NRC·CNRC

# Technical Report

# Risk Assessment of Hydrogen and Battery Power in Locomotives – Part 2 – Risks and Hazards Assessment

Prepared for: Transport Canada
330 Sparks St.
Ottawa, Ontario

Prepared by: M. Hernandez, I. Jimenez, C. Rabbitt and E. Toma

National Research Council of Canada
Automotive and Surface Transportation Research Centre

February 2, 2023

Project: A1-020723
Report number: AST-2022-0008

National Research Council Canada | Conseil national de recherches Canada

Canada

# Change control

| Version | Date | Description | Authors |
|---|---|---|---|
| **A** | March 25, 2021 | Interim draft release | M. Hernandez, I. Jimenez and C. Rabbitt |
| **B** | July 29, 2022 | Draft release after client review | M. Hernandez, I. Jimenez and C. Rabbitt |
| **1.0** | November 22, 2022 | Initial release | M. Hernandez, I. Jimenez, C. Rabbitt and E. Toma |
| **2.0** | February 2, 2023 | Revised Section 3.1 | M. Hernandez, I. Jimenez, C. Rabbitt and E. Toma |

Prepared by:

Hernandez, Manuel
Digitally signed by Hernandez, Manuel
DN: cn=Hernandez, Manuel, c=CA, o=GC, ou=NRC-CNRC, email=manuel.hernandez@canada.ca
Date: 2023.02.02 14:36:14 -08'00'

**Manuel Hernandez, P.Eng.**
Research Council Officer, Energy System Integration, Modelling and Demonstration

Isabella Jimenez
Digitally signed by Isabella Jimenez
Date: 2023.02.03 09:26:32 -05'00'

**Isabella Jimenez**
Junior Engineer, Design Engineering

Rabbitt, Christopher
Digitally signed by Rabbitt, Christopher
Date: 2023.02.03 09:24:23 -05'00'

**Christopher Rabbitt, P.Eng.**
Vehicle Systems Engineer, Testing and Evaluation

Toma, Elton
Digitally signed by Toma, Elton
DN: cn=Toma, Elton, c=CA, o=GC, ou=NRC-CNRC, email=elton.toma@canada.ca
Date: 2023.02.03 13:22:29 -05'00'

**Elton Toma, P.Eng.**
Senior Research Engineer, Vehicle Structural Dynamics and Simulation

Reviewed by:

Gaudet, Bruce
Digitally signed by Gaudet, Bruce
Date: 2023.02.02 19:08:56 -05'00'

**Bruce Gaudet, P.Eng.**
Test Engineer, Testing and Evaluation

PrestonThomas, Jonathan
Digitally signed by PrestonThomas, Jonathan
DN: cn=PrestonThomas, Jonathan, c=CA, o=GC, ou=NRC-CNRC, email=jon.preston-thomas@canada.ca
Date: 2023.02.03 14:57:31 -05'00'

**Jon Preston-Thomas, P.Eng.**
Principal Engineer, Transportation Engineering Centre

Approved by:

Marsh, Philip
Digitally signed by Marsh, Philip
DN: cn=Marsh, Philip, c=CA, o=GC, ou=NRC-CNRC, email=philip.marsh@canada.ca
Date: 2023.02.03 15:19:32 -05'00'

**Philip Marsh, P.Eng.**
Director R&D, Transportation Engineering Centre

*Note that this report, Version 2.0 dated February 2, 2023, supersedes Version 1.0 dated November 22, 2022.*

## DISCLAIMER

*This report reflects the views of the authors only and does not reflect the views or policies of Transport Canada.*

*Neither Transport Canada, nor its employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy or completeness of any information contained in this report, or process described herein, and assumes no responsibility for anyone's use of the information. Transport Canada is not responsible for errors or omissions in this report and makes no representations as to the accuracy or completeness of the information.*

*Transport Canada does not endorse products or companies. Reference in this report to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by Transport Canada and shall not be used for advertising or service endorsement purposes. Trade or company names appear in this report only because they are essential to the objectives of the report.*

*References and hyperlinks to external web sites do not constitute endorsement by Transport Canada of the linked web sites, or the information, products or services contained therein. Transport Canada does not exercise any editorial control over the information you may find at these locations.*

# Abstract

An assessment of the risks and hazards associated with the operation of hydrogen fuel cell and battery powered (hydrail) locomotives was conducted. Two complementary reports were produced: a literature review (Part 1), and a codes and standards review (Part 3). A risk analysis for a hypothetical hydrail locomotive was conducted using a failure modes and effects analysis (FMEA) methodology, focusing on the risks and hazards introduced due to the fuel-cell, hydrogen, and battery systems. The goal was to provide an initial assessment of the potential magnitude and severity of the associated risks. The highest risks were flagged and risk mitigation measures were presented. A gap analysis was also performed to highlight those areas where further risk analysis would be required.

# Executive summary

The purpose of this study was to perform an assessment of the risks and hazards associated with the operation of hydrogen fuel cell and battery powered (hydrail) locomotives. This report presents a risk analysis for a hypothetical hydrail locomotive using a failure modes and effects analysis (FMEA) methodology, focusing on the risks and hazards introduced due to the fuel-cell, hydrogen, and battery systems. Two complementary reports were produced: a literature review on the subject (M. Hernandez, I. Jimenez, D. Chuang, E. Toma, C. Rabbitt and S. Mackie, "Risk assessment of hydrogen and battery power in locomotives - Part 1 – Literature review," National Research Council of Canada, Ottawa, 2022.), and a review of applicable codes and standards (M. Hernandez, C. Rabbitt, I. Jimenez and E. Toma, "Risk assessment of hydrogen and battery power in locomotives - Part 3 - Codes and standards," National Research Council of Canada, Ottawa, 2022.). The highest risks were flagged and risk mitigation measures were presented. A gap analysis was also performed to highlight those areas where further risk analysis would be required.

Since the risks and hazards for currently used diesel-electric locomotives are assumed to be well understood, the report focuses on the risks and hazards introduced due to the fuel cell, hydrogen, and battery systems. Some hazard areas are common to both diesel-electric and hydrail locomotives (e.g., traction motors, air compressor, heating and air conditioning systems), and while risks associated with these systems are currently understood in the context of a diesel or electric powered system, new hazards that may exist for a hydrogen system were identified. Reference designs for a hydrail switcher locomotive and a locomotive with a fuel tender, as detailed in the literature review, were used to identify the systems and components for the risk analysis.

A failure modes and effects analysis (FMEA) was performed to methodically identify component failure modes and analyze the effects of those failures on the system. The consequence severity for each failure mode was estimated from NEGLIGIBLE DAMAGE to SEVERE/CATASTROPHIC, and the probability of occurrence was estimated from IMPROBABLE to FREQUENT. A risk matrix was then used to rate the associated risk of that failure from LOW to HIGH.

A total of 60 specific hazards were identified and grouped into the following systems: hydrogen dispensing system, hydrogen storage, fuel supply and fuel cell power plant. For each system the FMEA results were tabulated, listing the component, cause of the hazardous event, mode of failure, result, probability, impact and risk. It was assumed that expected risk mitigation measures were implemented, and that each of the hazards were analyzed independently. All of the risks associated with the hydrogen dispensing system, the fuel supply and the fuel cell power plant were rated as LOW. Only two hazards associated with the hydrogen storage had a risk assessment of MEDIUM: crash induced damage or penetration by external object, and inadequate tank / thermal pressure relief device (TPRD) arrangement resulting in no TPRD actuation during localized fire.

To further analyze the highest rated risks, and identify risk mitigation measures, the following specific events were considered: fire on board or around the vehicle, derailment, crash with another object on the track, crash on the track with a vehicle carrying flammable dangerous goods, excessive vibration and dispenser failure. Codes and standards as well as common practices that can be used to mitigate the

risks were identified. A gap analysis was performed to identify the key areas where codes and standards are lacking, and to recommend areas for further study. The report includes an appendix listing specific risk mitigation factors for each of the hazards that were analyzed.

# Table of contents

# List of tables

# List of figures

# 1 Introduction

This report presents a review of the risks & hazards, and a risk analysis, for a hypothetical hydrogen fuel cell powered locomotive. It is Part 2 of a three-part set of reports, where Part 1 is a literature review [1], and Part 3 is a review of applicable codes and standards [2]. The purpose, background, objectives, and scope of the overall project are detailed in the literature review report.

The objective of this report is to provide readers with an understanding of the risks and hazards associated with hydrogen fuel cell powered locomotives. By drawing together findings in literature from various hydrogen fuel cell deployments in rail, as well as other modes, it presents hazards that have been identified to date and evaluates those hazards to provide an initial assessment of the potential magnitude and severity of those risks. This work is not intended to be an exhaustive compendium of hazards associated with hydrogen fuel cell locomotive design or operation – much work with physical design and testing in the real world over time will be required to holistically understand the hazards and develop appropriate mitigation measures.

Since the risks and hazards for currently used diesel-electric locomotives are assumed to be well understood, the report focuses on the risks and hazards introduced due to the fuel-cell, hydrogen[1], and battery systems. The specific risks associated with the storage and use of hydrogen on the locomotive, the operation of the fuel cell, and the use of a large volume of storage batteries (expected to be lithium-based[2]) are discussed. The highest risk hazards have been flagged and a gap analysis based on the findings of the study has been performed. Appropriate risk mitigation measures (e.g., engineering and operational controls) that should be considered in early stage design and preparation for real world testing are discussed.

[1] For brevity in the tables throughout the report, hydrogen will be abbreviated as $H_2$.

[2] Throughout the report the term lithium will be used rather than lithium-ion. Common lithium-ion chemistries include Lithium Cobalt Oxide ($LiCoO_2$), Lithium Manganese Oxide ($LiMn_2O_4$), Lithium Nickel Manganese Cobalt Oxide ($LiNiMnCoO_2$), Lithium Iron Phosphate ($LiFePO_4$), Lithium Nickel Cobalt Aluminum Oxide ($LiNiCoAlO_2$), and Lithium Titanate ($Li_2TiO_3$) (https://batteryuniversity.com/article/bu-205-types-of-lithium-ion).

# 2 Freight locomotives: diesel-electric and hydrail

This section presents the risks associated with a hydrogen fuel cell and battery powered (hydrail) locomotive. The risks currently associated with diesel-electric locomotives are reviewed first, then a comparison of the major systems of diesel-electric and hydrail locomotives is performed. Common systems are identified, and the potential for unique risks associated with hydrail locomotive systems are outlined.

The operation and maintenance of diesel-electric freight locomotives are well understood, having been the accepted locomotive design for use on all railways in North America since the mid-20th century. The product is mature, risks and hazards are well understood, and procedures are in place in the industry which minimize risks to operators and the public during their use.

In contrast, hydrail locomotives are new designs, have not been in revenue service anywhere in North America, and there are few people who are trained or experienced in their operation and use. The risks and hazards associated with them are not as well understood as those for the diesel-electric locomotive.

This section will briefly summarize the typical North American diesel-electric locomotive and its known hazards, and then present two hypothetical hydrail locomotive designs to be used as reference designs, from which risks and hazards are identified.

## 2.1 Review of diesel-electric locomotive hazards

The diesel-electric locomotive is the most common type used by freight railway companies in North America. Heavy-rail passenger rail systems in Canada, such as VIA Rail with its Halifax to Vancouver operations, Metrolinx in Toronto and Exo in Montreal, primarily use diesel-electric locomotives as well. A typical diesel-electric locomotive is composed of various mechanical and electrical subsystems that convert the energy stored in the diesel fuel into forward motion developed by the electrical drive. The key components are shown in Figure 1 [3]. For more detail on the diesel locomotive design, refer to the literature review report [1].

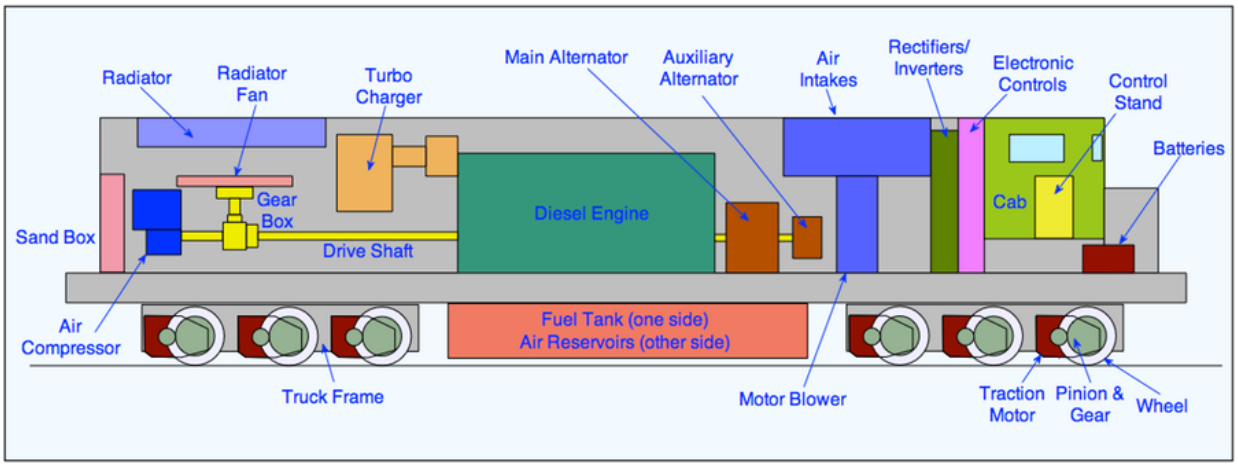


Figure 1: Schematic of diesel-electric locomotive

Section 2.1.1 presents some of the hazards associated with diesel-electric locomotives, which may also exist with hydrail locomotives. Other hazards which exist only with diesel-electric locomotives are then presented in Section 2.1.2, to provide a comparison to the hazards associated with hydrogen systems.

## 2.1.1 Hazards common to hydrail and diesel-electric locomotives

Regardless of which power system is used, locomotives present personal injury hazards that can result from the failure of or improper functioning of components such as slack adjusters, circuit breakers, contactors, relays, grid resistors, switches, and fuses. Other hazards may be caused by failure or excessive wear of components such as quill drives, axles, gears, pinions, traction motor gear cases, and fuel tanks. Additional hazards may be present near fan openings, exposed gears and pinions, exposed moving parts of mechanisms, pipes carrying hot gases and high-voltage equipment.

The high voltages from various pieces of equipment throughout a locomotive present an additional hazard. Locomotives may have a lethal voltage (30,000 V) even when the unit is shut down in the following areas: main electrical panel, cables, brake grids, contactors, main generator, batteries, and traction motors [4]. For example, cable and jumper connections may break, or insulation may become badly chafed. Broken wire strands, plugs, receptacles, or terminals may also cause hazards. Faults associated with motors and generators such as overheated support bearings, excessive accumulation of oil, shorted or grounded windings and mechanical failure (e.g., falling apart) may also create hazards.

These hazards and their associated risks, which are common to both hydrail and diesel-electric locomotives, are not considered in this study as the rail industry currently has risk mitigation procedures in place for these common hazards.

## 2.1.2 Hazards unique to diesel-electric locomotives

### 2.1.2.1 Diesel fuel / diesel exhaust

Locomotives have approximately 2,000 to 5,000 U.S. gal (7,600 to 19,000 L) of diesel fuel in the fuel tank. Diesel fuel is a flammable substance that may create a vapour/air explosive mixture if heated to a temperature above 52°C. The auto-ignition temperature of diesel fuel is 254°C to 285°C and it has a flammability range of 0.6 to 6.5% volume of air. There is a fire and explosion hazard that must be managed properly in order to avoid the risk of exposure of the diesel fuel vapour/air mixture to flame and

sparks. In addition to its flammability hazard, diesel fuel is poisonous to plants and animals. A spill of diesel fuel into the natural environment can contaminate ground water which will affect the fish, the potable water supply and irrigation [5]. When diesel fuel burns it creates diesel exhaust – a mixture of gases, vapours, aerosols, and particulate matter [5]. Human exposure to diesel exhaust can cause coughing, itching or burning eyes, and lung irritation. Exposure for a long period of time may increase the risk of lung cancer and bladder cancer [6]. Diesel fuel, oil, water, steam, and other leaks and accumulations of oil on electrical equipment may also create a hazard.

#### 2.1.2.2 Lead acid battery

In order to start the diesel engine, locomotives use lead acid batteries. During charging, the battery generates hydrogen and oxygen gas which create a highly flammable mixture. If flames or sparks occur near hydrogen that has become trapped in an enclosure, it may ignite and explode, causing acid to disperse. In addition, a risk of electric shock from battery charging equipment and strings of series-connected batteries is present whether the battery is being charged or not. Tipping of the battery can cause acid leakage. The sulfuric acid found in the battery may cause a fire and explosion if it contacts combustible or organic material. It may also react violently with strong reducing agents, metals, sulfur trioxide gas, strong oxidizers and water. If the acid has contact with metal it may also produce toxic sulfur dioxide fumes and hydrogen gas. The lead compound of the battery may also produce toxic fumes if it reaches temperatures above its melting point of 326°C [7].

## 2.2 Hydrogen fuel cell locomotive: reference designs

Two conceptual reference designs were created for a hydrogen and battery powered locomotive by the project team: a switcher locomotive and a line-haul locomotive with a tender [1]. The all-in-one switcher style hydrail locomotive, shown in Figure 2, outwardly has the same arrangement and footprint as a traditional diesel-electric locomotive; all the relevant hydrogen systems are packaged into the same form-factor. The main drawback of this design is the relatively small amount of hydrogen that can be carried, owing to compressed hydrogen's significantly lower volumetric energy density (assuming 70 MPa storage pressure) compared to diesel fuel. Multiple fueling cycles during a single 24-hour period may be necessary and could become an operational reality as a result of the limited fuel capacity of hydrail locomotives.

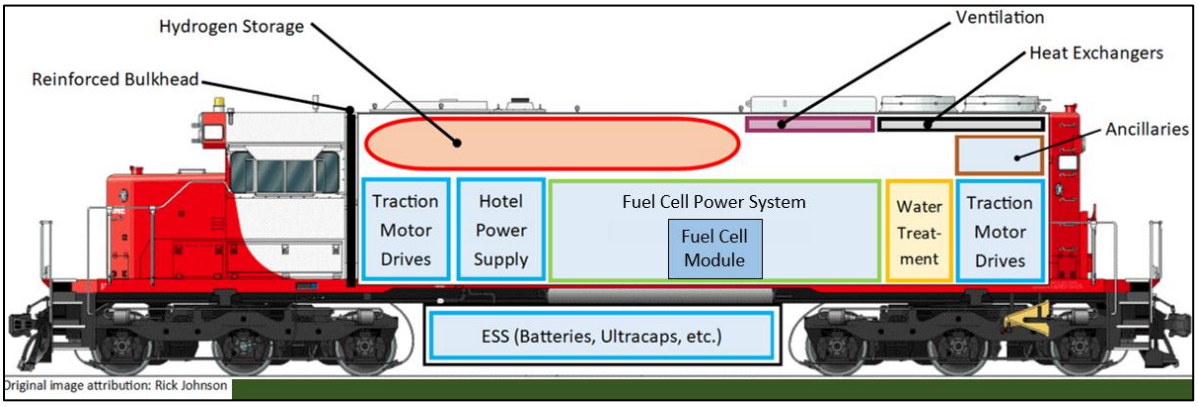


Figure 2: Conceptual fuel cell locomotive

The tender style of a line-haul hydrail locomotive, shown in Figure 3, typically has the hydrogen storage in a separate railcar that is married to the locomotive; a service umbilical connects the hydrogen tender to the locomotive. This umbilical carries fuel from the tender mounted storage tanks to the locomotive mounted fuel cell modules. This umbilical can also carry electrical power from the locomotive to the traction motors located on the tender. Additional details of this conceptual design are contained in the literature review report [1].

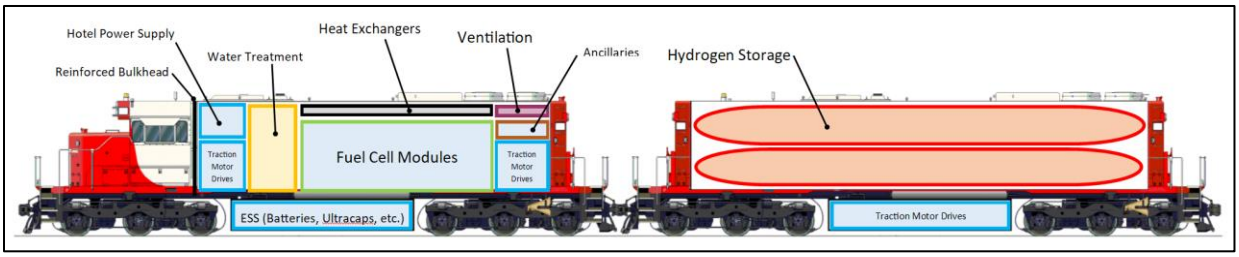


Figure 3: Conceptual fuel cell locomotive with hydrogen fuel tender

## 2.3 Major locomotive hazard areas

The major hazard areas for diesel-electric and hydrogen fuel cell powered locomotives are outlined in Figure 4.

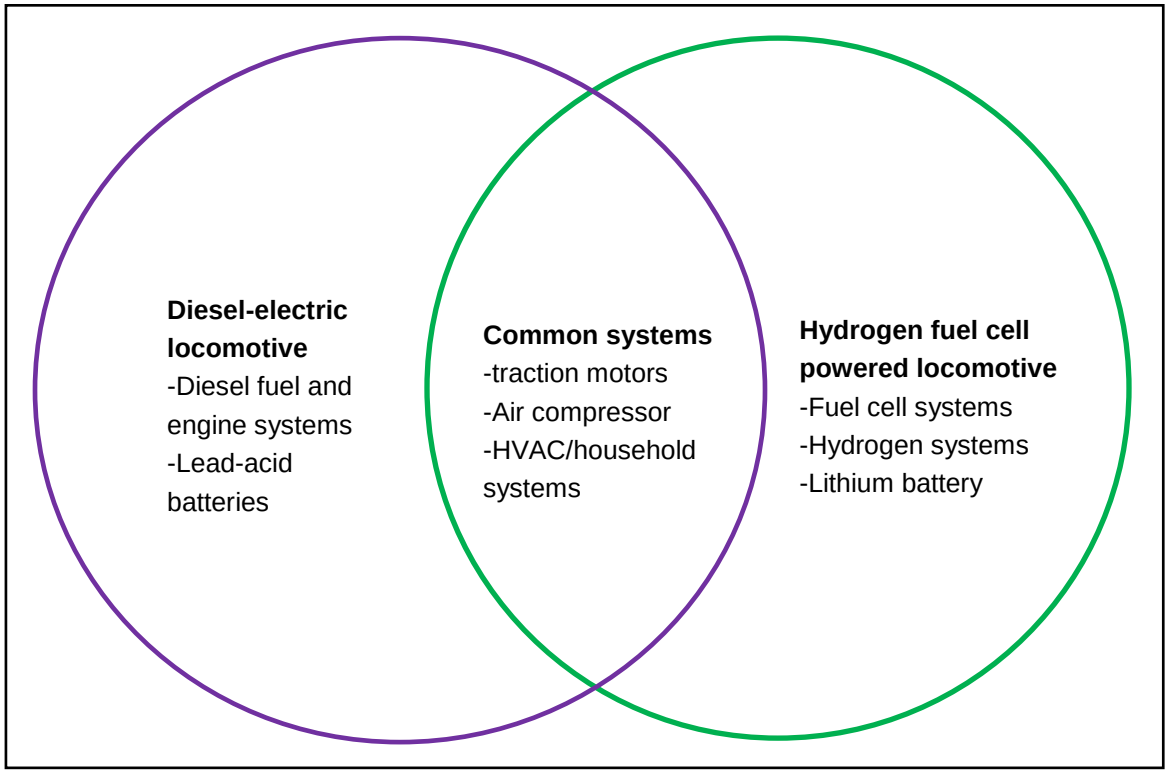


Figure 4: General outline of major hazard areas: diesel-electric and hydrail

The systems common to diesel-electric and fuel cell powered locomotives are the traction motors, the air compressors and the heating, ventilation and air conditioning (HVAC) systems shown in the intersection “Common Systems”. Risks associated with these systems are currently understood in the context of a diesel or electric powered system. For a hydrogen fuel cell powered system, the following new risks and hazards may exist:

- Traction motors: Traction motors are high voltage devices. As such the handling of the power systems poses risks, but these risks are currently known and understood. However, the presence of hydrogen may require that operations and procedures do not generate sparks or arcs that may pose an ignition source should hydrogen gas build up near the traction motors due to a leak in the general proximity or misdirected flow of hydrogen.
- Air compressor: Freight train brakes are powered and controlled by compressed air which is supplied by a compressor located on the locomotive. The air compressor hazards include electrical dangers, fumes, flying particles and debris, high pressure, and noise. As with traction motors, risks may be introduced if hydrogen gas builds up near the compressor motor.
- HVAC/household systems: Locomotives will have heated and air conditioned operator cabins, as well as washroom facilities on long-haul locomotives. The electrical and mechanical systems associated with these features may introduce risks to the operators related to the build-up of hydrogen gas (asphyxiation or fire). HVAC systems may need to be re-designed to prevent hydrogen build-up within cabin spaces as protection against undetected hydrogen leakage. As well, the current HVAC electrical systems may pose spark ignition hazards.

## 2.4 Hydrogen and fuel cell hazards

This section will present hazards for hydrogen and fuel cells. Section 3 will cover in more detail hydrogen fuel cell powered locomotive hazards. The hazards associated with hydrogen gas, hydrogen gas storage, and hydrogen fuel cells are discussed in Sections 2.4.1 to 2.4.3, respectively.

Table 1 presents working pressures for primary components of a hydrogen vehicle. These pressures have a significant effect on safety for a number of reasons. Higher-pressure hydrogen can result in higher energy ruptures and higher flow rates, exacerbating the effect of any leak [8] [9]. Higher pressure can also increase the effects of the hydrogen embrittlement discussed in Section 2.4.1 [10].

| Main components | Pressure (MPa) |
|---|---|
| storage tank on board | 70 |
| TPRD on storage tank | 70 |
| shut off valve on storage tank | 70 |
| pressure regulator for fuel supply to fuel cell | 70 |
| pressure relief valve (PRV) for fuel supply to fuel cell | 70 |
| fuel cell power plant | 2 |
| fuel cell module | 0.25 |
| ventilation system | N/A |
| compressor for air supply | 0.25 |
| cooling system | 0.25 |
| purge system | 0.25 |
| power management for fuel cell | N/A |

Table 1: Hydrogen vehicle component working pressures

### 2.4.1 Hazards associated with hydrogen

Hydrogen is the most abundant element in the universe with unique properties such that it must be handled safely as with other fuels [8]. Hydrogen disperses quickly into non-flammable concentrations in open air. In confined spaces, lighter-than-air gases such as hydrogen and methane accumulate near the top of the space. This is in stark contrast to heavier-than-air combustible gases and vapors such as propane, butane, and solvent vapors that accumulate near the bottom of the space. Since hydrogen is lighter than air, if it leaks to the atmosphere it is prone to be ignited by electro-static discharges. Due to its low density and viscosity, it is also prone to leak, which may present an asphyxiation hazard in enclosed environments. Hydrogen is also odorless, tasteless, colourless, nontoxic and noncorrosive. Adding odorants to allow humans to detect a leaking hydrogen system is typically not possible as the available odorants can poison fuel cells (i.e., contaminate the catalyst which degrades the fuel cell's performance). Additionally, hydrogen can interact at a molecular level with certain materials, most notably high-strength steels, which can lead to embrittlement and structural failure [11].

A pure hydrogen flame has low radiant heat that does not produce smoke unless impurities such as carbon are present [12]. The radiative heat transfer from a hydrogen flame is from 17 to 25%. The auto ignition temperature is 585°C and it has a burning speed of 2.65 to 3.25 m/s, which is much faster than methane or gasoline (at stoichiometric conditions). Therefore, hydrogen fires burn quickly, which increases the likelihood of an explosion due to the high flame velocity. The flammability range is 4 to 75% in air by volume, which is very broad compared to other common fuels. A combustible mixture of hydrogen in a pure oxygen environment can occur when there is 4 to 94% concentration of oxygen, and it requires merely 0.02 mJ of energy to ignite. Because of this flammability range, leaks of any size are a concern, and safety precautions are required where there may be oxygen or hydrogen concentrations at a dangerous level [8]. Also, hydrogen flames are difficult to extinguish; special flame arrestors for hydrogen are required. Table 2 highlights hazards for hydrogen, and the engineering controls used to reduce the risk.

| Hazard | Controls |
|---|---|
| potential for rapid accumulation in confined spaces (asphyxiant) | ventilation, leak detection sensors |
| high leak rate | ventilation, leak detection sensors |
| lack of smell | leak detection sensors |
| potential for undetected flames | flame sensors |
| wide flammability range | ventilation, leak detection sensors |
| minimal ignition energy | ventilation, grounding, bonding, segregation from ignition sources (area classification), use of equipment rated for classified areas (Group II C from Chapter 18 of the Canadian Electrical Code) |
| stored at high pressure | storage container design, Canadian registration numbers, pressure relief devices |
| material embrittlement | material selection |
| may react violently with some chemicals (e.g. oxidants and halogens) | segregation |

Table 2: Hydrogen hazards and engineering controls

### 2.4.2 Hazards associated with hydrogen storage

Gaseous hydrogen storage poses risks of its own, given the low density at atmospheric pressure and the ability of hydrogen to leak in gas storage systems where other heavier gases would not leak. Four types of storage tank for gaseous hydrogen used by industry are listed in Table 3 [13].

| Type | Operating Pressure (MPa) | Material | Advantages / disadvantages |
|---|---|---|---|
| Type I, seamless metallic containers | 25 | aluminum or steel | inexpensive / heavy |
| Type II, seamless metallic containers hoop-wrapped with fibre resin composites | 80 | aluminum or steel | heavy |
| Type III, metallic containers fully-wrapped with fibre resin composites | 35 | aluminum | lighter and less susceptible to hydrogen embrittlement |
| Type IV, polymeric liner fully wrapped with fibre resin composite | 70 | polymeric liner (hydrogen permeation is possible through this type of liner) | lighter than Type III but expensive |

Table 3: Types of storage for gaseous hydrogen

### 2.4.3 Hazards associated with fuel cells

Fuel cells will also have their own hazards. The electric motors of some fuel cell powered vehicles run on voltages exceeding 350 V, presenting both an electrocution hazard and an ignition source for fuel contained in the vehicle, or outside materials [14]. Additionally, fuel cells tend to leak hydrogen gas, leading to risks of hydrogen buildup in areas near the fuel cell.

## 2.5 Lithium battery hazards

Lithium batteries include a wide range of battery chemistries with various combinations of anode, cathode and electrolyte materials designs that allow battery tailoring for different energy and power ratings, and specifications that are defined by the application [15]. Within the last 15 years there have been several reports of lithium battery fires and/or explosions in vaping products, personal portable devices, e-bikes, laptops, electric vehicles, etc. In some cases these fires have occurred on-board aircraft (as cargo), as well as within cargo terminals. In response to these events, batteries have been considered dangerous goods when transported in Canada, and fall under specific transportation regulations. International governments and the air transportation industry are working to improve regulations, codes and standards to protect public safety. Battery manufacturers are also striving to improve product reliability.

Failures of lithium cells/batteries can be classified into two main categories [15]. The first category of failures are those that result in the cell/battery not delivering expected performance such as rated energy/power, lifespan, or shelf life. These types of failures bring about risks to the transportation end-use where a loss of power could be catastrophic. The second category of failures are those that result in the cell/battery not providing protection against known and likely safety hazards such as leakage, overheating, overpressure, and thermal runaway. Because of the number of lithium battery design parameters, it is usually a very challenging task to determine the potential faults, especially regarding cell/battery safety. Once a cell/battery has been manufactured, other factors related to inadequate storage environments, mishandling, and abusive operation add to the complexity in predicting and preventing failures.

Lithium batteries contain highly flammable materials (e.g., electrolyte) and combustible materials (e.g., carbon), as well as highly oxidizing cathode materials [15]. The lithium cell has a greater energy density than lead-acid batteries typically used on locomotives, and contains flammable organic solvents as part of the electrolyte. The cells have the potential to spontaneously ignite and catch fire or explode due to overheating and gas generation. Three elements must be simultaneously present for the combustion of the chemicals: fuel, oxygen, and an ignition source. However, there must be a proper portion of fuel and oxygen in local concentrations. The ignition source can be in the form of hot surfaces, hot metal sparks, internal battery shorts, exposed vehicle electrical wiring, or rupturing of the cell packaging. Furthermore, lithium batteries have a limited range of temperatures and operating voltages where the intercalation mechanism will work correctly. If the temperature or operating voltage goes beyond the range, undesirable side effects such as exothermic reactions and/or internal electric shorts creating self-heating may occur. If the heating persists, it will create the conditions for thermal runaway – self-heating reactions within the cells causing uncontrollable increases in temperature and pressure. Thermal runaway can affect surrounding cells and end in catastrophic cell failure and propagation beyond the individual cell. Catastrophic failure of lithium cells may be more severe than other rechargeable cells of equivalent size. The exothermic reactions and/or internal electrical shorts may be triggered by factors such as, but not limited to:

- cell manufacturing defects:
    - contaminated materials;
    - damaged electrodes;

  - defective axial offset registry (the distance between the anode deposition and the cathode deposition with respect to each other – these defects can lead to a thermal runaway due to shock or vibration); and
  - inadequate quality assurance program.

- cell integration errors:
  - mechanical damage during cell integration;
  - burrs;
  - weld spatter;
  - inadequate installation procedures (e.g., inadequate foil welding technique); and
  - inadequate quality assurance program.

- battery design deficiencies:
  - inadequate battery temperature management system (the most important safety aspect of lithium battery integration);
  - inadequate short circuit protection; and
  - inadequate battery management system.

- storage and use issues:
  - mechanical damage (e.g., crush, puncture, excessive shock and vibration);
  - electrical short circuit;
  - overheating;
  - rapid discharge;
  - overcharging;
  - over-discharging;
  - misuse; and
  - abuse.

Potential primary hazards caused by thermal runaway include venting of high-temperature electrolytic solvent vapors, combustion of ejected flammable electrolytic solvent vapors, local overpressure and failure of pressure relief devices, and cell casing rupture and release of projectiles. Potential secondary hazards may include toxic and/or incompatible materials, asphyxiation, ignition and burning of adjacent flammable vehicle components or surfaces, and high-voltage electrical shock hazards [16].

Some of the safety design elements to consider in the manufacturing of lithium batteries are:

- adequate battery thermal management system;
- battery management system control for charge, charge termination and discharge;
- cell chemistries and safety elements:
  - safer anode and cathode material (e.g., $LiFePO_4$ is safer than $LiCoO_2$ , titanate is safer than graphite, and low surface carbon is safer than large surface carbon);
  - high flash point organic electrolyte;
  - proprietary formulation additives to stabilize the solid electrolyte interface; and
  - internal safety design (e.g., shutdown separator, positive temperature coefficient, current interrupt device and safety vents).
- cell spacing and thermal path for heat dissipation;
- cell insulation between adjacent cells and battery elements; and
- adequate short circuit protection.

Table 4 shows the composition of a typical lithium cell and the respective hazards of each component [14] [16] [17].

| Cell components | Composition range (~wt. %) | Hazard |
|---|---|---|
| cathode active materials (e.g., lithium cobalt oxide) | 22 - 28 | decompose at high temperatures (above 180°C) and react with the electrolyte. Oxidative power increases with cell charging and creates a very strong oxidant when cell is overcharged |
| anode active materials (e.g., graphite) | 15 - 19 | exothermic reaction with electrolyte to form solid electrolyte interface. Thermal stability of lithium-intercalated carbon in electrolyte varied depending on the electrolyte, state of charge, and electrode surface area. |
| electrolyte | 12 - 14 | combustible |
| binder | 3 - 5 | combustible |
| plastics | 4 - 5 | combustible |
| aluminum parts | 12 - 13 | powder or dust forms are combustible in air |
| **Cell elements** | | |
| total lithium* | 1 - 4 | if deposited as metal, is highly flammable and corrosive. |
| total bonded oxygen | 8 - 13 | released if cathode materials decompose at high temperatures |
| total solvent | 12 - 14 | highly flammable, reacts with lithiated carbon to form solid electrolyte interface |
| total graphite | 15 - 17 | combustible |
| total carbon | 2 - 5 | combustible |

Table 4: Lithium cell components, elements, and associated hazards

Figure 5 illustrates the pattern of a lithium cell failure from an abuse stage to a thermal runaway event [15]. It shows that the first sign of a hazard occurrence is a cell heating. After this stage, the rate of cell self-heating or overheating will depend on many factors. The thermal runaway can happen in a few minutes, after a few hours, or even after a few days from the initial abuse. Figure 6 summarizes some possible failure paths when a lithium cell/battery is abused [15]. The blue pathways represent triggers occurring when the battery is in use (i.e., discharging or charging). The yellow pathways represent triggers occurring when the battery is not being used.

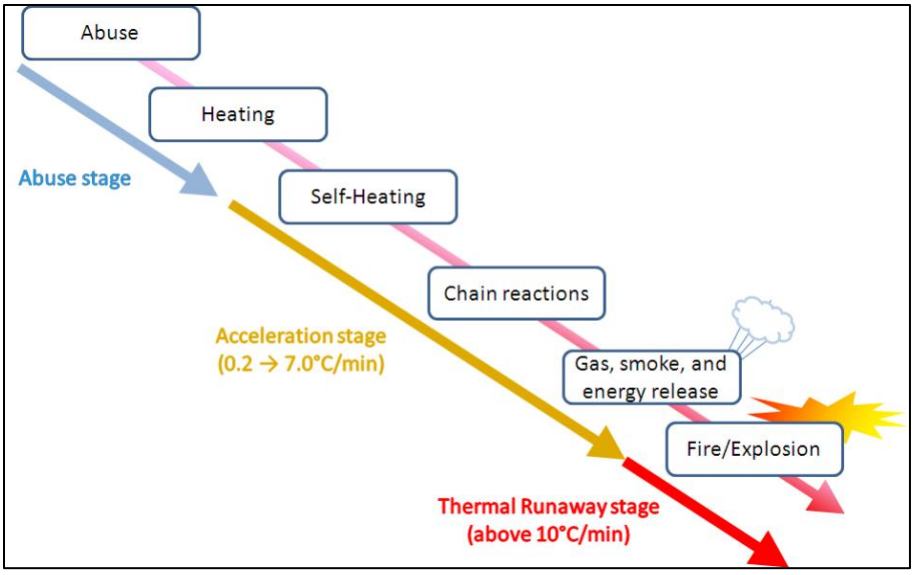


Figure 5: Pattern of a thermal runaway for lithium cells/batteries

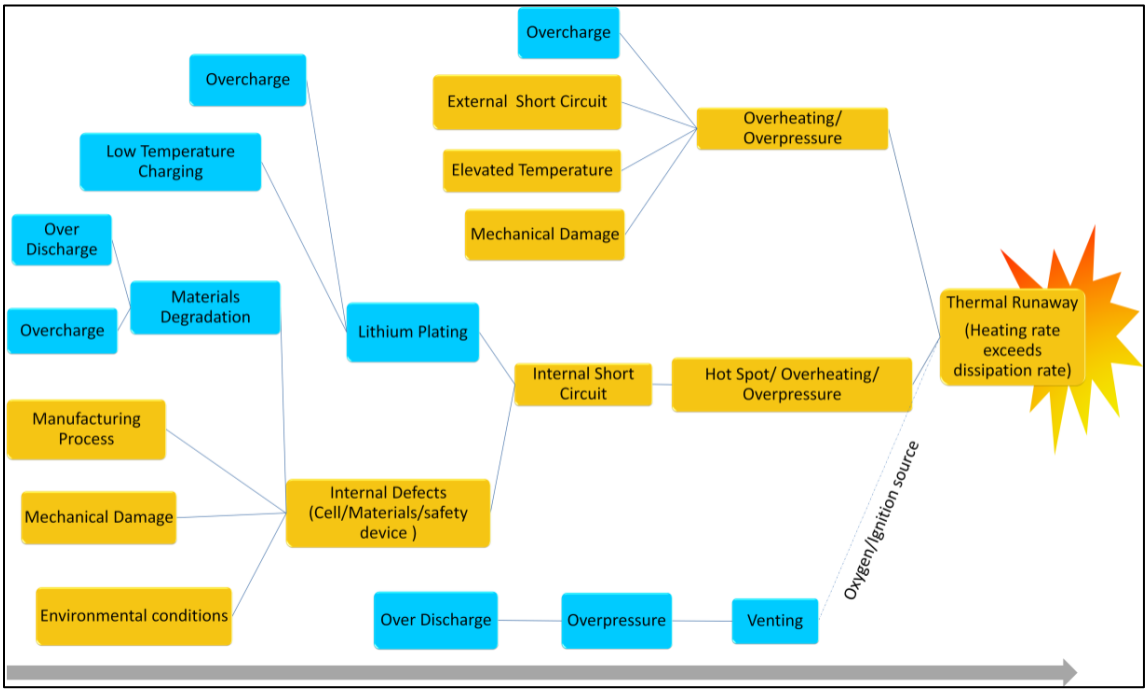


Figure 6: Triggers and possible pathways leading to catastrophic failures of lithium cells

Figure 7 illustrates typical voltage and temperature operating windows recommended by manufacturers for lithium cells [18]. Operating a cell/battery outside the recommended operating windows is considered an abuse and can lead to a variety of failure mechanisms. Lithium cells and battery failure rates are not well understood; however, Table 5 lists some estimates for failure rates of different applications [18].

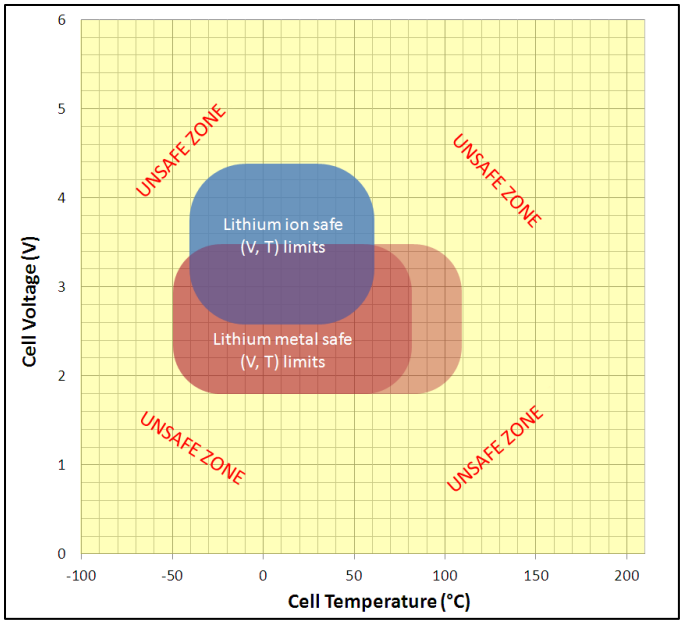


Figure 7: Typical lithium cell operating voltage and temperature windows

| Estimated failure rates as reported | Failure rate unit per billion | Comments |
|---|---|---|
| 1 in 10 million | 100 | estimation approach not found in the open literature |
| 1 in 1 million | 1,000 | for laptop cells in operation |
| 1 in 40 million | 25 | based on an estimated 100 failures per year for a production of 4 billion cells |
| 1 in 200,000 | 5,000 | it is not clear how it was estimated but it is mentioned that this rate triggered a recall of almost six million lithium packs used in laptops manufactured by Dell and Apple |
| 1 in 1 million | 1,000 | SRI International reported the origin of this rate from the failure analysis firm Exponent |
| 1 in 1 billion | 1 | this rate was assumed for failure during shipping |
| 1.99 in 1 billion | 1.99 | the rate is specific for plane accidents per ton-mile (The report is controversial and received critical comments from the Portable Rechargeable Battery Association about the methodology and the approach.) |

Table 5: Reported failure rates of lithium batteries

# 3 Hydrogen fuel cell locomotive risk analysis

A comprehensive system safety analysis must be an integral part of any hydrail initiative. Hazard and risk assessments are methods used to identify system safety susceptibilities and weaknesses and to understand mitigating measures to address those deficiencies. A project team comprising relevant stakeholders (whose expertise covers all the pertinent areas of the project) can use well established methods to perform the hazard and risk assessments. Some common risk assessment tools are [19]:

- checklist analysis;
- event tree analysis and barrier analysis;
- failure modes and effects analysis (FMEA);
- fault tree analysis (FTA);
- hazard and operability analysis (HAZOP);
- hazard identification (HAZID);
- probabilistic risk assessment (PRA);
- quantitative risk assessment (QRA); and
- risk matrix binning.

These and other methods are summarized in [19]. These methods, or a combination of them, should:

- cover all the hazards;
- consider prior near-misses, incidents and accidents;
- consider the coverage range of the vehicle;
- consider the operating conditions;
- include all required engineering and administrative controls appropriate for the hazards;
- include all relevant failures modes of the engineering and administrative controls and the consequences of those failures; and
- include, as a minimum, qualitative assessments of the health and safety consequences of control failures.

The NRC participated in an FMEA during a previous study for Metrolinx [20], so in order to leverage that knowledge, the authors decided to perform an FMEA for this current project. The FMEA risk assessment tool is semi-quantitative, and it methodically describes all component failure modes and analyzes the effects of those failures on the system. The main FMEA stages include defining:

- the scope – this includes determining the system boundaries and an adequate depth of the assessment (components, systems or subsystems that will be examined);
- the equipment and components, and their associated events and hazards (e.g., mechanical failure, hydrogen leak, breakage, etc.);
- the conceivable initiating failure modes and effects for the equipment and components;
- the possibility for early detection of the failure modes;

- the risk priority number (RPN)[3] (Note that this number is not always used); and
- the possible mitigation or corrective actions and RPN re-adjustment [19].

## 3.1 Definition of the risk register

In a previous project, Canadian Nuclear Laboratories (CNL) developed a risk register using the FMEA method for a number of postulated failure events that may occur in hydrogen production, storage, delivery, refueling and dispensing, and hydrogen fuel cell vehicle. The likelihood of each failure event and the severity of its consequence were ranked by the experts from A.V. Tchouvelev & Associates Inc. (AVT), the Canadian Standards Association (CSA), CNL and the NRC [20]. The assessment considered harm to people, property, and the environment, ranking each risk as LOW, MEDIUM or HIGH based on both the likelihood of occurrence of the events and the severity of the consequences. The risk matrix, as defined by the combination of these two parameters, is shown in Table 6. The definitions of the estimated probability of occurrence are provided in Table 7, and the definitions of the consequence severity are provided in Table 8. The assessment outcomes for the dispensing and hydrogen fuel cell vehicle are presented in Table 9 through Table 12 of this report. These outcomes represent the expert opinion of AVT, CSA, CNL and the NRC.

| **Consequence severity** | **Estimated probability of occurrence (per year)** | | | | |
|---|---|---|---|---|---|
| | 1-Improbable (<0.0001) | 2-Remote (0.01-0.001) | 3-Occasional (0.01-0.1) | 4-Probable (0.1-1) | 5-Frequent (>1) |
| 1-Negligible damage | LOW | LOW | LOW | LOW | LOW |
| 2-Minor damage | LOW | LOW | LOW | LOW | MEDIUM |
| 3-Damage | LOW | LOW | LOW | MEDIUM | HIGH |
| 4-Major damage | LOW | LOW | MEDIUM | HIGH | HIGH |
| 5-Severe/catastrophic | LOW | MEDIUM | HIGH | HIGH | HIGH |

Table 6: Risk matrix

| **Level** | **Description** | **Definition** | **Frequency** |
|---|---|---|---|
| **1** | IMPROBABLE | possible but may not be heard of or may not be experienced world wide | ≤$10^{-4}$ per year |
| **2** | REMOTE | unlikely to occur during lifetime/operation of one subsystem | $10^{-3}$ - $10^{-2}$ per year |
| **3** | OCCASIONAL | likely to occur during lifetime/operation of one subsystem | $10^{-2}$ - $10^{-1}$ per year |
| **4** | PROBABLE | may occur several times in the subsystem | 0.1 - 1 per year |
| **5** | FREQUENT | will occur frequently at the subsystem | > 1 per year |

Table 7: Estimated probability of occurrence

[3] Risk Priority Number is calculated as the Severity x Occurrence x Detection. The severity of the failure mode is rated on a scale from 1 to 10. A high severity rating indicates severe risk. The potential of failure occurrence is rated on a scale from 1 to 10. A high occurrence rating reflects high failure occurrence potential. The capability of failure detection is rated on a scale from 1 to 10. A high detection rating reflects low detection capability.

| Level | Description | People | Environment | Material |
|---|---|---|---|---|
| **1** | NEGLIGIBLE DAMAGE | no injury, annoyance, disturbance | negligible environmental damage | negligible material damage |
| **2** | MINOR DAMAGE | minor injury, annoyance, disturbance | minor environmental damage | minor material damage |
| **3** | DAMAGE | medical treatment; lost time injury | local environmental damage of short duration < 1 month | minor structural damage; minor production influence |
| **4** | MAJOR DAMAGE | permanent disability prolonged hospital treatment | time for restitution of ecological resource < 2 years | considerable structural damage; production interrupted for weeks |
| **5** | SEVERE / CATASTROPHIC | one to several fatalities | time for restitution of ecological resource such as recreation areas, ground water >2 years | loss of station and production interrupted for months |

Table 8: Consequence severity

The risks shown in Table 6 which are rated as HIGH are considered unacceptable; measures should be taken to reduce or remove any risks in this category. Those rated as MEDIUM may be acceptable, but measures should nevertheless be considered to reduce the risks as much as reasonably practical. Those risks rated as LOW are considered acceptable, and no further measures need to be taken.

## 3.2 Identified risks and hazards

The previous research (referenced in Section 3.1) identified 43 hazards related to the hydrogen locomotive through a collaborative brainstorming exercise. These hazards were augmented by others considered as being within the scope of this current report, and all of the hazards were grouped into the following systems: hydrogen dispensing system, hydrogen storage, fuel supply and fuel cell power plant.

The probability of occurrence of each hazard was estimated based on the experience of the participants, as well as statistics published by the Transportation Safety Board for the period 2005-2014 [21]. The risk assessment matrices are presented in the tables in Sections 3.2.1 to 3.2.4. Each matrix includes a column for the following:

- component (only the major components for each system);
- cause (of the hazardous event) (e.g., a mechanical failure, electrical failure or an event such as a crash that could result in a failure mode);
- mode (of failure) (e.g., hydrogen leak, mix of hydrogen and air, accumulation of hydrogen, etc.);
- result (e.g., ignition, explosion, unignited release, jet fire, etc.);
- probability (as described in Table 7);
- impact (i.e., consequence severity, as described in Table 8); and
- risk (assigned risk ranking from Table 6).

This current study assumed that the expected risk mitigation measures detailed in Section 4.4 have been implemented. It also assumed that the principle of separation of hazards is implemented. For example, it is assumed that the lithium battery and the fuel cell system are physically separated such that there is no interaction between them. It is also assumed that the American Society of Mechanical Engineers (ASME) steel storage tank pressure rating exceeds the compressor pressure capability, and that the compressor outlet PRV protects the hydrogen storage tank and that there is no check valve between the compressor and the storage tank. For Type III and Type IV composite tanks, it is assumed that thermal pressure relief devices (TPRDs) are installed on both ends.

It is also assumed that safety programmable controls comply with all the applicable standards from Table 12 of the codes and standards report [2], and that safety control equipment complies with all applicable standards from Table 11 of the codes and standards report.

### 3.2.1 Hydrogen dispensing system

As shown in Table 9, several risks and hazards were associated with the hydrogen dispensing system. This is external to the locomotive, but necessarily connected. Mechanical failure of the dispensing piping, hose, and/or nozzle all create the possibility of either an unignited release of hydrogen or a jet fire, with an associated consequence severity of DAMAGE or MINOR DAMAGE, respectively. The fire risk can be mitigated by controlling sources of sparks or ignition, and ensuring hoses meet CSA / International Organization for Standardization (ISO) standards. Failure to disconnect the nozzle prior to the locomotive departing would activate the breakaway device, causing a minor release of hydrogen; the consequence severity for this event is NEGLIGIBLE DAMAGE.

The dispensing system includes a number of valves, including the solenoid control valve, a flow controller, and a PRV. Any of these valves can fail open, causing a release of hydrogen which may be ignited or form a jet fire. In either case, the expected consequence severity is NEGLIGIBLE DAMAGE. The PRV may also fail closed, in which case the upstream line may fail, with the results identified above.

None of these hazards were considered to have an occurrence probability greater than OCCASIONAL, therefore all were considered LOW risk (in accordance with the risk matrix in Table 6). All of these risks should be subject to periodic re-evaluation as adoption of hydrail expands.

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| **Dispensing piping** | Leak due to mechanical failure | Leak of $H_2$ to atmosphere during dispensing | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| **Dispensing hose** | Leak due to mechanical failure | Leak of $H_2$ to atmosphere during dispensing | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| | Drive-away while connected with the nozzle | Stop $H_2$ flow due to activation of breakaway device | Unignited small release | REMOTE | NEGLIGIBLE DAMAGE | LOW |

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| **Dispensing nozzle** | O-ring or nozzle damaged | Leak of $H_2$ to atmosphere during dispensing | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| **Solenoid control valve for dispensing** | Fails open due to mechanical failure or human error | Release of $H_2$ from PRV to atmosphere at the end of dispensing | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| **Flow controller** | Fails open due to mechanical failure or human error | Release of $H_2$ from PRV to atmosphere | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| **PRV for dispensing** | Fails open due to mechanical failure | Release of $H_2$ from PRV to atmosphere | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | Fails to open at the set pressure | Release of $H_2$ due to system overpressure and line rupture | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |

Table 9: Risks and hazards associated with the hydrogen dispensing system

### 3.2.2 Hydrogen storage

Table 10 presents nine risks and hazards associated with hydrogen storage, which includes all three of the hazards that had a consequence severity of SEVERE/CATASTROPHIC. The most basic hazard encountered in hydrogen storage systems is a leak of hydrogen into the atmosphere due to mechanical failure of the storage system components. If it is not ignited, the hydrogen will simply dissipate into the atmosphere, and the expected consequence severity would be NEGLIGIBLE DAMAGE. However, if the leak is ignited at the source, the resulting jet fire would have a consequence severity of DAMAGE; this risk could be mitigated by closely controlling sources of sparks and ignition.

The most extreme release event would be complete tank failure due to a crash or other external impact, resulting in an uncontrolled release of hydrogen. This could result in a blast wave and fireball, with a consequence severity of SEVERE/CATASTROPHIC. This risk would need to be mitigated by designing tanks with suitable impact protection.

A related mechanism to the mechanical failures mentioned above are those related to thermal effects, either due to a localized fire or general overheating. Each hydrogen tank is equipped with TPRDs, which are designed to release hydrogen in a controlled manner when exposed to elevated temperatures. When functioning (either due to elevated temperature or mechanical failure), the release of hydrogen poses the same hazards as the leaks identified above. When the TPRD fails to operate, either due to a fire localized to a different part of the tank or a mechanical failure, uncontrolled release of hydrogen can result, accounting for two of the hazards with a consequence severity of SEVERE/CATASTROPHIC. These risks can be mitigated through the use of multiple TPRDs, as well as the provision of a fire detection system.

Previous research considered an unignited release to have an occurrence probability of OCCASIONAL, a failure of the TPRD(s) to operate in the event of fire or overheating to have an occurrence probability of IMPROBABLE, and all others to have an occurrence probability of REMOTE. Crash induced damage and localized fire received the highest risk ratings, in this study, of MEDIUM.

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| **On board storage tank** | Mechanical failure | Leak of $H_2$ to atmosphere | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | DAMAGE | LOW |
| | Crash induced damage or penetration by external object | Uncontrolled release of $H_2$ to atmosphere due to tank failure | Blast wave and fire ball | REMOTE | SEVERE / CATASTROPHIC | MEDIUM |
| **TPRD on storage tank** | Open due to mechanical failure | Release of $H_2$ from TPRD vent to atmosphere | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | REMOTE | MINOR DAMAGE | LOW |
| | Open in case of fire or overheating | Release of $H_2$ from TPRD vent to atmosphere | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | REMOTE | MINOR DAMAGE | LOW |
| | Inadequate tank/TPRD arrangement resulting in no TPRD actuation during localized fire | Uncontrolled release of $H_2$ due to tank rupture | Blast wave and fire ball | REMOTE | SEVERE / CATASTROPHIC | MEDIUM |
| | Mechanical failure resulting in TPRD failure to open during fire or excessive heat | Uncontrolled release of $H_2$ due to tank rupture | Blast wave and fire ball | IMPROBABLE | SEVERE / CATASTROPHIC | LOW |

Table 10: Risks and hazards associated with hydrogen storage

### 3.2.3 Fuel supply

Table 11 presents 12 risks and hazards associated with the fuel supply. The fuel supply incorporates safety systems, typically including one or more PRVs, pressure regulators, and a main shutoff valve. Failure of any one of these devices can result in a leak, which if ignited, would be expected to have a consequence severity of MINOR DAMAGE. If the leak occurs within an occupied compartment, there is an additional asphyxiation risk, although this can be mitigated through adequate ventilation. Whether the leak is into an occupied space or not, hydrogen buildup from a leak poses an explosion risk which could result in a consequence severity of MAJOR DAMAGE, which again can be mitigated by providing adequate ventilation of any enclosed compartments containing a fuel supply.

In the previous research, no risks with a consequence severity of DAMAGE were considered to have an occurrence probability higher than REMOTE; therefore all risks associated with this system were rated as LOW.

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| **Main shutoff valve for fuel supply** | Fail to close in case of leak | Release of $H_2$ to atmosphere from a break | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| **Pressure regulator for fuel supply to fuel cell** | Mechanical failure | Leak of $H_2$ to atmosphere | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the leak | REMOTE | MINOR DAMAGE | LOW |
| | Miss-adjustment or malfunction | Release of $H_2$ from PRV to atmosphere due to tank overpressure | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| **PRV for fuel supply to fuel cell** | Fails open due to mechanical failure | Release of $H_2$ from PRV to atmosphere | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the vent | REMOTE | MINOR DAMAGE | LOW |
| | Fails to open at the set pressure | Release of $H_2$ due to fuel cell overpressure and line rupture | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Asphyxiation hazard at the rupture | IMPROBABLE | DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| | | | Fire (delayed ignition of accumulated $H_2$) | REMOTE | DAMAGE | LOW |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | IMPROBABLE | MAJOR DAMAGE | LOW |

Table 11: Risks and hazards associated with the fuel supply

### 3.2.4 Fuel cell power plant

Table 12 presents the risks and hazards associated with the fuel cell power plant. Due to the complexity of this system, the presentation of the associated risks and hazards is broken down further below.

Fuel supply purging system

The purpose of the fuel supply purging system is to displace air (and thus oxygen) from the hydrogen fuel lines using an inert gas (e.g., nitrogen) before hydrogen fuel is introduced to the fuel cell. While the consequence severity of such an event would be DAMAGE, the occurrence probability of a mechanical, electrical, or control failure during this commissioning process is considered REMOTE; therefore, the risk was rated as LOW.

Fuel cell purge valve

The purpose of the fuel cell purge valve is to remove hydrogen when required due to excess water clogging the fuel cell channels. While this system is designed to vent hydrogen to a safe location, whenever the hydrogen is vented to the atmosphere there is always a risk of fire. The consequence severity of such an event would be MINOR DAMAGE. As this is a known venting location, the occurrence probability of an ignition source being present is considered REMOTE, therefore the risk was rated as LOW.

Fuel cell module

14 risks and hazards were associated with the fuel cell module. As with all other hydrogen carrying components, there exists a risk of leaks from the fuel cell due to mechanical failure. As with the other systems, an unignited release or jet fire would be expected to have a consequence severity of NEGLIGIBLE DAMAGE or MINOR DAMAGE respectively. However, there are the additional scenarios of a fire caused by delayed ignition within the cell, as well as an explosion from the same cause. These would be expected to have a consequence severity of DAMAGE in the case of fire, and MAJOR DAMAGE in the case of an explosion. An asphyxiation hazard also exists for personnel exposed to released hydrogen. Redundant ventilation systems can help mitigate the risks associated with hydrogen buildup, and impact protection can help mitigate the risk of mechanical failure due to an impact.

An unignited release of hydrogen due to mechanical failure was considered to have an occurrence probability of PROBABLE, an unignited release or jet fire due to impact was considered to have an occurrence probability of OCCASIONAL, with asphyxiation hazards considered to have an occurrence probability of IMPROBABLE. The remaining hazards were considered to have an occurrence probability of REMOTE; therefore, according to the risk matrix, all risks associated with the fuel cell module were rated as LOW.

Ventilation system

Three risks and hazards were associated with the ventilation system. As was discussed in the previous sections, a properly functioning ventilation system serves to mitigate the risks caused by hydrogen leaks throughout the vehicle. Failure of this system, therefore, raises those risks significantly, with fire having a consequence severity of DAMAGE, and asphyxiation and explosion both having a consequence severity of MAJOR DAMAGE. These risks can be mitigated through the design of redundancies in the ventilation system. This includes the use of a proven ventilation system (where it is assumed that if the air flow falls below a threshold limit, corrective action, such as shutting off the hydrogen flow at the earliest safe opportunity, is taken), as well as ensuring proper maintenance and thorough training of personnel. As with any hydrogen fire risk, limiting sources of sparking or ignition is also a method of risk mitigation.

Fire was considered to have an occurrence probability of OCCASIONAL, while explosion and asphyxiation were both considered to have an occurrence probability of REMOTE; therefore, all risks associated with the ventilation system were rated as LOW.

Oxidant conditioning

Mechanical, electrical, or control failure of the compressor supplying air to the fuel cell can result in membrane failure within the cell, possibly leading to a fire or explosion. This hazard could have a consequence severity of DAMAGE. Proper operator training and an appropriate maintenance schedule are mitigating measures for this type of risk.

Failure of this system has an occurrence probability of REMOTE; therefore the risk was rated as LOW.

Thermal management

As with hydrogen storage, if the thermal management of the fuel cell is not effective, it may experience a mechanical failure resulting in a fire or explosion, with a consequence severity of DAMAGE. This risk can be mitigated through appropriate maintenance, and provision of an automatic system for shutting down the fuel cell in case of excessive temperatures or a power failure.

Again, the failure of this system had an occurrence probability of REMOTE; therefore the risk was rated as LOW.

Automatic control system

Failure to appropriately manage power demand and distribution can lead to the failure of controlled components, overheating being a particular concern. Failure to shut off the supply of hydrogen following a fuel cell failure can lead to a buildup of gas, and a fire or explosion in the cell with a consequence severity of DAMAGE.

The occurrence probability of this hazard is considered REMOTE, therefore the risk was rated as LOW.

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| **Fuel supply purging system** | Mechanical, electrical, or control failure | Mix of $H_2$ and air inside the fuel cell system | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |
| **Fuel cell purge valve** | Mechanical, electrical, or control failure | Mix of $H_2$ and air at the purge valve outlet | Fire | REMOTE | MINOR DAMAGE | LOW |
| **Fuel cell module (inside an enclosure)** | Mechanical failure | Leak of $H_2$ from defect to the enclosure | Unignited release | PROBABLE | NEGLIGIBLE DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| | | | Fire (delayed ignition of accumulated $H_2$) | REMOTE | DAMAGE | LOW |
| | Fuel cell membrane break | Mix $H_2$ with air forming combustible gas | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |
| | Cell or vessel rupture due to freeze-up | Release of $H_2$ from the rupture to the enclosure | Unignited release | REMOTE | NEGLIGIBLE DAMAGE | LOW |
| | | | Asphyxiation hazard at the rupture | IMPROBABLE | DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | REMOTE | MINOR DAMAGE | LOW |
| | | | Fire (delayed ignition of accumulated $H_2$) | REMOTE | DAMAGE | LOW |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | REMOTE | MAJOR DAMAGE | LOW |

| Component | Cause | Mode | Result | Probability | Impact | Risk |
|---|---|---|---|---|---|---|
| | Impact damage | Release of $H_2$ from the damage to the enclosure | Unignited release | OCCASIONAL | NEGLIGIBLE DAMAGE | LOW |
| | | | Asphyxiation hazard at the rupture | IMPROBABLE | DAMAGE | LOW |
| | | | Jet fire (immediate ignition) at the break | OCCASIONAL | MINOR DAMAGE | LOW |
| | | | Fire (delayed ignition of accumulated $H_2$) | REMOTE | DAMAGE | LOW |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | REMOTE | MAJOR DAMAGE | LOW |
| **Ventilation system** | Electrical or mechanical fan failure; fan restriction due to foreign debris | Accumulation of $H_2$ from normal system leaks | Asphyxiation hazard in the enclosure | REMOTE | MAJOR DAMAGE | LOW |
| | | | Fire (delayed ignition of accumulated $H_2$) | OCCASIONAL | DAMAGE | LOW |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | REMOTE | MAJOR DAMAGE | LOW |
| **Oxidant conditioning - compressor for air supply to fuel cell** | Mechanical, electrical or control failure | Membrane failure due to abnormal pressure differential between the $H_2$ and air side | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |
| **Thermal management - cooling system** | Pump failure, cooling system line failure, etc. | Mix $H_2$ with air due to overheat fuel cell and membrane failure | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |
| **Automatic control system - power management for fuel cell** | Malfunction leading to fuel cell failure (e.g., overheating) | Release of $H_2$ if it is not shut off | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |
| **Automatic control system –fuel cell safety system** | Malfunction leading to fuel cell failure (e.g., cell reversal) | Cell overheating | Fire or explosion in the cell | REMOTE | DAMAGE | LOW |

Table 12: Risks and hazards associated with the fuel cell power plant

## 3.3 Summary of risks and hazards ratings

Of the 60 hazards that were identified and analyzed, only 3 had a consequence severity of SEVERE/CATASTROPHIC, 5 had a consequence severity of MAJOR DAMAGE, 14 had a consequence severity of DAMAGE, and 9 had a consequence severity of MINOR DAMAGE, with the remainder having a consequence severity of NEGLIGIBLE DAMAGE. Considering the occurrence probability of each of the hazards, and using the risk matrix presented in Table 6, only hydrogen storage contained two risks assessed as MEDIUM, and all other risks were assessed as LOW.

# 4 Highest risks and risk mitigation measures

## 4.1 Events considered

The events described in this section were considered in the risk register. Note that all of these events have a low likelihood.

### 4.1.1 Fire on board or around the rail vehicle

A fire on board or around the rail vehicle could be caused by locked wheels generating sparks, which could ignite dry flammable materials on the ground. Another possible scenario is over-heated brakes. The most vulnerable components in the event of a fire are the hydrogen storage containers, because they contain the highest pressure and have the highest hoop stress in the pressure vessel wall. Also, the heat from a fire reduces the tank material strength and increases the internal pressure at the same time (composite tanks are more susceptible yet). To address this risk, hydrogen storage tanks are fitted with TPRDs to prevent tank rupture as a result of the fire induced material degradation and tank internal pressure increase. These TPRDs are designed to relieve the tank's internal pressure (by allowing the hydrogen to escape to a safe location) in case of high temperatures or excessive pressures. If the TPRD fails to activate, the risk of tank rupture depends on the hydrogen tank resistance to fire (i.e., how long the tank can withstand the fire before it ruptures). A tank rupture would result in the fast release of hydrogen, which if ignited could produce a blast wave and a ball fire.

### 4.1.2 Derailment

Derailment can be the result of mechanical failure (e.g., wheel bearings, shaft, wheels), a collision with a foreign object, human error (e.g., speeding on a steep turn), track mechanical failure, etc. Derailment can result in hydrogen system damage leading to hydrogen release into the atmosphere and fire at the release point.

### 4.1.3 Crash with another object on the track

A crash with another object on the track could be the result of the train contacting another object at a railroad grade or level crossing. Usually, when trains collide at crossings, the railcars and any separated portions of the train take a long time to stop due to their high inertia. In addition, the initial impact or subsequent railcar motions may break locomotive components and result in a hydrogen leak that leads to a fire at the leak point.

### 4.1.4 Crash on the track with a vehicle carrying flammable dangerous goods

A train crash with a road vehicle that carries a flammable liquid (e.g., gasoline) may result in a gasoline spill around the train, which may ignite and surround the train in fire. The impact may also result in a hydrogen leak, which may intensify the fire. A similar situation may result from a derailment involving dangerous goods. However, the likelihood of this event is extremely low.

### 4.1.5 Excessive vibration

Excessive vibration may occur due to a mechanical failure or rail defect. This may also be the effect of normal vibration but inadequate hydrogen system mounting (inadequate damping system). These abnormal vibrations may subject the hydrogen system to vibrations beyond the design limits, causing

leaks (over time) and possible jet fires at the leak points. They may also cause the fuel cell to malfunction and cease operation.

### 4.1.6 Dispenser failure (resulting in over pressure)

A dispenser failure (resulting in over pressure) could be the result of a failure of the refueling system pressure sensors (there is one sensor upstream from the transfer point and another sensor downstream from the transfer point to stop the hydrogen flow when the rail tank has been filled). This could also be the result of a failure of the valve in the fueling nozzle (stuck open). However, the dispensing line also has a PRV to protect the rail tank against an over pressure. This could cause an on board TPRD activation. Failure of all the pressure relief devices in this sequence could result in tank over pressure. However, the likelihood of this event is extremely low.

## 4.2 Codes and standards mitigating factors

Existing codes and standards that have been developed by recognized experts can offer a means of mitigating risks inherent to the different components. Table 13 lists some of the relevant codes and standards that can be applied to hydrail locomotives, with reference to the respective tables from the codes and standards report [2] (where a full list of the relevant codes and standards can be found).

| Hydrail subsystem | Main components | Existing regulation, code, or standard title | Comments |
|---|---|---|---|
| Gaseous hydrogen dispensing | Dispensing nozzle | ISO 17268,<br>SAE J2600 | See Table 22: Standards for hydrogen dispensers in Ref. [2] |
| Vehicle (powered by $H_2$ fuel cell) | On board storage tank | CSA B51,<br>CSA/ANSI HGV 2,<br>ISO 19881,<br>IEC 63341-2 (not published) | See Table 24: Standards for hydrogen storage system and gas valve trains in Ref. [2] |
| | TPRD on storage tank on board (mandatory) | CSA/ANSI HPRD 1,<br>ISO 19882 | See Table 24: Standards for hydrogen storage system and gas valve trains in Ref. [2] |
| | Main shutoff valve for fuel supply (ex-tank) | CSA/ANSI HGV 3.1,<br>CSA C22.2 No. 139 | See Table 24: Standards for hydrogen storage system and gas valve trains in Ref. [2] |
| | Pressure regulator for fuel supply to fuel cell | CSA/ANSI HGV 3.1 | See Table 24: Standards for hydrogen storage system and gas valve trains in Ref. [2] |

| Hydrail subsystem | Main components | Existing regulation, code, or standard title | Comments |
|---|---|---|---|
| | PRV for fuel supply to fuel cell | CSA/ANSI HGV 3.1 | See Table 24: Standards for hydrogen storage system and gas valve trains in Ref. [2] |
| | Fuel cell power system (inside an enclosure) | IEC 62282-4-101, CSA/ANSI FC 1, ANSI/CSA AMERICA FC 3-2004, IEC 63341-1 (not published) | See Table 25: Standards for fuel cell power system and vehicle in Ref. [2] |
| | Fuel cell module | IEC 62282-4-101, CSA/ANSI FC 1, ANSI/CSA AMERICA FC 3-2004, IEC 63341-1 (not published) | See Table 26: Standards for fuel cell module in Ref. [2] |
| | Ventilation system | CSA/ANSI FC 1, ANSI/CSA AMERICA FC 3-2004 | See Table 27: Standards for ventilation system in Ref. [2] |
| | Compressor for air supply to fuel cell | ISO 4414, ISO 5388, CAN/CSA C22.2 No. 60335-2-34 | See Table 18: Standards for air compressors in Ref. [2] |
| | Cooling system | IEC 63341-1 (not published), CSA/ANSI FC 1, CSA C22.2 No. 62282-3-100, ANSI/CSA AMERICA FC 3-2004, IEC 62282-5-100, IEC 62282-4-101 | See Table 27: Standards for ventilation system in Ref. [2] |
| | Purge supply system | CSA B51, ASME B31.12, ASME BPVC, ASME STP-PT-006, NFPA 55, CGA S-1.1 | See Table 3: Standards for pressurized hydrogen containing or conveying components in Ref. [2] |
| | Power management (electrical/software) for fuel cell | CAN/CSA C22.2 No. 61511-1, CAN/CSA C22.2 No. 61508-1, UL 1998, UL 991 | See Table 11: Standards for control equipment and Table 12: Standards for functional safety in Ref. [2] |
| | Fuel cell safety system | CAN/CSA C22.2 No. 61511-1, CAN/CSA C22.2 No. 61508-1, UL 1998, UL 991 | See Table 11: Standards for control equipment and Table 12: Standards for functional safety in Ref. [2] |

Table 13: Mitigating codes and standards

## 4.3 Highest risks identified

Contemporary hydrogen equipment has fail safe redundant safety systems, which will stop the flow of hydrogen during hazardous events by closing safety solenoid hydrogen tank valves. Therefore, automated safety systems can mitigate the probability of a fire to an acceptable level. Similarly, in the case of attended operations, the system operator can also stop the hydrogen flow during hazardous events. However, in the case of a tank rupture no actions can be taken to stop the resulting uncontrolled hydrogen release. Furthermore, once the integrity of the tank is compromised, hydrogen can be released at large rates and, if ignition occurs, can result in high energy blast waves and fire balls. For these reasons, the highest risks identified in this study were all associated with a catastrophic hydrogen storage tank failure. This is due to the severity of such an event.

As hydrogen storage tanks are meticulously designed according to standards set out in Table 13, and tested and inspected, the most likely cause of a tank rupture is a crash event. The tank rupture could be caused by the crash itself or from foreign objects that impact the tanks. However, preventive measures can be taken to lower the risk of tank rupture during a crash. Table 14 includes the details of this scenario and lists some preventive measures.

| **Main components** | **Storage tank** |
|---|---|
| **Cause of failure** | Crash resulting in tank rupture from impact or by penetration of a foreign object |
| **Potential failure modes** | Hydrogen uncontrolled release |
| **Potential consequence of failure** | Blast wave and fire ball |
| **Level of frequency** | REMOTE (2) |
| **Level of severity** | SEVERE / CATASTROPHIC (5) |
| **Impact to workers** | YES |
| **Impact to the public** | YES |
| **Risk** | MEDIUM |
| **Preventative measures** | • Tank mounting can withstand adequate g-forces.<br>• Tank and piping connection are protected from impact (front, rear, sides and bottom).<br>• Tank and piping connection are protected from foreign object impact.<br>• Tanks and piping connection are protected during roll over scenarios.<br>• The tanks are not placed in the vehicle crushing zone.<br>• Simulation or crash testing should be performed. |
| **Comments supporting the ranking** | A crash is a major event |

Table 14: Ruptured storage tank hazard profile

If a hydrogen storage tank is subjected to a localized fire (where only a small part of the tank is subjected to a flame), and it is made of non-conductive materials, and if for any reason the heat and pressure does not activate the TPRD, it can break. This could happen if the tank and TPRD arrangement is not adequate. Table 15 includes the details of this scenario and lists some preventive measures.

| Main components | TPRD on storage tank |
|---|---|
| **Cause of failure** | Inadequate tank/TPRD arrangement resulting in no TPRD actuation during localized fire |
| **Potential failure modes** | Hydrogen uncontrolled release |
| **Potential consequence of failure** | Blast wave and fire ball |
| **Level of frequency** | REMOTE (2) |
| **Level of severity** | SEVERE / CATASTROPHIC (5) |
| **Impact to workers** | YES |
| **Impact to the public** | YES |
| **Risk** | MEDIUM |
| **Preventative measures** | • Two TPRDs per tank.<br>• Relief valves routed to a safe location away from other tanks.<br>• Tank/TPRD arrangement confirmed to relief during localized fire by testing.<br>• Fire detection. |
| **Comments supporting the ranking** | 1. An external localized fire is very unlikely.<br>2. A hydrogen localized prompted fire is very unlikely. |

Table 15: TPRD activation failure hazard profile

Hydrogen tanks can also break if the internal temperature or pressure increases and the TPRD fails to open. The overpressure could be the result of a fire that heats up the tank making the hydrogen gas pressure increase. Table 16 includes the details of this scenario and lists some preventive measures.

| Main components | TPRD on storage tank |
|---|---|
| **Cause of failure** | Mechanical failure resulting in TPRD failure to open during fire or excessive heat |
| **Potential failure modes** | Hydrogen uncontrolled release |
| **Potential consequence of failure** | Blast wave and fire ball |
| **Level of frequency** | IMPROBABLE (1) |
| **Level of severity** | SEVERE / CATASTROPHIC (5) |
| **Impact to workers** | YES |
| **Impact to the public** | YES |
| **Risk** | LOW |
| **Preventative measures** | • Two TPRDs per tank.<br>• Fire detection. |
| **Comments supporting the ranking** | Engulfing fires are most likely caused by external sources. |

Table 16: TPRD mechanical failure hazard profile

Hydrogen storage tank TPRDs can also fail by opening when they are not supposed to. This can also result in an uncontrolled release. However, the occurrence probability and the consequence severity were deemed to be REMOTE and MINOR. The reason for this is that TPRDs are vented to a safe location opened to the atmosphere where hydrogen tends to dilute very quickly due to its high diffusivity and buoyancy. However, such a failure inside an enclosed building was not considered in the study (because

of the uncertainty and variability of the different possible building structures) and thus operation in enclosed buildings, structures or tunnels where the locomotive can enter needs to be considered.

## 4.4 Risk mitigating factors

In this study it was assumed that risk mitigating measures such as those described herein (or better) are used. Therefore, it is assumed that the design and assembly of all components meet the following criteria:

- all components are correctly designed for the intended use and properly tested; and
- all components are installed, used and maintained within their tested and certified ratings, environmental conditions and service intervals.

It is also assumed that the following components or systems are used:

- thermal protection is used (as required) and tested to ensure it prevents hydrogen storage container rupture during exposure to fire;
- fire protection systems consisting of hydrogen gas detection and fire mitigating systems are in place;
- an adequate hydrogen vehicle fuel supply and control system is in place comprising:
    - pressure sensors that provide appropriate signals to the control system to manage the fuel supply system pressure; and
    - a flow meter that provides appropriate signals to the control system to manage the hydrogen flow to the fuel cell.
- fail-safe systems are used such that a single point failure of fuel shutoff systems do not result in fuel flow; and
- adequate overcurrent protection to prevent component failures and fires.

It is also assumed that the systems are appropriately tested as follows:

- tested for shock and vibration;
- tested for electromagnetic compatibility compliance;
- simulation or physical crash testing is performed to ensure some level of crash worthiness is assured for the hydrogen storage system, and to minimize the potential release of hydrogen in the event of a crash; and
- parts that are expected to be exposed to hydrogen including rail vehicle components are tested for hydrogen material compatibility.

Appendix A provides specific preventive measures for each component of the fuel dispensing system, hydrogen storage, fuel supply, and fuel cell power plant.

# 5 Gap analysis

Although the most important and consequential hydrogen components inside the locomotive are included in this study, only high level components were considered, and thus this study may have gaps in identifying and addressing some potential risks. Some risk identification gaps will be addressed in further studies, as these gaps (such as human factors) may require a more detailed system design to better understand the consequences of their failures. As well, this study did not address mitigation factors for risks where there are currently no well-established mitigating factors in existence today, and where, in order to address this gap, further literature reviews or physical testing will be required. As well, codes and standards need to be developed for North America to address all hazards and gaps in risk identification detailed in this report.

This study did not look into the following components and equipment as part of the risk analysis (it is expected that these systems and components will be addressed in future studies):

- ground equipment such as dispensers, hydrogen storage and compressors;
- fuel cell module safety management system (automatic control system);
- fuel cell module terminals and connections;
- pressure regulators;
- hydrogen sensing systems;
- liquid hydrogen;
- hydrogen valves; and
- lithium battery safety management.

As well, this study did not discuss potential mitigation factors for the risks associated with the proximity of lithium batteries to hydrogen storage and hydrogen fuel cell systems. The risk of batteries igniting and combusting during use or charging due to thermal runaway is real, as is the risk of a hydrogen leak resulting in a fire igniting the batteries and compounding the consequence of fire. This risk is complex, and this study did not identify any well-established mitigating factors relating to lithium batteries in proximity to hydrogen and fuel cell systems. It would be prudent to perform further literature review or to design and execute a physical testing program to better understand the risk that lithium battery thermal runaway poses to the hydrogen and fuel cell systems. More specifically, it is important to understand the probability and magnitude of a thermal runaway and the likelihood of propagation from cell to cell within the battery depending on the cell chemistry. A better understanding of the hazards arising from different lithium cell chemistries would lead to various mitigation factors and testing requirements that could be suggested to address those hazards.

The consequences of component failures depends on their location (and function) within the hydrogen gas distribution system. Therefore, some gaps in component risk require a more detailed understanding of the system design to better understand the consequences of their failures. Examples of these types of components include check valves and manual valves in the hydrogen distribution system.

As detailed in the associated codes and standards report [2], fuel cell and hydrogen storage standards specific to rail, that include the criteria to determine component adequacy for the North American

environment, are required. Similarly, lithium battery standards for all types of rail vehicles will need to be developed, as will codes, standards and regulations that address the required training for operators, maintenance staff, emergency responders, etc. Sections 5.1 to 5.9 briefly describe the main gaps identified above.

## 5.1 Ground equipment

Future studies on the hazards, and risk mitigation requirements for ground equipment related to locomotive operations and repairs are recommended. This should include shop related equipment as well as equipment required when performing repairs in the field, away from a shop environment. This equipment should also include hydrogen dispensers, compressors, hydrogen storage systems, electrolyzers and other relevant ground equipment that could be located in the train terminal refuelling station.

## 5.2 Fuel cell module safety management system (automatic control system)

Fuel cell modules have a safety management system that takes action when it detects a lower voltage in one of the cells or one group of cells (or by other means of measurement) to prevent cell reversal, which can result in a fire. Similarly, this system looks at other parameters to protect the fuel cell stack and to purge the system when necessary to get rid of excess water. The mitigating factor for a failure of this system must be thoroughly tested to the applicable standards from Tables 11 and 12 in the associated codes and standards report [2].

## 5.3 Fuel cell module terminals and connections

Terminals and connections of fuel cell equipment must be locked in place in a way that does not loosen with time due to vibration. This is very important to avoid excessive heat as well as sources of arcing or sparking close to the fuel cell stack, which is a source of hydrogen leaks. The mitigating factor for this is to have types of connectors approved by the authority having jurisdiction which are proven not to become loose due to vibration.

## 5.4 Check valves

From a system safety analysis point of view, the consequences of a check valve failure (either open or closed when unintended) need to be considered. The failure rates can vary depending on the design of each check valve and the type of media passing through it. Check valves may fail to seal properly in the closed position, or become stuck open with debris, or have excessively high or variable pressure drops. Depending on the system, the mitigating factors may include using certified check valves, and system design and monitoring.

## 5.5 Pressure regulators

The hydrogen labs at NRC Energy, Mining and Environment (EME) in Vancouver have experienced two incidents where the high pressure regulators have failed, allowing hydrogen to escape. Usually pressure regulators have a large surface area (as compared to other components) where seals are used, and thus they are more prone to fail in external leaks than other pieces of equipment or fittings. The mitigating factors for this type of failure include using certified regulators, properly classifying areas and using appropriate equipment for classified areas [22], having hydrogen sensing systems, using ventilation, and having a means to limit the flow of hydrogen.

## 5.6 Hydrogen sensing system

Hydrogen sensing systems employ sensors that often drift over time due to exposure to different vapours or dirt. The mitigating factors are to regularly clean and test and recalibrate if necessary (e.g., every 3 or 6 months). Similarly, they MUST be tested in the environment they will be serving (exposed to all foreseeable environmental elements) and certified to be adequate.

## 5.7 Manual valves

Manual valves are known to leak through the stem and regular inspection and maintenance is important to mitigate this. In addition, a well-designed ventilation system will dilute any leaks that occur to further mitigate the risk.

## 5.8 Liquid hydrogen

The current study only considered the use of gaseous hydrogen. It should be expanded to include liquid hydrogen as well. Liquid hydrogen brings new hazards related to the use of cryogenic liquids, such as spills, burns to people, material limitations at low temperatures and very wide temperature cycles (resulting in very limited service life), etc. Other factors related to liquid hydrogen (which has a boiling point of -252.9°C) include having oxygen liquefaction (oxygen has a boiling point of -183°C and nitrogen has a boiling point of -196°C) thus creating oxygen depleted atmospheres, as well as the fact that nitrogen does freeze at higher temperatures than oxygen (nitrogen has a freezing point of -210°C and oxygen has a freezing point of -218.8°C).

## 5.9 Lithium batteries

There are many hazards associated with lithium batteries, as detailed in the following sections. Their history from manufacturing to shipping to installation and use determine the likelihood of a failure. Failure modes include performance degradation, battery failure, cell venting and thermal runaway.

### 5.9.1 Lithium battery terminal connections

If connections to lithium battery terminals are not adequate, the added resistance can increase the temperature in the connection and battery terminal, which can heat up the cell adjacent to the battery

connection. This uneven temperature between battery cells can induce thermal abuse to cells, which eventually could degrade battery performance or its safety.

### 5.9.2 Battery management system

The battery management system is designed to protect lithium batteries during charging and discharging by avoiding:

- operation outside the cell working temperature range;
- cell overcharge;
- cell under discharge;
- excessive discharging rates; and
- excessive charging rates.

### 5.9.3 Overcurrent protection

External short circuits can overheat cells and increase the thermal runaway hazard. For this reason it is important to have adequate overcurrent protection in the electrical system.

### 5.9.4 Cooling system

The cooling system is the most important part to maintain battery safety. Overheating a lithium battery can result in battery degradation, failure or even thermal runaway resulting in a fire or explosion.

### 5.9.5 Lithium cells

Lithium cells are susceptible to entering a thermal runaway if overheated or crushed and ruptured during a crash, which can lead to a subsequent fire or explosion. Furthermore, unlike during a hydrogen fire, in a lithium battery fire the fuel cannot be stopped and the fire can spontaneously re-ignite even after the fire has been suppressed.

### 5.9.6 Vibration and shock

The user needs to ensure the battery can withstand the expected vibration and shock during the lifetime of the product.

# 6 Prioritizing and addressing gaps

Future studies should include the components and hazards presented in Section 5. The lithium battery system and the fuelling system should be a priority as this information is required for the current research being conducted by the University of British Columbia, Transport Canada and the NRC.

Table 17 includes the system and component gaps and the perceived need to prioritize each component (based on availability of standards, maturity of the technology, and perceived failure rates of the components). The codes and standards report [2] describes how to address the lack of existing Canadian codes and standards.

| Item No. | System location | System | Component | Perceived need to prioritize |
|---|---|---|---|---|
| 1 | Ground equipment | $H_2$ production | Electrolyzer | ISO standards exist and technology is not new (**Medium**) |
| 2 | Ground equipment | $H_2$ production | Hydrogen cooling system | (**Medium-High**) |
| 3 | Ground equipment | $H_2$ production | Purification and drying system | (**Medium-High**) |
| 4 | Ground equipment | $H_2$ production | Control system (electrical/ software) for safety device | Codes and standards exist for this. (**Medium**) |
| 5 | Ground equipment | $H_2$ storage | $H_2$ compressing system | (**Medium-High**) |
| 6 | Ground equipment | $H_2$ storage | Control system (electrical/software) for compressing system | (**Medium**) |
| 7 | Ground equipment | $H_2$ storage | Check valves | (**Medium-High**) |
| 8 | Ground equipment | $H_2$ storage | Manual valves | (**Medium**) |
| 9 | Ground equipment | $H_2$ storage | Hydrogen storage | (**Medium**) |
| 10 | Ground equipment | $H_2$ storage | Hydrogen storage TPRV | (**Medium**) |
| 11 | Ground equipment | $H_2$ storage | Hydrogen storage Shutoff solenoid valves | (**Medium-High**) |
| 12 | Ground equipment | $H_2$ storage for refuelling system | $H_2$ compressing system | (**Medium**) |
| 13 | Ground equipment | $H_2$ storage for refuelling system | PRV at compressor outlet | (**Medium-High**) |
| 14 | Ground equipment | $H_2$ storage for refuelling system | Control system (electrical/software) for compressing system | (**Medium**) |
| 15 | Ground equipment | $H_2$ storage for refuelling system | $H_2$ storage system tanks | (**Medium**) |

| Item No. | System location | System | Component | Perceived need to prioritize |
|---|---|---|---|---|
| 16 | Ground equipment | $H_2$ storage for refuelling system | Hydrogen storage TPRV | (**Medium**) |
| 17 | Ground equipment | $H_2$ storage for refuelling system | Hydrogen storage shutoff solenoid valves | (**Medium-High**) |
| 18 | Ground equipment | $H_2$ storage for refuelling system | Hydrogen storage manual valves | (**Medium**) |
| 19 | Ground equipment | Dispenser | Flow controller | (**Medium-High**) |
| 20 | Ground equipment | Dispenser | Piping | (**Medium**) |
| 21 | Ground equipment | Dispenser | Hose | (**Medium**) |
| 22 | Ground equipment | Dispenser | Nozzle | (**Medium-High**) |
| 23 | Ground equipment | Dispenser | Solenoid valve | (**Medium-High**) |
| 24 | Ground equipment | Dispenser | PRV | (**Medium**) |
| 25 | Rail vehicle | Fuel cell power plant | Fuel cell module safety management system | (**Medium-High**) |
| 26 | Rail vehicle | Fuel cell power plant | Fuel cell module terminals and connections | (**Medium**) |
| 27 | Rail vehicle | Fuel supply | Check valve | (**Medium-High**) |
| 28 | Rail vehicle | Fuel supply | Pressure regulator | (**Medium-High**) |
| 29 | Rail vehicle | Fuel supply | Manual valves | (**Medium**) |
| 30 | Rail vehicle | Fuel cell power plant | Hydrogen sensing system | (**Medium-High**) |
| 31 | Rail vehicle | Hydrogen storage | Hydrogen sensing system | (**Medium-High**) |
| 32 | Rail vehicle | Lithium battery | Lithium batteries terminal connections | (**High**) |
| 33 | Rail vehicle | Lithium battery | Battery management system | (**High**) |
| 34 | Rail vehicle | Lithium battery | Overcurrent protection | (**High**) |
| 35 | Rail vehicle | Lithium battery | Cooling system | (**High**) |
| 36 | Rail vehicle | Lithium battery | Lithium cells | (**High**) |
| 37 | Ground equipment | All | All - liquid hydrogen | (**Medium**) |
| 38 | Rail vehicle | All | All - liquid hydrogen | (**Medium**) |

Table 17: Prioritization of hydrail risk assessment gaps

# 7 Recommendations

The FMEA study was limited to the main components deemed to be most critical as per the reference design. However, it is recommended that future studies be expanded to include the ground equipment and missing rail vehicle components as described in this report. It is also recommended to have all the FMEA information transposed into a nationally recognized risk assessment framework such *as ISO 31000:2018: Risk management - Guidelines*. It is also recommended that the FMEA information be evaluated in the context of guidelines that are specific to machinery and rail such *as ISO 12100:2010: Safety of machinery - General principles for design - Risk assessment and risk reduction*, or *CSA EXP11:20: Canadian method for risk evaluation and assessment for railway systems*.

Putting the knowledge generated from the FMEA work into standardized frameworks will help to set up more formal processes for examining and evaluating risk between operators and safety regulators. The codes and standards listed in Section 4.2 of this report can be leveraged in the short term as mitigating factors for the applicable rail components including the fuel cell power plant and hydrogen storage system. The companion codes and standards report [2] describes how to leverage existing compressed natural gas and liquefied natural gas standards for hydrogen. That report also lists relevant lithium battery standards that can be leveraged for hydrogen rail vehicles.

The knowledge gathered here should be applied to a project which uses lithium battery and hydrogen fuel cells as a demonstration program to gain real-world experience with the physical apparatus. This will ensure that components and hazards which were not discussed in this report are included, and that the most relevant components and the highest identified risks are confirmed. Also, this will ensure that the risk mitigation measures described in this report are practical and effective at reducing the hazards to acceptable levels in an actual installation.

Similarly, having an actual installation can be used to ensure that the application of the referenced codes and standards is feasible, does not result in conflicts and is effective at lowering the risks. It is very likely that deviations from the referenced codes and standards will be necessary in an actual installation as some of the referenced documents may not be applicable to freight rail applications. All required deviations should be noted and be included in a feedback loop to the standards development organizations working on rail standards.

Future follow up work should also include determining an acceptable proximity or a fire barrier and adequate atmospheric pressure differential between the lithium batteries with respect to the fuel cell system and hydrogen storage, so that a failure in either system does not compromise the other system. In other words, a hydrogen leak should not migrate to the lithium battery enclosure and a lithium battery thermal runaway or fire should not result in a hydrogen fire. However, this proximity should be deemed safe in an actual installation so that acceptable methods to develop the distance or barrier requirements are confirmed and tested.

# 8 Conclusions

In order to assess the risks and hazards associated with the operation of hydrogen fuel cell and battery powered (hydrail) locomotives, an FMEA risk analysis was conducted, focusing on the risks and hazards introduced due to the fuel-cell, hydrogen, and battery systems.

The highest risk was associated with damage to the hydrogen storage system, potentially due to a TPRV failing to open during a fire, or due to the impact from a crash. Modern hydrogen equipment has fail safe redundant safety systems, which will stop the flow of hydrogen during hazardous events by closing safety solenoid hydrogen tank valves. Therefore, automated safety systems can mitigate the probability of a fire to an acceptable level. However, in the case of a tank rupture, there are no actions that can be taken to stop the resulting uncontrolled hydrogen release, which could result in events with a high consequence severity. Nevertheless, there are mitigating measures that can be taken to lower the risk as described in Appendix A. These measures include tank mounting that can withstand adequate *g*-forces, tank and piping connections are protected from impact due to a crash or due to foreign objects, simulation or crash testing to ensure tank protection and location away from the vehicle crushing zone, tank/TPRD arrangement confirmed to relieve pressure during localized fire by testing, redundant TPRVs per tank, etc.

It is assumed that the fuel cell power plant and ancillaries use appropriate components and systems to mitigate their risks. These include the use of components evaluated for shock, vibration, electromagnetic compatibility, etc. This also includes using fail safe systems and meticulously tested control systems (hardware and software).

Hydrogen storage tank TPRDs can also fail by opening when they are not supposed to. This can result in an uncontrolled release. However, TPRDs are vented to a safe location open to the atmosphere, where hydrogen tends to dilute very quickly due to its high diffusivity and buoyancy. Nevertheless, such a failure inside an enclosed building was not considered in the study and thus operation in enclosed buildings, structures or tunnels, where the locomotive can enter, needs to be considered.

Because this study did not involve an actual hydrail system design, the FMEA was limited to a high level reference design and only included the main components deemed to be most critical. The high level FMEA proved to be a good method to understand risks and to rank them. However, it is important to expand this work to include more hydrogen and fuel cell components as well as the lithium battery (to close some of the gaps in this current study). Similarly, it is recommended that a risk analysis (such as an FMEA) be conducted on an actual installation in the future to understand all the details and to confirm the findings.

The next steps should include addressing the identified gaps in the risk assessment as well as applying the gathered knowledge to a project involving an actual lithium battery hydrogen fuel cell demonstration program to gain real-world experience with the physical apparatus. As well, determining an acceptable proximity, a fire barrier design, or an adequate pressure differential, between the lithium batteries and the fuel cell and hydrogen storage systems is required, as there are no current standards which define this.

# Acronyms and abbreviations

| | |
|---|---|
| ANSI | American National Standards Institute |
| ASME | American Society of Mechanical Engineers |
| CGA | Compressed Gas Association |
| CNL | Canadian Nuclear Laboratories |
| CSA | Canadian Standards Association |
| FMEA | failure modes and effects analysis |
| FTA | fault tree analysis |
| HAZID | hazard identification |
| HAZOP | hazard and operability analysis |
| HVAC | heating, ventilation and air conditioning |
| IEC | International Electrotechnical Commission |
| ISO | International Standards Organization |
| NFPA | National Fire Protection Association |
| NRC | National Research Council of Canada |
| PRA | probabilistic risk assessment |
| PRV | pressure relief valve |
| QRA | quantitative risk assessment |
| RPN | risk priority number |
| SAE | Society of Automotive Engineers |
| TPRD | thermal pressure relief device |
| TPRV | thermal pressure relief valve |
| UL | Underwriters Laboratories |

# References

[1] M. Hernandez, I. Jimenez, D. Chuang, E. Toma and S. Mackie, "Risk assessment of hydrogen and battery power in locomotives - Part 1 - Literature review," National Research Council of Canada, Ottawa, 2022.

[2] M. Hernandez, C. Rabbitt, I. Jimenez and E. Toma, "Risk assessment of hydrogen and battery power in locomotives - Part 3 - Codes and standards," National Research Council of Canada, Ottawa, 2022.

[3] P. Connor, "Diesel locomotives," The Railway Technical Website, 2019. [Online]. Available: http://www.railway-technical.com/trains/rolling-stock-index-l/diesel-locomotives/.

[4] Railway Association of Canada, "Railway emergency awarness guide," Railway Association of Canada, 2017.

[5] R. J. Irwin, "Environmental contaminents encyclopedia references entry a listing of references by number," National Park Service, Fort Collins, 1997.

[6] Canadian Centre for Occupational Health and Safety, "Diesel exhaust: hazardous to your health," Canadian Centre for Occupational Health and Safety, 04 November 2022. [Online]. Available: https://www.ccohs.ca/newsletters/hsreport/issues/2012/06/ezine.html.

[7] U.S. Battery, "Safety data sheet lead-acid battery, wet electrolyte (sulfuric acid)," U.S. Battery Manufacturing Company, Corona, 2020.

[8] M. Hernandez, "Hydrogen safety protocol - H2 safety training," in *Nationa Research council of Canada*, 2018.

[9] R. W. Schefer, W. G. Houf, C. San Marchi, W. P. Chernicoff and L. Englom, "Characterization of leaks from compressed hydrogen dispensing systems and related components," *International Journal of Hydrogen Energy,* vol. 31, no. 9, pp. 1247-1260, 2006.

[10] H. Barthélémy, "Effects of pressure and purity on the hydrogen embrittlement of steels," *International Journal of Hydrogen Energy,* vol. 36, no. 3, pp. 2750-2758, 2011.

[11] V. S. Raja and T. Shoji, Stress corrosion cracking: theory and practice, Elsevier, 2011.

[12] R. Rhodes, "Explosive lessons in hydrogen safety," *ASK Magazine of NASA,* p. 46, 2011.

[13] International Organization for Standardization, *ISO/TS 15869:2009 - Gaseous hydrogen and hydrogen blends - Land vehicle fuel tanks,* International Organization for Standardization, 2009.

[14] International consortium for fire safety, health and the environment, *Safety issues regarding fuel cell vehicles and hydrogen fueled vehicles,* International consortium for fire safety, health and the environment.

[15] K. Fatih, M. Hernandez and M. Rossetto, "Lithium battery transport study: canadian risk perspective," National Research Council Canada, Vancouver, 2014.

[16] D. Stephens, P. Shawcross, G. Stout, E. Sullivan, J. Saunders, S. Risser and J. Sayre, "Lithium-ion battery safety issues for electric and plug-in hybrid vehicles," NHTSA, Columbus, 2017.

[17] Thermal Hazard Technology, "Safety studies on lithium batteries using the accelerated calorimeter," Thermal Hazard Technology, Edinburg, UK, 1998.

[18] B. Lawson, "Electropaedia," Woodbank Communications Ltd, 2005. [Online]. Available: www.electropaedia.com.

[19] Pacific Northwest National Laboratory, *Safety planning for hydrogen and fuel cell projects,* United State Department of Energy, 2020.

[20] Canadian Nuclear Laboratories; Tchouvelev & Associates Inc., A.V.; Canadian Standards Association; National Research Council of Canada, *Metrolinx Study,* Unpublished, 2015.

[21] Transportation Safety Board of Canada, "Data and statistics on rail transportation occurrences," Transportation Safety Board of Canada, [Online]. Available: http://www.bst-tsb.gc.ca/eng/stats/rail/.

[22] Canadian Standards Association, *Canadian Electrical Code - Part 1 - Safety standard for electrical installations,* Canadian Standards Association, 2021.

[23] Quincy Compressor, "Full guide to air compressor safety," Quincy Compressor, 23 September 2015. [Online]. Available: https://www.quincycompressor.com/tips-for-working-safely-with-compressed-air/#common-air-compressor-hazards.

# Appendix A: Hydrogen fuel cell risk mitigating factors

Table A-1: Fuel dispensing system

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| **Dispensing piping** | Leak due to mechanical failure | Leak of $H_2$ to atmosphere during dispensing | Unignited release | LOW | Preventive measures:<br>1. Adequate components:<br>1.1 Qualified components (including piping) pressure tested and capable of withstanding the fluid media ($H_2$).<br>2. Avoiding flammable concentrations:<br>2.1 Proved ventilation.<br>2.2 All components are leak tested.<br>2.3 Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>3. Avoiding ignition sources:<br>3.1 Area classification in confined spaces where hydrogen can accumulate (adequately rated equipment used in this areas as well as non-arching non-sparking equipment).<br>3.2 Compliance with NFPA 77 to avoid static electricity buildup.<br>4. Automatic Emergency Shutoff Systems:<br>4.1 Automatic emergency shutoff system with redundant shutoff valves.<br>4.2 Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>5. Automatic Safety Systems:<br>5.1 Hydrogen gas sensing system connected to the alarm and fuel shutoff system.<br>5.2 Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>5.3 Flame sensing system.<br>6. Hydrogen Flow Limiting Devices:<br>6.1 Flow restrictors to limit the maximum hydrogen that can be released.<br>7. Emergency E-Stop Next to Dispenser. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Adequate components:<br>1.1 Qualified components (including piping) pressure tested and capable of withstanding the fluid media ($H_2$).<br>2. Avoiding flammable concentrations:<br>2.1 Proved ventilation.<br>2.2 All components are leak tested.<br>2.3 Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>3. Avoiding ignition sources:<br>3.1 Area classification in confined spaces where hydrogen can accumulate (adequately rated equipment used in this areas as well as non-arching non-sparking equipment).<br>3.2 Compliance with NFPA 77 to avoid static electricity buildup.<br>4. Automatic Emergency Shutoff Systems:<br>4.1 Automatic emergency shutoff system with redundant shutoff valves.<br>4.2 Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>5. Automatic Safety Systems:<br>5.1 Hydrogen gas sensing system connected to the alarm and fuel shutoff system.<br>5.2 Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>5.3 Flame sensing system.<br>6. Hydrogen Flow Limiting Devices:<br>6.1 Flow restrictors to limit the maximum hydrogen that can be released.<br>7. Emergency E-Stop Next to Dispenser. |
| **Dispensing hose** | Leak due to mechanical failure | Leak of $H_2$ to atmosphere during dispensing | Unignited release | LOW | Preventive measures:<br>1. Qualified hose, pressure tested and validated to an appropriate number of cycles. CSA/ANSI HGV4.2, Host and Hose Assemblies for Hydrogen Vehicles and Dispensing Systems.<br>2. Periodical replacement of the hose to ensure staying within cycle limits with sufficient safety factor.<br>3. Grounding the hose to avoid static electricity.<br>4. Flow restrictors to limit the maximum hydrogen that can be released.<br>5. Automatic emergency shutoff system with redundant shutoff valves.<br>6. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>7. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>8. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>9. Flame sensing system.<br>10. Outdoors location will dilute hydrogen leaks fast lowering the probability of a fire.<br>11. Emergency E-Stop Next to Dispenser. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Qualified hose, pressure tested and validated to an appropriate number of cycles.<br>2. Periodical replacement of the hose to ensure staying within cycle limits with sufficient safety factor.<br>3. Grounding the hose to avoid static electricity.<br>4. Flow restrictors to limit the maximum hydrogen that can be released.<br>5. Automatic emergency shutoff system with redundant shutoff valves.<br>6. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>7. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>8. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>9. Flame sensing system connected to the automatic emergency shutoff system.<br>10. Outdoors location will dilute hydrogen leaks fast lowering the probability of a fire.<br>11. Emergency E-Stop Next to Dispenser. |
| | Drive-away while connected with the nozzle | Stop $H_2$ flow due to activation of breakaway device | Unignited small release | LOW | Preventive measures:<br>1. Breakaway hose coupling device will shut the hydrogen flow.<br>2. Flow restrictors to limit the maximum hydrogen that can be released.<br>3. Automatic emergency shutoff system with redundant shutoff valves.<br>4. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>5. Flame sensing system connected to the automatic emergency shutoff system. |
| **Dispensing nozzle** | O-ring or nozzle damaged | Leak of $H_2$ to atmosphere during dispensing | Unignited release | LOW | Preventive measures:<br>1. Nozzle (compliant with SAE J2600[4] and SAE J2799).<br>2. Grounding the hose to avoid static electricity.<br>3. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>4. Flow restrictors to limit the maximum hydrogen that can be released.<br>5. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>6. Automatic emergency shutoff system with redundant shutoff valves.<br>7. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>8. Flame sensing system.<br>9. Outdoors location will dilute leaks fast.<br>10. Emergency E-Stop Next to Dispenser. |

[4] Compressed Hydrogen Surface Vehicle Fueling Connection Devices 201510.

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Nozzle (compliant with SAE J2600[5] and SAE J2799).<br>2. Grounding the hose to avoid static electricity.<br>3. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>4. Flow restrictors to limit the maximum hydrogen that can be released.<br>5. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>6. Automatic emergency shutoff system with redundant shutoff valves.<br>7. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>8. Flame sensing system.<br>9. Outdoors location will dilute leaks fast.<br>10. Emergency E-Stop Next to Dispenser. |
| **Solenoid control valve for dispensing** | Fails open due to mechanical failure or human error | Release of $H_2$ from PRV to atmosphere at the end of dispensing | Unignited release | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Pressure monitoring<br>3. PRV vented to a safe location.<br>4. Emergency E-Stop Next to Dispenser. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Pressure monitoring.<br>3. PRV vented to a safe location.<br>4. Emergency E-Stop Next to Dispenser. |
| **Flow controller** | Fails open due to mechanical failure or human error | Release of $H_2$ from PRV to atmosphere | Unignited release | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Pressure monitoring<br>3. PRV vented to a safe location.<br>4. Emergency E-Stop Next to Dispenser. |
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Pressure monitoring<br>3. PRV vented to a safe location.<br>4. Emergency E-Stop Next to Dispenser. |
| **PRV for dispensing** | Fails open due to mechanical failure | Release of $H_2$ from PRV to atmosphere | Unignited release | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>3 Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>4. PRV vented to a safe location.<br>5. Emergency E-Stop Next to Dispenser. |

[5] Compressed Hydrogen Surface Vehicle Fueling Connection Devices 201510.

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. Automatic emergency shutoff system with redundant shutoff valves.<br>2 Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>3 Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>4. PRV vented to a safe location.<br>5. Emergency E-Stop Next to Dispenser. |
| | Fails to open at the set pressure | Release of $H_2$ due to system overpressure and line rupture | Unignited release | LOW | Preventive measures:<br>1. Grounding components to avoid static electricity.<br>2. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>3. Flow restrictors to limit the maximum hydrogen that can be released.<br>4. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>5. Automatic emergency shutoff system with redundant shutoff valves.<br>6. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>7. Flame sensing system.<br>8. Emergency E-Stop Next to Dispenser. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Grounding components to avoid static electricity.<br>2. Automatic leak test (of the dispenser, hose and nozzle) before and during filling.<br>3. Flow restrictors to limit the maximum hydrogen that can be released.<br>4. Pressure monitoring (capable of detecting abnormal pressure drop due to a leak).<br>5. Automatic emergency shutoff system with redundant shutoff valves.<br>6. Adequate automatic fuel shutoff system time to stop hydrogen flow in case of leaks.<br>7. Flame sensing system.<br>8. Emergency E-Stop Next to Dispenser. |

Table A-2: Hydrogen storage

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| **On board storage tank** | Mechanical failure | Leak of $H_2$ to atmosphere | Unignited release | LOW | Preventive measures:<br>1. No ignition sources.<br>2. Ventilation.<br>3. Pre purge before start-up (5 air changes). |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. No ignition sources. |
| | Crash induced damage or penetration by external object | Uncontrolled release of $H_2$ to atmosphere due to tank failure | Blast wave and fire ball | MEDIUM | Preventive measures:<br>1. Tank mounting can withstand adequate Gg-forces.<br>2. Tank and piping connection are protected from impact (front, rear, sides and bottom).<br>3. Tank and piping connection are protected from foreign object impact.<br>4. Tanks and piping connection are protected during roll over scenarios.<br>5. The tanks are not placed in the vehicle crushing zone.<br>6. Simulation or crash testing should be conducted. |
| **TPRD on storage tank** | Open due to mechanical failure | Release of $H_2$ from TPRD vent to atmosphere | Unignited release | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | Open in case of fire or overheating | Release of $H_2$ from TPRD vent to atmosphere | Unignited release | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | Inadequate tank/TPRD arrangement resulting in no TPRD actuation during localized fire | Uncontrolled release of $H_2$ due to tank rupture | Blast wave and fire ball | MEDIUM | Preventive measures:<br>1. Two TPRDs per tank<br>2. Relief valves routed to a safe location away from other tanks.<br>3. Tank/TPRD arrangement confirmed to relief during localized fire by testing.<br>4. Fire detection.<br>Other factors:<br>1. An external localized fire is very unlikely in a well-designed system.<br>2. A hydrogen localized prompted fire is very unlikely. |
| | Mechanical failure resulting in TPRD failure to open during fire or excessive heat | Uncontrolled release of $H_2$ due to tank rupture | Blast wave and fire ball | LOW | Preventive measures:<br>1. Two TPRDs per tank.<br>2. Fire detection.<br>Other factors:<br>1. Engulfing fires are most likely caused by external sources. |

Table A-3: Fuel supply

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| **Main shutoff valve for fuel supply** | Fail to close in case of leak | Release of $H_2$ to atmosphere from a break | Unignited release | LOW | Preventive measures:<br>1. Two valves in series for redundancy.<br>2. Active proved ventilation.<br>3. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>4. Area classification<br>5. Adequate equipment used in classified areas.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Two valves in series for redundancy.<br>2. Active proved ventilation.<br>3. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>4. Area classification<br>5. Adequate equipment used in classified areas.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| **Pressure regulator for fuel supply to fuel cell** | Mechanical failure | Leak of $H_2$ to atmosphere | Unignited release | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Jet fire (immediate ignition) at the leak | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | Miss-adjustment or malfunction | Release of $H_2$ from PRV to atmosphere due to tank overpressure | Unignited release | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| **PRV for fuel supply to fuel cell** | Fails open due to mechanical failure | Release of $H_2$ from PRV to atmosphere | Unignited release | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | | | Jet fire (immediate ignition) at the vent | LOW | Preventive measures:<br>1. TPRD are vented to an open air high safe location pointing away from the vehicle.<br>2. TPRD vent lines compliant with CGA G 5.5. |
| | Fails to open at the set pressure | Release of $H_2$ due to fuel cell overpressure and line rupture | Unignited release | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Asphyxiation hazard at the rupture | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Hydrogen sensor(s) connected to alarm and fuel shutoff system. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Fire (delayed ignition of accumulated $H_2$) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

Table A-4: Fuel cell power plant

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| **Fuel supply purging system** | Mechanical, electrical, or control failure | Mix of $H_2$ and air inside the fuel cell system | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Controls compliant with applicable standards for controls (Table 11 in [2]) and functional safety (Table 12 in [2]).<br>2. Standard procedures. |
| **Fuel cell purge valve** | Mechanical, electrical, or control failure | Mix of $H_2$ and air at the purge valve outlet | Fire | LOW | Preventive measures:<br>1. Purge valves are vented to a safe location pointing away from the vehicle.<br>2. Purge valve vent lines compliant with CGA G 5.5.<br>3. Area classification<br>4. Adequate equipment used in classified areas. |
| **Fuel cell module (inside an enclosure)** | Mechanical failure | Leak of $H_2$ from defect to the enclosure | Unignited release | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Fire (delayed ignition of accumulated H2) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | Fuel cell membrane break | Mix $H_2$ with air forming combustible gas | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Fuel cell safety system will detect low voltage and shut the hydrogen flow.<br><br>Other factors:<br>1. It is very unlikely that the membrane will completely break and will most likely start by exposing a small volume of hydrogen and air. The temperature would go up and the voltage would go down as the air and hydrogen mix and local fire could start. |
| | Cell or vessel rupture due to freeze-up | Release of $H_2$ from the rupture to the enclosure | Unignited release | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Asphyxiation hazard at the rupture | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Hydrogen sensor(s) connected to alarm and fuel shutoff system. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Fire (delayed ignition of accumulated H2) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | Impact damage | Release of $H_2$ from the damage to the enclosure | Unignited release | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s).<br>6. Impact sensing system that stops fuel flow and removes electrical power.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Asphyxiation hazard at the rupture | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br>4. Impact sensing system that stops fuel flow and removes electrical power. |
| | | | Jet fire (immediate ignition) at the break | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s) connected to the alarm and fuel shutoff system.<br>6. Impact sensing system that stops fuel flow and removes electrical power.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| | | | Fire (delayed ignition of accumulated $H_2$) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s).<br>6. Impact sensing system that stops fuel flow and removes electrical power.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | LOW | Preventive measures:<br>1. Active proved ventilation.<br>2. Flow limiting devices. An excess flow valve will shut the hydrogen flow in case of larger leaks.<br>3. Area classification<br>4. Adequate equipment used in classified areas.<br>5. Hydrogen sensor(s).<br>6. Impact sensing system that stops fuel flow and removes electrical power.<br><br>Other factors:<br>1. Low probability of ignition if ventilation reduces $H_2$ concentration below 25% of the LFL. |
| **Ventilation system** | Electrical or mechanical fan failure; fan restriction due to foreign debris | Accumulation of $H_2$ from normal system leaks | Asphyxiation hazard in the enclosure | LOW | Preventive measures:<br>1. The ventilation must be proved so that failures are detected. A certified sail switch or equivalent means can be used.<br>2. The sail switch should close the circuit when sufficient flow is established and open the circuit when the flow goes below a safe value.<br>3. Hydrogen sensor(s) connected to the alarm and fuel shutoff system. |
| | | | Fire (delayed ignition of accumulated $H_2$) | LOW | Preventive measures:<br>1. The ventilation must be proved so that failures are detected. A certified sail switch or equivalent means can be used.<br>2. The sail switch should close the circuit when sufficient flow is established and open the circuit when the flow goes below a safe value.<br>3. Hydrogen sensor(s) connected to the alarm and fuel shutoff systems. |
| | | | Explosion (delayed ignition of accumulated $H_2$ in confined space) | LOW | Preventive measures:<br>1. The ventilation must be proved so that failures are detected. A certified sail switch or equivalent means can be used.<br>2. The sail switch should close the circuit when sufficient flow is established and open the circuit when the flow goes below a safe value.<br>3. Hydrogen sensor(s) connected to the alarm and fuel shutoff system. |

| Component | Cause | Mode | Result | Risk | Mitigating factors |
|---|---|---|---|---|---|
| **Oxidant conditioning - compressor for air supply to fuel cell** | Mechanical, electrical or control failure | Membrane failure due to abnormal pressure differential between the $H_2$ and air side | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Compressor pressure relief device activation.<br>2. Stack leak before rupture design.<br>2. Fuel cell safety system will detect low voltage and shut the hydrogen flow.<br>3. Fuel cell safety system will detect Fuel cell stack high temperature and shut the hydrogen flow. |
| **Thermal management - cooling system** | Pump failure, cooling system line failure, etc. | Mix $H_2$ with air due to overheat fuel cell and membrane failure | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Fuel cell safety system will detect low voltage and shut the hydrogen flow.<br>2. Fuel cell safety system will detect Fuel cell stack high temperature and shut the hydrogen flow. |
| **Automatic control system - power management for fuel cell** | Malfunction leading to fuel cell failure (e.g., overheating) | Release of $H_2$ if it is not shut off | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Fuel cell safety system will detect low voltage and shut the hydrogen flow.<br>2. Fuel cell safety system will detect Fuel cell stack high temperature and shut the hydrogen flow.<br>3. Controls compliant with applicable standards for controls (Table 11 in [2]) and functional safety (Table 12 in [2]). |
| **Automatic control system –fuel cell safety system** | Malfunction leading to fuel cell failure (e.g., cell reversal) | Cell overheating | Fire or explosion in the cell | LOW | Preventive measures:<br>1. Controls compliant with applicable standards for controls (Table 11 in [2]) and functional safety (Table 12 in [2]).<br>2. Redundant hard wired temperature sensor(s) or other sensors as required. |

*This page intentionally left blank*

NRC.CANADA.CA • INFO@NRC-CNRC.GC.CA • 877-672-2672 •