat. It must operate without fail. It shall be operated electromagnetically and normally closed when the power source fails. • **Pressure Regulation:** Pressure reducing valve shall not be place upstream of the main stop valve; does not apply where shut-off function is at the passage from the pressure reducing valve to the atmosphere or where there is no passage leading the atmosphere.

System	Tests or Requirements
	• **Air tightness of Housing**: Component - For gas lines in passenger, luggage, or insufficiently ventilated compartments, test gas line for air tightness and the air tightness of the compartment, and the ventilation of an opened compartment. • **Air tightness of Piping**: Component/System - All piping, etc. shall be airtight under general use pressure. High-pressure portions shall be airtight to 1.5 times the general use pressure, taking into account embrittlement due to hydrogen. • **Piping Removal:** Piping shall not be such that it is removed for filling the hydrogen gas. • **Piping Supports:** Metal piping supports shall not be in direct contact with the piping, except where the piping is welded to the support structure. • **Piping Installation:** Gas piping secured at both ends shall have an appropriate bend at its midpoint and supported at 1 m or less intervals.
HP Flow Control Sub-System	• See Hydrogen Flow Control System
MP Flow Control Sub-System	• See Hydrogen Flow Control System
LP Flow Control Sub-System	• See Hydrogen Flow Control System
Fuel Cell System	• See Vehicle and Electric Power Management System
Fuel Cell Stack Sub-System	• **Purge:** System - Measure the hydrogen gas concentration at the fuel cell purge line during operation and shutdown. Cannot be above 4%. • See Vehicle and Electric Power Management System
Fuel Cell Cooling Sub-System	• **Protection against Electrical Shock Due to Fuel Cell Stack Refrigerant**: System/Vehicle - Similar tests to "Direct Contact" and "Indirect Contact", treating any components that touch fuel cell stack refrigerant as an electrically "live" fluid.
Fuel Cell Air Supply Sub-System	• Not Addressed
Electric Power Management, Control, & Propulsion System	• **Insulation Resistance:** Component/System - Test for insulation resistance between energized components and the chassis. Alternatively a system that monitors for a drop in insulation resistance can be tested. The insulation resistance can be measured for the whole vehicle or by dividing according to each part/component and then using these measurements to calculate the insulation resistance of the entire vehicle. • **Power Supply Cutoff**: System - Test for confirmation of function of a switch to shut-off power when an electrical leakage is detected. • **Function Confirmation Method of Power Supply Shut-off at Time of Electric Leakage:** The time elapsed between the electric current leakage and shut-off shall be measured. The leakage current can be caused by a resistor installed between the component and the electrical chassis or a pseudo signal input to the sensor.

EUROPEAN WORKING GROUP

WP.29 Draft Standard for Compressed Gaseous Hydrogen

To enhance the safety of hydrogen vehicles, and to facilitate the approval of hydrogen vehicles, the European Integrated Hydrogen Project was established. A main objective of the EIHP was the development of draft standards for the use of hydrogen as a vehicle fuel. The EIHP aimed at creating the basis for the harmonization of European regulations for the use of hydrogen in road vehicles and procedures for periodic vehicle inspections. The work was based on a dual strategy: analysis of existing hydrogen related legislation in Europe, Japan, and the United States, and analyses of existing hydrogen vehicles and infrastructure in Europe complemented by safety studies.[*]

This draft standard was prepared by the United Economic Commission for Europe's Working Party, WP-.29 GRPE Informal Group for Hydrogen Fuel Cell Vehicles. The standard sets forth uniform provisions for the approval of specific components of motor vehicles using gaseous hydrogen and the vehicle with regard to the installation of those components. Table A-9 provides an overview of the tests or requirements for each fuel storage and supply systems covered in the FMEA.

Table A-9. Overview of European Standard WP.29

System	Tests or Requirements
Vehicle	• **Vehicle Ventilation:** The ventilating or heating system for a passenger compartment shall be kept separate from places where leakage or accumulation of hydrogen is possible so that hydrogen is not drawn into the vehicle compartment. • **Hydrogen Accumulation:** In the event of hydrogen leaking or venting, hydrogen shall not be allowed to accumulate in enclosed or semi-enclosed spaces. • **Hydrogen Sensors**: Component - Endurance test (same as that of the component on which it is installed). • **Gas Tight Housing:** Vehicle - No gas leakage (bubbles) shall be present for 3 minutes in test; no permanent deformation; vented to the atmosphere at the highest point of the housing but not into the wheel arch or aimed at a heat source (exhaust) and must not enter inside the vehicle; electrical connections and components shall be constructed so that no sparks are generated. • **Fail-Safe Design:** Safety instrumented systems shall be fail-safe or redundant (if fail-safe or self-monitoring electronic systems; must meet special requirements) • **Component Design & Tests:** The hydrogen components shall function safely and correctly as specified over the entire range of mechanical, thermal, and chemical service conditions without leaking or visibly deforming. Tests include: Hydrogen compatibility test, ageing test, ozone compatibility test, corrosion resistance test, endurance test, hydraulic pressure cycle test, internal leakage test, and external leakage test. Applicable tests for each component (and material) are specified; The effects on the external surfaces of the hydrogen components in their installed position shall be considered in relation to water, salt, UV, radiation, gravel impact, solvents, acids, alkalis, fertilizers, automotive fluids, and exhaust gases. • **Component Installation:** Installation of components shall be such they are within the outline of the vehicle or else adequately protected if outside the protective structure; the system, including PRD vents shall be installed so they are protected against damage; no component shall be located near the exhaust of an ICE or other heat source unless adequately shielded; components that can leak hydrogen in passenger, luggage, or other non-ventilated compartment shall be in a gas tight housing.

[*] European Integrated Hydrogen Project: C. Devillers, K. Pehr, D. Stoll, J.S. Duffield, S. Zisler, T. Driessens, H. Vandenborre, A. Gonzalez, R. Wurster, M. Kesten, M. Machel, F. Heurtaux, P. Adams, Contract JOE3-CT97-0088, 1.02.1998 to 30.04.2000

System	Tests or Requirements
Hydrogen Fuel System	• **Leak Test:** System - Leak test on the assembled hydrogen components, from fueling port to hydrogen conversion system and on the gas tight housing (with the vent line hermetically sealed). • **Acceleration Absorbance:** System (Container & Safety Devices) - Can perform a test demonstrating performance or equivalently use a numerical calculation. • **System Design:** The hydrogen system shall function in a safe and proper manner. It shall withstand the chemical, electrical, mechanical, and thermal service conditions without leaking or visibly deforming. The number of components and length of lines shall be kept to a minimum; the specific components shall be approved pursuant to Part I of this regulation. • **Fail-Safe Design:** Automatic valves shall fail-safe. • **Excess Flow:** An excess flow system shall be part of the hydrogen system.

Hydrogen Storage Sub-System	• **Container Installation:** A container/assembly shall be permanently installed on the vehicle; removed only for maintenance; shall not be installed in ICE compartment; a removable storage system may be removed but the components making up this system must be permanently installed within the removable storage system. A container or assembly with non-metallic liner shall not be installed inside the vehicle unless integrated into a system that ensures permeated hydrogen will be vented outside the vehicle (gas tight housing).
	• **Container Requirements:** A maximum of 4 containers per container assembly is permitted; The location of the container and assembly shall take into account possible sources of corrosion (inc road ice and leaking batteries); A minimum overpressure of 0.2 MPa shall be maintained in the container or assembly at ambient temp; A container or container assembly shall be designed to fulfill the vehicle's integrated function requirements plus the container requirements.
	• **Crashworthiness:** A container or assembly (including safety devices) shall be mounted and fixed so that specified accelerations can be absorbed without degrading the function of the safety devices when full; no uncontrolled release of hydrogen is permitted.
	• **Container Materials Approval Tests**: - Subcomponent - Tests include: Tensile test (plastic liner, Type 4), softening temperature test (polymeric liners, Type 4), glass transition temperature test (composite resin materials, Type 2, 3, 4), resin shear strength test (composite resin materials, Types 2, 3, 4), coating test (all container types), hydrogen compatibility test (container or liners, Types 1, 2, 3), hardness test (metallic liners and containers, Type 1, 2,3).
	• **Finished Containers Approval Tests** - Component - Test include: Burst test (all types), ambient temperature pressure cycling test (all types), leak-before-break test (all types), bonfire test (all types), penetration test (all types), chemical exposure test (Type 2, 3, 4), composite flaw tolerance test (Type 2, 3, 4), accelerated stress rupture test (Type 2, 3, 4), extreme temperature pressure cycling test (Type 2, 3, 4), impact damage test (Type 3, 4), leak test (Type 4), permeation test (Type 4), boss torque test (Type 4), hydrogen gas cycling test (Type 4), hydraulic test (all types).
	• **Container Manufacturing Batch Tests**: - Component - Tests include: Ambient temperature pressure cycle test (container), burst test (container), tensile test (container or liner), Charpy impact test (container or liner), bend test (container or liner), macroscopic examination (container or liner), softening/melting temperature test (container or liner), coating batch test (container). Applicable tests for each container type or liner are specified.
	• **Container Production Tests**: - Component - Tests include: Verification of principal dimensions and mass, verification of surface finish, verification that the maximum defect size does not exceed specified limits (metallic containers and liners), hardness test (Type 1, 2, 3), leak test (Type 4), hydraulic test (all types), markings verification (all types).
	• **Overpressure Protection:** The container, PRD(s), and any added insulation or protective material shall collectively protect the container from rupture when exposed to fire; materials used shall be suitable for the service conditions and comply with applicable standards; incompatible materials shall not be in contact; thermal insulation or other protective measures shall not influence the response and performance of PRDs.
	  - The set pressure of the PRV shall be <= the MAWP or >= 1.3x the nominal working pressure for the appropriate section of the hydrogen system.
	  - All PRDs, other safety components, and vent lines shall be protected against unauthorized interference; PRD shall be directly installed into the opening of a container so that it will discharge hydrogen to an atmospheric outlet that vents to the outside of the vehicle.
	  - PRD cannot be isolated from the container/assembly it protects by normal operation or failure of another component.
	  - Vent of the PRD shall not discharge into a wheel arch, nor be aimed at a heat source (exhaust) or at other containers/assemblies even in the event that the vent dislodges; shall discharge so hydrogen cannot enter the vehicle; vent shall be of sufficient size, free from obstruction, and protected from blockage.

System	Tests or Requirements
	• **Container Isolation Valve:** The flow of hydrogen from a container or assembly into the fuel supply line shall be secured with an automatic valve (idle closed); the valve shall be mounted directly on or within every container or one container in the assembly. - In the event of breakage of the refilling lines or fuel supply line(s), the isolating valves shall not be separated from the container/assembly. - Automatic valves isolating each container/assembly shall close if there is a malfunction of the hydrogen system that results in a release or severe leakage between the container/assembly and hydrogen conversion system.
Hydrogen De-Fueling Sub-System	• Not addressed
Hydrogen Fueling Sub-System	• **Endurance Test** : Component - Connection/disconnection cycles • **Receptacle Installation:** Receptacle shall be secured against maladjustment, rotation, unauthorized interference, and ingress of dirt/water and comply with ISO 17268; shall not be mounted within the external energy absorbing elements (i.e., bumper). • **Receptacle Access:** Access to receptacle shall not be in the passenger, luggage, or other unventilated compartment • **Check Valve:** Receptacle shall be integrated with a non-return valve; if receptacle not mounted on container, the refilling line shall be secured by a non-return or automatic valve integrating the function of a non-return valve; valve shall be mounted directly on the container or one in an assembly. • **Nominal Working Pressure:** NWP of receptacle shall be equal to the Class 0 (HP > 3 MPa) components upstream and including the first regulator. • **Safe Fueling:** The propulsion system (excluding safety devices) shall not operate when the vehicle is immobilized while the receptacle is connected to the refilling infrastructure.
Hydrogen Flow Control System	• **Safety Design:** The automatic valve for the fuel supply line of the propulsion system shall be operated such that the hydrogen supply to the propulsion system is cut off when the propulsion system is switched off, irrespective of the position of the activation switch, and shall remain so until the propulsion system is required to operate. • **Piping Tests**: Component - Endurance testing (Flexible fuel lines shall show no visible signs of damage; Hydraulic pressure testing (upstream and downstream rigid piping cannot rupture) • **Piping Vibration & Stresses:** Rigid fuel lines shall be secured such that they will not be subjected to critical vibration or other stresses; flexible fuel lines shall be secured such that they shall not be subjected to torsional stresses and abrasion is avoided; rigid and flexible lines must be designed to minimize stresses in the lines during removal or installation of adjoining hydrogen components; protect lines against corrosion. • **Piping Location:** Rigid and flexible fuel lines shall be routed to reasonably minimize exposure to accidental damage whether inside or outside the vehicle; if inside the vehicle must be within gas tight housing. • **Electrical Resistance:** Flexible fuel lines shall have an electrical resistance of less than 1Mohm per meter.
HP Flow Control Sub-System	• See Hydrogen Flow Control System
MP Flow Control Sub-System	• See Hydrogen Flow Control System
LP Flow Control Sub-System	• See Hydrogen Flow Control System
Fuel Cell System	• See Electric Power Management System
Fuel Cell Stack Sub-System	• See Electric Power Management System
Fuel Cell Cooling Sub-System	• **Leakage Test**: - Component- shall only be on the hydrogen circuit of the heat exchanger. • **Leak Detection:** A system shall be provided to detect failure in either circuit of the heat exchanger and prevent hydrogen from entering the other circuit(s), if the interface(s) is not able to withstand the loss of pressure in either circuit.
Fuel Cell Air Supply Sub-System	• See Electric Power Management System

System	Tests or Requirements
Electric Power Management, Control, & Propulsion System	• **Electronic Control Systems**: System - Test to verify function of the system under normal operating conditions. Test to verify the safety concept of the system (appropriate and expected actions are taken when internal faults are simulated) • **Basic Protection Measures:** Reasonable precautions shall be taken to avoid failure of other circuits affecting the hydrogen system. The electrical components of the hydrogen system shall be protected against overloads. • **Electrical Isolation:** Power supply connections shall not permit the ingress of hydrogen where hydrogen components are present or hydrogen leaks are possible. • **Bonding and Grounding:** The metallic components of the hydrogen system shall have electrical continuity with the vehicle's earth (e.g., chassis). During the refilling process the hydrogen system shall have the means to provide electrical continuity with the refilling facilities before hydrogen transfer is permitted. • **Insulation:** Provisions Regarding Electrical Components: The electrical system of any component in contact with hydrogen shall be insulated from the body of the component and the container or container assembly such that no current passes through the hydrogen containing parts.

APPENDIX B
FAILURE MODES AND EFFECTS ANALYSIS OF COMPRESSED-HYDROGEN FUELED FCV WITH CODES AND STANDARDS

High-Level FMEA for the NHTSA Hydrogen Fuel-Cell Vehicles Project

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A. Compressed-Hydrogen Fuel Storage System															
A.1 Compressed-Hydrogen Storage Sub-System															
A.1.1-a	Compressed-hydrogen fuel container	Compressed-hydrogen fuel container	Store and deliver hydrogen fuel to the fuel system. (5,000, 10,000 psi)	Inadequate design/test/manufacture/installation Degradation Seal failure Impact	Leak, loss of hydrogen without a substantial drop in pressure.	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Container design requirement	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.2, Design and Performance Req. for fuel container		WP.29 14.1 General Requirements	HGV2, 1.2 Container Types, 4.0 Service Conditions, 6.0 Material Qualification Tests & Requirements	
									Container qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 7.A, 7.B Design Qualification Tests	HGV2,18.0 Design Qualification Tests	304
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			Annex 7.A Approval Provisions	HGV2, 9.0 Inspection, 10.0 Manufacture, 11.0 Production Tests & Exams, 12.0 Batch Tests, 17.0 QA	
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100, 3.5 WP.29 Location and Installation	WP.29 14.1 Location, 14.2., Annex 7B Container Test Procedures		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1 (Component Test)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.1.1-b				Inadequate design//test/manufacture/installation Crash induced damage or penetration by external object. Fire induced damage	Rupture – loss of fuel and fragmentation of container (mechanically, chemically or thermally induced damage).	L	• Explosive release of mechanical energy (stored in the gas and the container) and explosive release of the container materials. • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1-a	See A.1-a (Design & Installation)	See A.1-a (Installation)	See A.1-a	See A.1-a	See A.1-a (Qualification)
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)	WP.29 14.2.4 (container mounting-calculation instead of test)		301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			WP.29 (bonfire) ECE R34 (pan fire test)	HGV2, 14.0 container shall be protected from fire with a pressure relief device, 18.9 bonfire test	304 (bonfire)
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									PRD	See A.1.2-a	See A.1.2-a	See A.1.2-a	See A.1.2-a	See A.1.2-a	See A.1.2-a
A.1.2-a	Thermally Activated Pressure Relief Device (PRD)	Thermally-activated device that vents the contents of the container when exposed to fire.	Maintains fuel container contents in normal service. Vents fuel containers in the case of a fire.	Inadequate design/test/manufacture/installation Mechanical failure	Fails to vent the contents in the event of a fire. (Single-point failure)	L	• Rupture of container, explosive release of mechanical energy (stored in the gas and the container) and explosive release of the container materials. • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	PRD design requirements	J2579, 4.1 & 6.2 Design Considerations 4.1.1.4 Overpressure Protection	23273-2, 5.2.2, Design and Performance Req. for fuel container	Article 100.3.1.4 Thermally activated PRD required;	WP.29 7A2.2 Overpressure Protection 14.1.8, 14.1.11, 14.5, 14.6	HPRD1 4.0 (general design statement), 6.1 (materials) 6.2 (fully vent)	
									PRD qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 7A, 7.B Design Qualification Tests	HPRD1 7.0 (design qualification), 9.0 (production batch testing)	
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 7.A	HPRD1 5.0 (QA), 7.3, 7.4 (inspection/acceptance)	
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 4.2.5 Discharges from PRD J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100.3.1.4 location requirements	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components		
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			WP.29 (bonfire) ECE R34 (pan fire test)	HGV2, 14.0 container shall be protected from fire with a pressure relief device, 18.9 bonfire test	304

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.1.2-b				Inadequate design/test/manufacture/installation Mechanical/failure	Vents contents inappropriately (in the absence of fire)	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Mass inertial release (launch container – blow away anything near the container	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.2-a Also, J2578 4.2.5 PRD should be vented outside vehicle	See A.1.2-a (design & installation) Also, 23273-2, 5.4 PRD shall vent to outside vehicle	See A.1.2-a (installation)	See A.1.2-a Also, 14.1.8 General Ventilation Requirement		
									Hydrogen leak sensors (notify driver)	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to determine measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
A.1.2-c				Inadequate design/test/manufacture/installation Crash induced damage or penetration by external object. Mechanical failure of the PRD.	Venting of contents/blowdown,-- loss of fuel and pressure in the container without fragmentation of the container. (mechanically induced damage)	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Mass inertial release (launch container – blow away anything near the container)	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.2-a Also, J2578 4.2.5 PRD should be vented outside vehicle	See A.1.2-a (design & installation) Also, 23273-2, 5.4 PRD shall vent to outside vehicle	See A.1.2-a (installation)	See A.1.2-a Also, 14.1.8 General Ventilation Requirement	HPRD1 Thermal test	
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)	WP.29 14.2.4 (container mounting-calculation instead of test)		301, 303 (Currently not applicable to Hydrogen)
									Hydrogen leak sensors (notify driver)	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
A.1.2-d				Inadequate design/test/manufacture/installation Mechanical Crash /Fire induced	Rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard. • Launch PRD	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.2-a	See A.1.2-a (design & installation)	See A.1.2-a (installation)	See A.1.2-a		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)	WP.29 14.2.4 (container mounting-calculation instead of test)		301, 303 (Currently not applicable to Hydrogen)

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.1.3-a	Container Shut-off/Selector Valve	Manual or electronic valve to shut off fuel flow from a storage container.	Shuts off fuel flow from a storage container.	Inadequate design/test/manufacture/installation Mechanical/electrical failure	Restrict or limit fuel flow. (*Assumes fuel meets purity levels required for PEM fuel cell operation and therefore will not clog)	L	• Performance issue – No Hazard • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	-	Valve design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.	Article 100 (fail-safe design)	WP.29 14.1 Design Statement 6. Specifications for hydrogen components 14.12 Fail-safe Design		
									Valve qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components, 14.1.10,14.10.4 Leak Test		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
A.1.3-b				Inadequate design/test/manufacture/installation Mechanical/electrical failure Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.3-a & J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	See A.1.3-a (design & installation)	See A.1.3-a (installation)	See A.1.3-a		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)	WP.29 14.2.4 (container mounting-calculation instead of test)		301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			WP.29 (bonfire) ECE R34 (pan fire test)		
									Downstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.1.3-c				Inadequate design/test/manufacture/installation Mechanical/electrical failure	Fail open	L	• Inability to shut off fuel flow (requires controlled de-fueling of the container) • Inability to shut off flow in an emergency or accident.	L	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.3-a & J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	See A.1.3-a (design & installation)	See A.1.3-a (installation)	See A.1.3-a		
A.1.3-d				Inadequate design/test/manufacture/installation Mechanical/electrical failure	Fail closed	L	• Inability to supply fuel; Performance Issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	-	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.1.3-a & J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	See A.1.3-a (design & installation; 6.1 fail-safe design)	See A.1.3-a (installation; fail-safe design)	See A.1.3-a (fail-safe design)		
									Second container				WP.29 (max of 4 containers per assembly)		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.1-a	Hydrogen fuel storage line and connections		Transfer compressed hydrogen to the HP flow control system.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact	Leak, rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 Annex 8A, 8B Design Qualification Tests		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 8 Conformity of Production		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100 (air tight)	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components WP.29 14.1.10,14.10.4 (protect against damage; leak test)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)	WP.29 14.2.4 (container mounting-calculation instead of test)		301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Downstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2579, 4.2 & 6.2.6 Design Qualification Tests	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.2 Hydrogen De-Fueling Sub-System															
A.2.4-a	De-fueling Manual Valve	Manual valve	Seal fuel from the environment when closed and permit emptying of fuel containers when open.	Inadequate design/test/manufacture/installation Mechanical failure	Restrict or limit fuel flow.	L	• Slows down emptying of fuel container	L	Design requirements	J2578, 4.2.7 Defueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Defueling Design	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 defueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
A.2.4-b				Inadequate design/test/manufacture/installation Mechanical failure Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/Manufacturing/QC/Installation reqs.	See A.2.4-a	See A.2.4-a (design & installation)	See A.2.4-a (installation)	See A.2.4-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Downstream HP Safety Relief (prevention)	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.2.4-c				Inadequate design/test/manufacture/installation Mechanical failure	Fail open	L	• Inability to shut off fuel flow, Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.2.4-a	See A.2.4-a (design & installation)	See A.2.4-a (installation)	See A.2.4-a		
									Container shut-off valve	J2578, 4.2.2, 4.5.1, & 4.6 fail-safe design to isolate fuel J2579, 4.1.1.2 & 6.2.1 fail-safe design to isolate fuel	ISO 23273-1, 6.1.1 fail safe design ISO 23273-2, 5.1 main shut-off valve shall be closed when not operating	Article 100 (main stop valve must be fail-safe)	WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
				Inadequate design/test/manufacture/installation Mechanical failure	Fail closed	L	• Inability to empty fuel container	-	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.2.4-a	See A.2.4-a (design & installation)	See A.2.4-a (installation)	See A.2.4-a		
A.2.5-a	De-Fueling Port	Fitting for removal of fuel from containers, downstream of de-fueling valve.	Allow for connection to fuel containers and removal of fuel.	Inadequate design/test/manufacture/installation Mechanical failure	Restrict or limit fuel flow.	L	• Reduced de-fueling flow rate; takes longer to de-fuel.	-	Design requirements	J2578, 4.2.7 Defueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Defueling Design; refer to SAE J2600	23273-1 23273-2		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests	23273-2, 5.2.1, Design and Performance Req		WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 defueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
A.2.5-b				Inadequate design/test/manufacture/installation	Become bent or damaged.	L	• Unable to connect so unable to empty container. • May leak which could result in ignition	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.2.5-a	See A.2.5-a (design & installation)	See A.2.5-a (installation)	See A.2.5-a		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.2-a	Hydrogen de-fueling line and connections		Allow de-fueling of compressed-hydrogen containers	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2578, 4.2.7 Defueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Defueling Design	23273-2, 5.2.1, Design and Performance		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 defueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100 (air tight)	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Downstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		
A.3 Hydrogen Fueling Sub-System															
A.3.6-a	Hydrogen Fill Stop/Check Valve Required by J2579, 6.2.9 Article 100.3.1.3	Automatic valve	Allow filling of fuel containers when while preventing back flow when open and maintain container pressure when closed.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Restrict or limit fuel flow.	L	• Takes longer to fill fuel container, No Hazard	-	Design requirements	J2578, 4.2.6 Fueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Fueling Design;	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 Fueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
A.3.6-b				Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Fail open	L	• May lead to back flow, and potential release of fuel to the atmosphere, Fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.3.6-a	See A.3.6-a (design & installation)	See A.3.6-a (installation)	See A.3.6-a		
A.3.6-c				Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection	Fail closed	L	• Prevents flow of fuel to the container; performance issue; No Hazard • Potential back flow and release of fuel to the atmosphere	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.3.6-a	See A.3.6-a (design & installation)	See A.3.6-a (installation)	See A.3.6-a		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
A.3.7-a	Hydrogen Fill Port	Fitting for connection to fuel containers when filling.	Allow for connection to fuel containers when filling with fuel.	Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Restrict or limit flow	L	• Reduced fueling flow rate; takes longer to fill fuel container.	L	Design requirements	J2578, 4.2.6 Fueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Fueling Design; refer to SAE J2600	23273-2, 5.2.1, Design and Performance Req. See ISO 17268.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 Fueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components, 8.2 fuelling inlet	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
A.3.7-b				Inadequate design/test/manufacture/installation Overpressure Degradation Impact Damaged or Degraded	Become bent or damaged	L	• Unable to connect so unable to fill container – Performance Issue; No Hazard	-	Design/Qualification/ Manufacturing/QC/Installation reqs.	See A.3.7-a	See A.3.7-a (design & installation)	See A.3.7-a (installation)	See A.3.7-a		
A.3-a	Hydrogen Fuel Filling Line and connections		Supply compressed hydrogen to the storage containers	Inadequate design/test/manufacture/installation Impact Overpressure Damaged Degraded Crash induced damage Fire induced damage	Leak/rupture	L	• Immediate ignition - Hydrogen jet flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2578, 4.2.6 Fueling Design J2579, 4.1 & 6.2 Design Considerations, 6.2.9 Fueling Design;	23273-2, 5.2.1, Design and Performance Req		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation, 7.2 Fueling procedure J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100 (air tight)	WP.29 Tbl. 8A1 14.1.10,14.10.4 (protect against damage; leak test) WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Downstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B. Hydrogen Flow Control System															
B.1 High-Pressure Flow Control Sub-System															
B.1.8-a	High-Pressure Safety Relief Valve	Pressure activated valve.	Release fuel in the event of high pressure in the delivery line. Protects downstream components and prevents fuel-line rupture.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow.	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 Annex 8A, 8B Design Qualification Tests WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Downstream MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.8-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.8-a	See B.1.8-a (design & installation)	See B.1.8-a	See B.1.8-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578 (minimize discharges <25% LFL; barriers, venting, reaction) J2579 (manage flammable conditions)	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Container Shut-off Valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.8-c				Inadequate design/test/manufacture/installation Mechanical	Fail open	L	• Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.8-a	See B.1.8-a (design & installation)	See B.1.8-a	See B.1.8-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	See B.1.8-a	See B.1.8-a		
									Container Shut-off Valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
B.1.8-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.8-a	See B.1.8-a (design & installation)	See B.1.8-a	See B.1.8-a		
									Downstream MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 Discharges; PRD shall vent to outside of vehicle	Article 100, 3.5.2 (shall be provided to discharge leaked H_2 & vent in a safe manner)	WP.29 (PRD vent to outside of vehicle)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.9-a	Main System Manual Valve	Manual valve	Permit fuel flow in the fuel line when open and isolate the fuel containers from downstream components when closed.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow.	L	• Performance issue – No Hazard	-	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.9-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.9-a	See B.1.9-a (design & installation)	See B.1.9-a	See B.1.9-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Upstream Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Upstream MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.9-c				Inadequate design/test/manufacture/installation Mechanical	Fail open (During maintenance or after crash – when you want it closed)	L	• Inability to isolate the fuel containers from downstream components.	M	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.9-a	See B.1.9-a (design & installation)	See B.1.9-a	See B.1.9-a		
									Downstream solenoid valves	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve	Article 100.3.1.2 (main-stop valve must operate electromagnetically without fail)	WP.29 (fail-safe design)		
									Upstream Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
B.1.9-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Performance issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.9-a	See B.1.9-a (design & installation)	See B.1.9-a	See B.1.9-a		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Upstream HP Safety Relief Valve	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.10-a	Main System Solenoid Valve	Electronically-activated solenoid valve.	Permit fuel flow in the fuel line when open and isolate the fuel containers from downstream components when closed. Operated by vehicle control system. Closes when engine is not running and/or the ignition is off.	Inadequate design/test/manufacture/installation Electronic failure Clogged with contaminants	Restrict or limit fuel flow.	L	• Performance issue • Reduced flow of hydrogen to fuel cell, potential membrane failure and fire.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)		Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.10-b				Inadequate design/test/manufacture/installation Electronic failure Damaged during a fire Crash induced damage	Leak or rupture (out of system 0	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.10-a	23273-2, 5.2.1, Design and Performance Req.	See B.1.10-a	See B.1.10-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)		Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)		Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.3, Location and Installation of Components	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-2, 5.2.1, Design and Performance Req.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main System Manual Valve & Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Upstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.10-c				Inadequate design/test/manufact ure/installation Electronic failure Stuck open due to contaminants	Fail open (During maintenance or after crash)	L	• Inability to stop fuel flow in an emergency or for maintenance	M	Design/Qualification/ Manufacturing/QC/Instal lation reqs.	See B.1.10-a	See B.1.10-a (design & installation)	See B.1.10-a	See B.1.10-a		
									Main System Solenoid Valve and Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
B.1.10-d				Inadequate design/test/manufact ure/installation Electronic failure Clogged with contaminants	Fail closed	L	• Stop, restrict, or limit flow of fuel, loss of power; potential for membrane rupture and fire.	H	Design/Qualification/ Manufacturing/QC/Instal lation reqs.	See B.1.10-a	See B.1.10-a (design & installation)	See B.1.10-a	See B.1.10-a		
									Upstream HP safety relief valve	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
B.1.11-a	High-Pressure Hydrogen Filter	Filter with fuel inlet and outlet and media to capture particles and droplets in the fuel line.	Remove solid and liquid contaminants from the hydrogen fuel stream to prevent damage of downstream components.	Inadequate design/test/manufact ure/installation Poor quality Hydrogen	Restrict or limit fuel flow (plugged/clogged).	L	• Performance issue • Limited fuel flow could lead to lower pressure on anode, membrane failure, and potential fire.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	14.1.10,14.10.4 (protect against damage; leak test)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Filter replacement						

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.11-b				Inadequate design or testing for hydrogen service Damaged, deformed	Allow passage of contaminants (Leak or rupture)	L	• Potential malfunction of downstream components • Performance Issue	M	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.11-b	See B.1.11-b (design & installation)	See B.1.11-b	See B.1.11-b		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
B.1.12-a	High-Pressure Regulator	Pressure regulator	Isolates high-pressure section of fuel line from the low-pressure section. Ensures delivery of fuel to downstream components at the proper pressure.	Inadequate design/test/manufacture/installation Damaged, deformed Clogged, plugged	Restrict or limit fuel flow.	L	• Performance issue • Limited fuel flow could lead to lower pressure on anode and membrane failure, potential rupture and fire	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.12-b				Inadequate design/test/manufacture/installation Damaged, deformed Crash induced damage Fire induced damage	Seal leak or rupture (out of system)	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.12-a	See B.1.12-a (design & installation)	See B.1.12-a	See B.1.12-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			301, 303 (Currently not applicable to Hydrogen)
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main System Solenoid Valve and Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Upstream HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.12-c				Inadequate design/test/manufacture/installation Damaged, deformed	Fail to control pressure – fail open	L	• Damage downstream components • Potential rupture and fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.12-a	See B.1.12-a (design & installation)	See B.1.12-a	See B.1.12-a		
									Downstream MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29, 14.6		
									Main System Solenoid Valve and Container Shut-off Valve	J2578, 4.1.1.2, 4.1.1.4, 4.2.2, & 4.6 fail-safe design, isolation, redundancy J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	See B.1.12-b	See B.1.12-b		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1.12-d				Inadequate design/test/manufacture/installation Damaged, deformed	Fails closed	L	• Prevents fuel flow, potential line rupture and fire • Performance issue	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.1.12-a	See B.1.12-a (design & installation)	See B.1.12-a	See B.1.12-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Upstream HP Safety Relief Valve	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.1-a	HP Hydrogen Flow Control Line		Transfers HP compressed Hydrogen to the MP flow section.	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100 (air tight)	14.1.10,14.10.4 (protect against damage; leak test)		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									HP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2 Mid-Pressure Flow Control Sub-System															
B.2.13-a	Mid-Pressure Safety Relief Valve	Pressure-activated valve	Release fuel in the event of high pressure in the delivery line. Protects downstream components and prevents fuel-line rupture.	Inadequate design/test/manufacture/installation Mechanical	Restrict or limit fuel flow	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Downstream Anode Safety Relief Valve	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29, 14.6		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	See B.1.12-b	See B.1.12-b		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.13-b				Inadequate design/test/manufacture/installation Mechanical Crash induced damage Fire induced damage	Leak or rupture	L	• Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	B.2.13-a	See B.2.13-a (design & installation)	B.2.13-a	B.2.13-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.13-c				Inadequate design/test/manufacture/installation Mechanical	Fail open	L	• Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	B.2.13-a	B.2.13-a (design & installation)	B.2.13-a	B.2.13-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.13-d				Inadequate design/test/manufacture/installation Mechanical	Fail closed	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.2.13-a	See B.2.13-a (design & installation)	See B.2.13-a	See B.2.13-a		
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Anode Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.14-a	Low Pressure Hydrogen Filter	Filter with fuel inlet and outlet and media to capture particles and droplets in the fuel line.	Remove solid and liquid contaminants from the hydrogen fuel stream to prevent damage of downstream components.	Inadequate design/test/manufacture/installation Poor quality Hydrogen	Restrict or limit fuel flow (plugged/clogged)	L	• Performance Issue • Limited fuel flow could lead to lower pressure on anode and membrane failure.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Filter replacement						
B.2.14-b				Inadequate design/test/manufacture/installation Degradation – wear/tear	Allow passage of contaminants to downstream components (leak or rupture)	L	• Potential malfunction of downstream components • Performance Issue	M	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.2.14-a	See B.2.14-a	See B.2.14-a	See B.2.14-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.15-a	Anode Pressure Regulator	Pressure regulator	Isolates the anode from the medium pressure section of the fuel delivery line. Ensures delivery of fuel to the anode at the proper pressure.	Inadequate design/test/manufact ure/installation Damaged, deformed Clogged, plugged	Restrict or limit fuel flow.	L	• Limit flow of fuel to engine – Performance Issue • Limited fuel flow could lead to lower pressure on anode and membrane failure. Potential rupture and fire	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.15-b				Inadequate design/test/manufacture/installation Damaged, deformed Crash induced damage Fire induced damage	Seal leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.2.15-a	See B.2.15-a (design & installation)	See B.2.15-a	See B.2.15-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Upstream MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2.15-c				Inadequate design/test/manufacture/installation Damaged, deformed	Fail to control pressure – Fails open	L	• Overpressure downstream components – membrane rupture/fire • Performance Issue	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.2.15-a	See B.2.15-a (design & installation)	See B.2.15-a	See B.2.15-a		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Flow meter	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards				
									Anode Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
B.2.15-d				Inadequate design/test/manufacture/installation Damaged, deformed	Fails closed	L	• Prevents fuel flow, potential line rupture and fire • Performance issue	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.2.15-a	See B.2.15-a (design & installation)	See B.2.15-a	See B.2.15-a		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Upstream Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.2-a	MP Hydrogen Flow Control Fuel Line		Transfers MP compressed Hydrogen to the LP flow section.	Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									MP Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3 Low-Pressure Flow Control Sub-System															
B.3.16-a	Anode Safety Relief Valve	Pressure activated valve.	Release fuel in the event of high pressure in the fuel cell. Protects fuel cell from overpressure and rupture.	Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection or fire protection	Restrict or limit fuel flow.	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels				

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.16-b				Inadequate design or testing for hydrogen service Inadequate design or testing for vehicular service Inadequate installation and mechanical protection or fire protection Crash induced damage Fire	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.16-a	See B.3.16-a (design & installation)	See B.3.16-a	See B.3.16-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels				
									Crash test requirements	Refers to FMVSS 301, 303 with modifications for Hydrogen Fuel J2579; design system to minimize releases	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.16-c					Fail open	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.16-a	See B.3.16-a (design & installation)	See B.3.16-a	See B.3.16-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels				
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
B.3.16-d					Fail closed	L	• Potential rupture of fuel line; Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment/potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.16-a	See B.3.16-a (design & installation)	See B.3.16-a	See B.3.16-a		
									Ventilation	J2578, 4.2.5 PRD should be vented to outside the vehicle J2579, 4.4.4.2 See J2578 for PRD discharge	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels				
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.17-a	Hydrogen Flow Meter	Flow meter	Measures the flow of fuel to the anode in the fuel cell.	Mechanical	Fail to function properly.	L	• If false high flow, will send signal to decrease flow unnecessarily – Performance issue or potential membrane failure and fire. • If false low flow, will send signal to increase flow when not needed, too much flow – damage fuel stack. Fire	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
B.3.17-b				Degradation, wear/tear	Leak or rupture.	L	• Damage downstream components – Fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	B.3.17-a	See B.3.17-a (design & installation)	B.3.17-a	B.3.17-a		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.18-a	Hydrogen Pressure Sensor	Sensor for fuel-line pressure measurement.	Measure pressure in fuel line for feedback to vehicle control system. Controls the reaction rate	Electronic failure	Fail to function properly.	L	• If false high flow, will send signal to decrease flow unnecessarily; reduced flow of hydrogen to anode could rapidly lead to membrane failure, and fire. • If false low flow, will send signal to increase flow when not needed, too much flow – damage fuel stack. Fire	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Flow meter	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards				
B.3.18-b					Leak or rupture.	M	• Fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.18-a	See B.3.18-a (design & installation)	See B.3.18-a	See B.3.18-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.19-a	Final Hydrogen Solenoid Valve	Electronically-activated solenoid valve.	Enable delivery of fuel to the fuel cell at the proper flow rate. Operated by vehicle control system.	Electronic failure Clogged with contaminants Inadequately designed or manufactured Damaged during installation	Restrict or limit fuel flow.	L	• Performance issue • Reduced flow of hydrogen to anode could rapidly lead to membrane failure, and fire.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1 (notify driver of FC power reductions)	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.19-b				Inadequately designed or manufactured Damaged during installation Damaged during a fire Crash induced damage	Leak or rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.19-a	See B.3.19-a (design & installation)	See B.3.19-a	See B.3.19-a		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels	Article 100.3.5.2 (discharge H_2 outside <4% concentration)	WP.29 14.10 (gas tight housing; vent to atmosphere)		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
									Upstream Anode Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3.19-c				Electronic failure Inadequately designed or manufactured Stuck open due to contaminants	Fail open (During maintenance or after crash)	L	• Inability to stop fuel flow in an emergency or for maintenance	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.19-a	See B.3.19-a (design & installation)	See B.3.19-a	See B.3.19-a		
									Main system solenoid valves; container shut-off selector valve	J2578, 4.1.1.4, 4.2.2, & 4.6 fail-safe design J2579, 4.1.1.2, 6.2.1 fail-safe fuel shutoff	23273-1, 6.1.1 fail-safe design 23272-2, 5.1, 5.2.4, means to close main H_2 shut-off valve; excess flow valve		WP.29 14.4.1 (container isolation valve; automatic valves must fail-safe)		
B.3.19-d				Electronic failure	Fail closed	L	• Stop, restrict, or limit flow of fuel, loss of power; potential for membrane rupture and fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.	See B.3.19-a	See B.3.19-a (design & installation)	See B.3.19-a	See B.3.19-a		
									Upstream Anode Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection	Article 100.3.4 (PRD or pressure detector & shut-down of HP H_2)	WP.29 14.5, 14.6 Pressure Relief		
									Monitor fuel cell voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
B.3-a	LP Hydrogen Flow Control Fuel Line		Transfers LP compressed Hydrogen to the fuel cell	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire induced damage	Leak, rupture	L	• Immediate ignition - Hydrogen flame • Collection of combustible mixture in closed environment, fire • Potential asphyxiation hazard • Delayed Ignition of collected vapors, potential explosion or detonation hazard.	H	Design requirements	J2579, 4.1 & 6.2 Design Considerations	23273-2, 5.2.1, Design and Performance Req.		WP.29 14.1 Design Statement 6. Specifications for hydrogen components		
									Qualification test requirements	J2579, 4.2 & 6.2.6 Design Qualification Tests			WP.29 Annex 8A, 8B Design Qualification Tests		
									Manufacturing and QC requirements	J2579, 4.3 & 6.2.7 Process Verification & QC Tests			WP.29 8 Conformity of Production		
									Installation, design and test requirements	J2578, 4.2.1 & 5.2 Installation J2579, 4.4 System and Vehicle Integration	23273-2, 5.3, Location and Installation of Components	Article 100 (air tight)	WP.29 14.1, 14.2.1, 14.2.2 Location and Installation of Components 14.1.10,14.10.4 (protect against damage; leak test)		
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Hydrogen pressure sensor	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (pressure gauge indicating HP side of fuel system)			
									Ventilation	J2578, 4.2.3 & 5.2 minimize discharges <25% LFL; barriers, venting, reaction	23273-2, 5.4 tests to ensure H_2 emissions under normal and failure conditions are below hazardous levels				
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.	Article 17, 100.3.5.5 (use He, test for fuel leakage in front, side, rear)			
									Thermal protection & fire test requirements	J2579, 6.2.6.7 bonfire & 6.2.6.8 localized fire; complete storage system; 4.1.1.5 thermal protection			ECE R34 (pan fire test)		
									Anode Safety Relief	J2579, 4.1.1.4 Overpressure Protection	23273-2, 5.2.3 Overpressure Protection		WP.29 14.5, 14.6 Pressure Relief		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C. Fuel Cell System															
C.1 Fuel Cell Stack Sub-System															
C.1.20-a	Fuel Cell Stack	Polymer Electrolyte Membrane (PEM) fuel cell	Convert hydrogen fuel to electric power	Inadequate design/test/manufact ure/installation Overpressuring of the anode; wear and tear	Membrane rupture (or small holes)	M	• Hydrogen in contact with air and catalyst at cathode, fire likely; permanent damage to stack.	H	Design requirements	J2578 4.3.1, 4.3.2 (General Design Principles; Ref. SAE J2344)					
									Qualification test requirements	J2578 4.3.4: High-Voltage Dielectric Withstand Capability	23273-3, 8.2 High-Voltage Isolation Test				
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Hydrogen sensor on cathode						
									Oxygen sensor on anode.						
									Voltage Monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
C.1.20-b				Inadequate design/test/manufact ure/installation Manufacturing, assembly, overheating	Seal leakage	M	• Low pressure hydrogen leak within the stack; fire possible • Low pressure external hydrogen leak, potential fire.	H	Design/Qualification/ Manufacturing/QC/Instal lation reqs.	J2578 4.3.1, 4.3.2 (General Design Principles; Ref. SAE J2344)					
C.1.20-c				Inadequate design/test/manufact ure/installation	Short circuit	M	• Shock • Ignition of vapors	H	Design/Qualification/ Manufacturing/QC/Instal lation reqs.	J2578 4.3.1, 4.3.2 (General Design Principles; Ref. SAE J2344)					

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.1.21-a	Anode Recirculation Pump	Pump for return of excess fuel from outlet to inlet of anode.	Allows for excess fuel to be pumped from the fuel cell back to the fuel inlet section. (low pressure 1-2 psi)	Inadequate design/test/manufacture/installation Pump damage or electrical failure	Fails to function	M	• Slow loss of electrical power – No Hazard.	-	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Cell voltage monitor with pump trip on low voltage	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions				
									Thermal protection & fire test requirements						
C.1.21-b				Inadequate design/test/manufacture/installation	Leak	M	• Low pressure Hydrogen release, potential for fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
C.1.22-a	Anode Purge Valve	Valve	Allow release of water and contaminants from the anode of the fuel cell (to exhaust)	Inadequate design/test/manufacture/installation	Restrict or limit flow.	M	• Slow loss of electrical power • Possible membrane rupture and fire	H	Design requirements				WP.29 14.12 Fail-safe Design		
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.1.22-b				Inadequate design/test/manufacture/installation Crash induced damage Fire induced damage	Leak or rupture	M	• Low pressure Hydrogen release, potential for fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Hydrogen leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.				
									Thermal protection & fire test requirements						
C.1.22-c				Inadequate design/test/manufacture/installation	Fail open	M	• Low pressure Hydrogen release, potential for fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Hydrogen Leak sensors	J2578, 4.2.8 (discharge & ventilation fault monitoring) J2579, 4.1.1.6 (fault monitoring)	23273-2, 7.3.2 Hydrogen-related fault conditions; FMEA or FTA to ID measures to limit hazards	Article 100.3.9 (at least 1 detector at appropriate position) & 3.9.5 (sensor warning & shut-down)	WP.29 Table 8A.1		
C.1.22-d				Inadequate design/test/manufacture/installation	Fail closed	M	• Slow loss of electrical power – No Hazard.	-	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
C.1.23-a	Cathode Humidifier	Humidifier	Assists in regulating the amount of water in the fuel cell, particularly in the cathode, to maintain fuel cell activity.	Inadequate design/test/manufacture/installation	Not functional	M	• Loss of moisture from the fuel cell, gradual power loss • Possible cell failure, holes - fire	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Severity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.1.23-b				Inadequate design/test/manufacture/installation	Leak from inlet to exit	M	• Loss of air to the fuel cell, rapid power loss. • Possible cell failure, holes - fire	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
C.2 Cooling Sub-System															
C.2.24-a	Radiator	Heat exchanger	Fluid to air heat exchanger to prevent overheating of fuel cell.	Inadequate design/test/manufacture/installation Degradation/wear-tear	Restrict or limit coolant flow.	M	• Overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					
C.2.24-b				Inadequate design/test/manufacture/installation	Fails to function	M	• Overheat fuel cell, membrane failure, fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.2.25-a	Stack Coolant Pump	Pump	Pumps coolant fluid through the fuel-cell stack and back through the radiator.	Inadequate design/test/manufacture/installation Loss of power	Fails to function	M	• Overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					
C.2.25-b				Inadequate design/test/manufacture/installation Impact External fire	Leak or rupture	M	• Overheat fuel cell, membrane failure, fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.2.25-c	Coolant line		Recirculates coolant through the fuel cell	Inadequate design/test/manufacture/installation Overpressure Degradation Crash induced damage Fire	Leak, rupture	M	• Overheat fuel cell, membrane failure, fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	23273-1 (notify driver of FC power reductions)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					
									Crash test requirements	J2578, 4.1.3 Refers to FMVSS 301, 303 with modifications for H_2 Fuel, 4.6.2 response to crash J2579, 4.1.1.7 minimize releases in crash; refer to J2578	23273-1, 5.4 Shall meet applicable national/international stds.				
									Thermal protection & fire test requirements						
C.3 Air Supply Sub-System (to the cathode)															
C.3.26-a	Cathode Air Filter	Filter	Removes particles and droplets from air feed stream to cathode. Chemical – Activated carbon removes sulfur	Inadequate design/test/manufacture/installation Failure to replace at required intervals	Restrict or limit air flow (partially plugged/clogged)	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.3.26-b				Degradation Failure to replace at required intervals	Hole in filter media	M	• Quickly contaminates fuel cell– performance issue (Contaminants take up room on the filter so efficiency is reduced.)	-	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
C.3.26-c				Contaminants Failure to replace at required intervals	Plugged	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	Design/Qualification/ Manufacturing/QC/Installation reqs.						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					
C.3.27-a	Cathode Air Blower	Blower/Fan	Forces ambient air into the cathode of the fuel cell.	Electrical/mechanical failure	Fails to function	M	• Sudden loss of power • Overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					

No.	Component	Component Description	Component Function	Cause of Failure Mode	Potential Failure Modes	Freq.	Failure Mode Consequences	Seve rity	Design Controls	SAE	ISO	Japanese	European	CSA	FMVSS
C.3.28-a	Cathode Air Flow Meter	Flow Meter	Measures the flow of air into the cathode.	Mechanical	Fails to function properly	M	• To much air flow will damage the membrane, fire • To little air flow is a performance issue, will lead to loss of power – but could also result in overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					
C.3-a	Air line		Supplies ambient air to the cathode of the fuel cell – line is heated to maintain design temperature for the fuel cell	Inadequate design/test/manufacture/installation	Leak, rupture	M	• Reduced air flow – performance issue • Overheat fuel cell, membrane failure, fire.	H	Design requirements						
									Qualification test requirements						
									Manufacturing and QC requirements						
									Installation, design and test requirements						
									Fuel cell voltage monitoring	J2578 4.1.1.3 monitor critical control & 4.3.5: low-voltage fault monitoring	23273-1, 5.2.1 notify driver of FC power reductions	Article 101.3.4.3 (test for function of switch to shut-off power from electrical leak)	WP.29 Annex 9 (electronic control system must be tested to verify safety concept)		
									Temperature sensors	J2578 4.2.8: process fault monitoring J2579 4.1.1.6 fault monitoring)					

DOT HS 811 075
February 2009

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA
www.nhtsa.gov