Proceedings of the 2017 Joint Rail Conference
JRC2017
April 4-7, 2017, Philadelphia, PA, USA

JRC2017-2275

FAILURE ANALYSIS OF LNG RAIL LOCOMOTIVES

Chris B. LaFleur
Sandia National Laboratories
Albuquerque, NM, USA

Alice B. Muna
Sandia National Laboratories
Albuquerque, NM, USA

Katrina M. Groth
Sandia National Laboratories
Albuquerque, NM, USA

Matthew St. Pierre
Sandia National Laboratories
Albuquerque, NM, USA

Melissa Shurland
Federal Railroad Administration
Washington D.C., USA

ABSTRACT

This paper presents a risk assessment of a Liquefied Natural Gas (LNG)/diesel hybrid locomotive to identify and rank failures that could result in the release of LNG or Gaseous Natural Gas (GNG) to the surrounding environment. The Federal Railroad Administration (FRA) will analyze industry safety assessments of the proposed rail vehicles and the goal of this risk analysis is to identify and prioritize hazard scenarios so the FRA can ensure that they are properly addressed. For operational activities, a Failure Modes and Effects Analysis (FMEA) was performed to identify high risk failure modes. A modified hazard and operability study (HAZOP) methodology was used to analyze hazard scenarios for the maintenance activities for the LNG and Compressed Natural Gas (CNG) dual-fuel locomotives and the LNG tender car. Because refueling operations are highly dependent on human interactions, a human factors assessment was also performed on a sample refueling procedure to identify areas of improvement and identify best practices for analyzing future procedures.

The FMEA resulted in the identification of 87 total failure modes for the operational phase, three of which were deemed to have a High risk priority, all involving the cryogenic storage tank. The HAZOP for the LNG tender resulted in the identification of eight credible hazard scenarios and the HAZOP for the locomotive in the maintenance mode identified 27 credible hazard scenarios. The high and medium risk failure modes and hazard scenarios should be prioritized for further analysis.

INTRODUCTION

Recently, restrictive emissions requirements and historically low natural gas prices have resulted in efforts to develop a fleet of dual-fueled Liquefied Natural Gas (LNG)/diesel hybrid locomotives. The Federal Railroad Administration (FRA) is responsible for making defensible regulatory decisions in response to the safety assessments of the proposed rail vehicles in a timely manner. As a result, the FRA has partnered with Sandia National Laboratories (Sandia) on research activities that will assess the safety of using natural gas as a locomotive fuel.

FMEA METHODOLOGY FOR OPERATIONAL ACTIVITIES

Failure Modes and Effects Analysis (FMEA) is a qualitative, inductive process used to identify the effect of component failures on subsystems and systems. It is important to follow an established, standardized FMEA methodology to ensure that the FMEA process is sufficiently rigorous. There are several different FMEA methodologies; most adhere to a similar process, with the main differences stemming from the target industry, how the method handles varying degrees of design maturity and how the severity, probability and criticality are handled and prioritized.

Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 5580, titled “Recommended Failure Modes and Effects Analysis Practices or Non-Automobile Application,” is an appropriate methodology for the

FRA application [1]. Specifically, a Product Design Hardware FMEA provides a top-down functional and interface FMEA based on the state of the developing technology and available information about the detailed design of the dual-fueled LNG and diesel locomotive tender. The SAE ARP 5580 document provides the basic, common process, evolved from the Military Standard, and reflects improvements made to the process over time [2]. The SAE ARP 5580 methodology effectively considers different levels of analysis based on the maturity of the system design and articulates the evolution of the FMEA process. Because of its ability to deal with significant uncertainty in the design of a new technology, this method is particularly attractive for the LNG and diesel dual-fuel locomotive application. The purposes of a functional FMEA are to support the functional assessment of system architecture and to identify critical functions for more detailed analysis.

The FMEA focused on the LNG tender system during the operation phase. The only failures considered were the release of natural gas (in any form) from any part of the LNG tender system. No other failures were identified or evaluated. The analysis focused on systems where direct release of LNG or Gaseous Natural Gas (GNG) was possible. Failure modes in the other units may lead indirectly to a release of Natural Gas (NG) by causing an accident or derailment. This analysis, however, dealt with this potential by characterizing failure modes of the rupture of a component in the direct NG system caused by an accident; it does not delve into the many varied potential causes of an accident. Failure modes on the Brake System can lead to an accident, for example, but the rupture of the tank as a result of the accident is the failure mode considered in this analysis. The FMEA process cannot identify failures resulting from sequences of events: it is not intended to be used to identify accident sequences. These limitations can be addressed by using more complex quantitative risk assessment techniques, e.g., Event Trees and Fault Trees.

Failure Modes

A *failure mode* is the manner in which a component fails, and a *failure cause* (also called a failure mechanism) is the basic reason for the failure. A failure mode answers the question “How does the part fail?” and a failure cause answers the question “why does the part fail?” The primary focus of this functional FMEA is to comprehensively identify failure modes. In this FMEA, different causes resulting in the same failure mode are grouped together as one failure mode to simplify the analysis.

Potential failure modes were determined by examining functional block diagrams as well as examining each component for the failure mode models identified in SAE ARP-5580 [1]:

- Premature operation
- Failure to operate at prescribed time
- Failure to cease operation at prescribed time
- Failure to meet functional specifications
- Failure conditions caused by the operational environment

A credible scenario was evaluated for each combination of component and failure mode, specifically focusing on failure modes that could lead to a release of natural gas in either liquid or gaseous phase. For each component, credible failure scenarios were developed based on failure experience data collected in the Reliability Information Analysis Center (RIAC) Non-Electric Parts Reliability Database (NPRD) [3] and Failure Mode Distribution (FMD) [4], previous FMEAs conducted for LNG-fueled trucks [5] and LNG refueling facilities [6], LNG marine transport and onshore terminals [7], and from LNG experts at Sandia.

If no credible NG release scenario could be developed for the combination of component and failure mode, the failure mode was excluded from the FMEA. Redundant causes for a given failure mode were grouped together to simplify the analysis. As more detailed component and part information for the system is available, this Functional FMEA can evolve into a Detailed FMEA in which the distinct causes of each failure mode may be separated into distinct failure modes for further characterization.

Failure Effects

Failure effects are the consequences of a failure mode on the operation, function, or status of an item. In a functional FMEA, failure effects are classified as local effect, next higher level effect, and end effect. Local Effects are defined as the effects that result directly from the failure mode under consideration and are the basis for identifying compensatory measures and corrective actions. The Next Higher Level effects are the impacts of the failure mode on the next higher indenture level in the system. End Effects are the impacts of the failure on the system.

A failure effects analysis was performed for each failure mode by identifying the consequence of each failure mode on operation of the assembly operation as well as the next higher indenture level. The end effect on the system was also identified.

For this analysis, the End Effect considered specifically was whether or not LNG or GNG potentially could be released in an uncontrolled manner. If the Local Effects identified included a potential release of LNG or GNG or the next level effect was not apparent, the End Effect was listed and the Next Level Higher column left blank.

Severity Classes

Severity is an assessment of the magnitude of consequence (the end effect) of the failure. In assigning severity, the analysis team considered the worst possible consequence of a failure; the probability distribution of the severity of consequences was not considered in making the severity determination. In this FMEA, because the focus of the analysis is on failure modes resulting in a release of natural gas, the ranking system and criteria used to classify the severity of failures hinges on this issue. The three severity classes and their definitions are presented in Table 1.

Table 1: Severity Classes and Definitions used to Rank Severity in the FMEA

Severity Class	Criteria: Severity of Effect
Minor	No potential release of LNG or GNG (e.g., from failure of a component that does not process LNG or GNG)
Moderate	Potential leak or small- scale release of LNG or GNG (e.g., from a leaking seal, breach of line carrying vented GNG)
Critical	Potential for catastrophic release of LNG or GNG (e.g., from a break of a line carrying LNG, from a rupture of the storage tank, from failure of a tank relief valve)

This is a Functional FMEA so it is appropriate to limit the number of severity classifications to a number corresponding to the amount of detail suitable for the level of detail in the analysis. The main differentiating factor in the classification criteria is whether a potential release is a small scale leak of natural gas or whether the failure mode could result in the uncontrolled release of the full contents of the natural gas tank.

Probability Classes

In general risk assessment, probability is used as a measure of the likelihood of occurrence of an event, such as the failure of a component or the occurrence of a specific consequence. In an FMEA, the probability class refers to the likelihood of occurrence of the failure event (defined as the failure mode). The criteria used to differentiate the High, Medium and Low probability class are based on an order of magnitude scale and are presented in Table 2.

Table 2: Probability Class Definitions

Probability Class	Criteria: Failure Rate
High	λ>10.0 per Million Hours or Million Track Miles
Medium	λ between 1and 10 per Million Hours or Million Track Miles
Low	λ<1.0 per Million Hours or Million Track Miles

Reliability data can be used to provide an objective basis for the assignment of failure probabilities. For screening-level analyses, it is common to use a failure rate as an approximation of the likelihood of a given failure mode. In this analysis, the failure rate criteria used to determine the probability class is the Failure Mode Rate.

The RIAC Non-Electric Parts Reliability Database (NPRD) [3] was used as a source of generic failures rates for estimating failure rates for the assemblies in this analysis. The failure rates are most representative when calculated from field data from the exact equipment used in the same manner and environment as the system under analysis. In the case of new technology where actual failure data is not available, where specific components have not been identified, or when a functional FMEA is being performed at levels of indenture above the piece part, it is appropriate to utilize failure rates from similar systems, tables of generic component failure rates, or other methods to derive failure rates. In this analysis, all three of the above criteria are in effect. Therefore, the generic data from RIAC Non-Electric Parts Reliability Database [3] is suitable for this analysis.

The failure rates are assumed to be constant over the lifetime of the components. The Failure Mode Rate, λ, corresponds to the failure rate for a specific failure mode of a specific component. This is calculated by using:

$$\lambda = \alpha\lambda_p$$

where λ_p is the failure rate (for all failure modes) for a specific component and α is the failure mode distribution ratio, which is the fraction of component failures corresponding to the failure mode.

The RIAC database also included the number of operational hours and failures reported during that time period. This data was used to calculate the failure rate, $\lambda_{p,}$ for each component, per million hours of operation, using:

$$\lambda_p\,(per\ million\ hrs) = \frac{Number\ of\ \ failures}{Total\ hours\,(million)}$$

In the case where no failures were reported in the database, a Bayesian methodology is used to calculate the failure rate. In this approach, the Jeffrey's prior: 0.5 failures (half of an event) is used as the number of failures in the rate calculation.

For some assembly-level components, certain failure modes result from the failure of one specific part-level component; for example, the failure of a relief valve located on a storage tank. While the FMEA in this report does not go to the part level, in cases where an assembly-level component failure mode is the result of a specific part-level component, the failure rate for the part-level component is listed and identified under the assembly-level component. Global failure rates from the RIAC dataset were used where failure mode details were unavailable.

For the failure modes involving the train being involved in an accident or derailment, a railroad accident rate totaled for all failure modes was used [8]. This data is presented in Table 3.

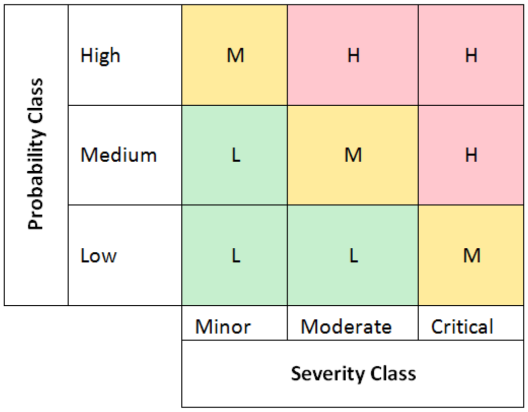
Table 3: Railroad Accident Frequencies

Number of Train Accidents[1]	Train Miles (Millions)	Rate (#events/10^6 miles)
1,897	708.19	2.68

[1] Includes all reported train accident scenarios involving on-track rail equipment (both standing and moving) in 2010.

Risk Ranking Matrix

A traditional, simplified tool used to communicate risk priority with an FMEA is a qualitative risk ranking matrix, in this case a three-by-three matrix. The vertical axis represents the three probability classes and the horizontal axis represents the three severity classes, as shown in Table 1 and Table 2. The matrix can be used to target specific, higher risk failure modes for mitigating factors to be incorporated into the design requirements of the LNG tender system. Using the risk ranking matrix, the each failure mode was given a risk priority.



Probability Class				
	High	M	H	H
	Medium	L	M	H
	Low	L	L	M
		Minor	Moderate	Critical
		Severity Class		

Figure 1: Risk Ranking Matrix

Discussion of Key Results

The FMEA resulted in the identification of three failure modes which were deemed to have a High risk priority and twenty-one that had a Medium risk priority. These failure modes should be prioritized in the overall system design to ensure engineered safety methods are used to mitigate these risks. The FMEA is an iterative process and as the design matures, as the level of detail improves, the safety and risk reduction can be built into the system to ensure that all potential unacceptable failure modes are addressed and mitigated. The remainder of the failure modes identified resulted in Low risk priority.

All three of the High risk priority failure modes involved the cryogenic storage tank. The first high risk failure mode captured the chance that the tank may need to vent due to gradual warming of the contents and the pressure relief device fails on demand. Unmitigated, this could lead to a rupture of the tank due to over-pressurization. Pressure relief devices have a failure mode rate that results in a medium probability class. The second high risk failure mode identified the failure of an outlet or fitting on the tank, especially those that penetrate both layers of the tank, potentially leading to a direct release of LNG. The final high risk priority failure mode was a failure of the outer tank due to embrittlement or cracking. This would lead to a loss of the vacuum insulation in the interstitial space between the inner and outer tank. This would in turn lead to a rapid warming of the LNG and potential over-pressurization of the inner tank, leading to rupture.

Eight of the twenty-one failure modes ranked as Medium risk priority also are related to the cryogenic storage tank. This is expected because failures of the components, penetrations and piping leading to the bulk of the LNG product could lead to a release of the entire contents of the tank. This is necessarily a High severity class and leads to higher risk priorities. Of special interest is any piping or penetration that connects to the LNG inner tank in the lower half of the tank. This is due to the fact that any damage to this type of piping could lead to a gravity drain of the entire contents. It would be difficult to mitigate if the break occurs upstream of any safety or isolation valves.

HAZOP METHODOLOGY FOR MAINTENANCE ACTIVITIES

A modified Hazard and Operability Study (HAZOP) methodology was used to analyze the maintenance mode, which includes all routine maintenance activities associated with the LNG and CNG dual-fuel locomotives and the LNG tender car. This includes maintenance activities unrelated to the fuel system, activities to remove the fuel system from service (for example, placing the LNG in a safe state before performing maintenance), and also testing and returning the system to service. Maintenance to the LNG and CNG fuel systems themselves were not included in this analysis as any work performed on these systems would be the responsibility of the manufacturer. For this analysis CNG locomotives were analyzed along with the LNG system.

During maintenance on the LNG locomotive, it was assumed that the tender is disconnected—including securing isolation valves on the tender—and all tender maintenance occurs outdoors. For all maintenance on the LNG system, it was assumed the tender is brought to the OEM site. The LNG locomotive, once disconnected from the tender, therefore should contain only residual GNG. For locations where an OEM representative will conduct maintenance on the fuel system, it is assumed that this maintenance involves only replacing components; any major overhauls would occur at an OEM facility.

HAZOP studies are usually performed on discrete industrial processes, with defined inputs and outputs from each process step or system component. Hazard scenarios are developed using a system of guide words indicating relevant deviations from system design intents. The guide words used in this analysis are shown in Table 4. Because the goal of this analysis is to identify and prioritize hazard scenarios so they can be properly addressed in the system design, a modified HAZOP method that incorporates the most useful aspects of an FMEA and a HAZOP was used. The HAZOP procedure involved an examination of each system component and identification of scenarios, conditions or failure modes that could lead to a release of natural gas. As in the FMEA, the relative severity and probability classes (Table 1 and Table 2) for each hazard scenario are assigned and the same risk matrix, Figure 1, is used to prioritize the scenarios as High, Medium, or Low.

Table 4: HAZOP Guide Words

Guide Word	Operating Deviations
None	No flow No signal No power
More	Increased flow Increased pressure Increased temperature More time
Less	Reduced flow Reduced pressure Reduced temperature Less time
Wrong	Signal Maintenance/installation
Other	As well as Shutdown/Close Start/open Relief Corrosion External event Accident Sabotage

For each scenario identified, the system and component targeted as the source of the release were numbered sequentially and recorded. For example, releases associated with the CNG manifold were labeled CNG-5. Additionally, the relevant Maintenance States when the Hazard Scenario was applicable, discussed in the next section, were documented. If no natural gas was expected to be in the manifold (CNG-5) because the isolation valve (CNG-4) was expected to be closed, then a release from the manifold was not deemed feasible for this analysis and was not included. Situations where a release is possible due to human error or failure to close the isolation valve were dealt with in the Hazard Scenarios associated with the isolation valve itself. The potential Causes and Consequences for each Hazard Scenario were determined and documented. As in the FMEA, the relative severity and probability class (Table 1 and Table 2) for each hazard scenario were assigned and the same risk matrix (Figure 1) is used to prioritize the scenarios as High, Medium, or Low.

Table 5 lists the typical maintenance activities performed on the tender and locomotive, or both. The first step in the maintenance processes for the LNG system is for the dual-fueled locomotive to be decoupled from the LNG tender. Once decoupled, the locomotive operates solely on diesel power. Because the maintenance on the two parts of the system will be handled separately, the discussion will also be separate.

Table 5: Typical Maintenance Activities

Service Maintenance and Repair Activities	Tender or Locomotive
Decouple tender from Locomotive	Both
Wheel maintenance - includes trueing	Both
Brake servicing	Both
Truck/axle maintenance	Both
Boiler maintenance	Locomotive
Heavy repair	Locomotive
Truck repair	Both
Running repair	Locomotive
Painting	Both
Inspection	Both
Troubleshooting/testing	Locomotive
Load Testing - diesel	Both
Load Testing - Natural gas	Both

Tender Maintenance Mode Analysis

A maintenance framework was developed to provide a structure for addressing the state of the fuel system for each phase of maintenance activities. This framework is intended to be roughly chronological and is shown in Table 6. The maintenance states were used in the HAZOP documentation to indicate which hazard scenarios apply. This was based on whether the components contain natural gas during each given fuel state. The fuel system state for T-3 was listed as "To Be Determined" because the LNG system maintenance activities are intended to be performed only at the OEM's facility.

Table 6: LNG Tender Maintenance Framework

Maintenance State	LNG Tender—Outdoor Only	Fuel System State
T-1	Yard storage – waiting for service	Fuel system charged but idle, key-off
T-2	Service on non-fuel systems	Tank valved off, downstream of isolation valve vented
T-3	Service on fuel system (LNG only—OEM only)	To be determined
T-4	Recouple with Locomotive	Tank valved off, downstream of isolation valve vented
T-5	Load Testing- LNG fueled	Key-on operation

The HAZOP resulted in the identification of eight credible hazard scenarios, although many were applicable to multiple maintenance states. Three of the eight credible scenarios had a Medium risk priority. The first scenario involved a coupled failure mode where the LNG tank needs to vent due to gradual warming of the contents or excessive hold time and the Pressure

Relief Device (PRD) fails, resulting in a catastrophic tank rupture. The probability class for this failure mode was Low although the severity was ranked High, resulting in a medium risk priority. The second scenario involved the intentional damage of the outer tank due to vandalism or sabotage while the tender was waiting in the yard. The third scenario involved the use of a crane to lift one end of the tender to remove or exchange the truck. Lifting one end of the tender exposes the remaining truck in contact with the ground to elevated mechanical stress, can shift or slosh the LNG in the tank which could cause unexpected movement or balance issues with the tender. A failure of the crane could also allow the raised end of the tender to drop suddenly or unexpectedly cause damage to the outer tank or external piping leading to a release of the LNG. These Medium risk scenarios are shown in Table 7.

Table 7: High and Medium Risk Priority Scenarios for LNG Tender Maintenance

Hazard Scenario and Maintenance State	Causes	Consequences	Risk
Overpressure of tank and failure of relief valve to open (T-1)	Valve failure, insulation failure, excessive hold time	Explosive vessel rupture	M
Compromise of outer tank leading to loss of vacuum (T-2)	Sabotage or vandalism to induce failure	Potential release of total volume of tank	M
Crane used to lift one end of tender to change out trucks and drop occurs (T-3)	Mechanical defect, material defect, installation error, maintenance error	Damage to piping penetrations leading to potential release of total volume of tank	M

Locomotive Maintenance Mode Analysis

A maintenance framework was also developed for the structure of the HAZOP on the locomotives. The framework is shown in Table 8 and differs from the tender framework in that it denotes where the activities are anticipated to occur–either indoor or outdoor. In the case of L-2, Storage–awaiting service, this could take place either indoors or outdoors and is therefore separated into L-2 Out and L-2 In.

Table 8: Locomotive Maintenance Framework

Maintenance States			CNG and LNG Dual-Fueled Locomotives	Fuel System State
Outdoors	Preparation for	L-1	Venting of residual NG pressure in lines	Tanks are valved off at CNG-4 isolation valve, system downstream of isolation valve is vented to atmosphere
		L-2 out	Storage-awaiting service	Diesel capability only (may be residual NG in system)
I		L-2 in	Storage-awaiting service	Diesel capability only (may be residual NG in system)
	Service	L-3	Engine operation/idling (during testing, inspection and troubleshooting activities)	Key-on operation- diesel only
		L-4	Service on non-fuel systems	Diesel capability only (may be residual NG in system)
		L-5	Service on fuel system	LNG-at OEM facility only CNG-OEM staff onsite
		L-6	System refilling or valve opening followed by restart	Fuel system recharging
Outdoors	Restart	L-7	Load test	Key-on operation – diesel or natural gas

For the CNG powered locomotive, key hazard scenarios were related to the high pressure in the system. Inadvertent or spurious opening of valves or loose fittings due to mechanical damage, defect, installation or maintenance error not only could create a fire hazard by releasing the natural gas, but could eject the parts or component fragments at a high velocity, which could lead to injury. The severity classes for the potential releases are classified only by the relative size of the release (minor leak, partial release or total volume of the cylinder or system) and are not prioritized based on the potential for human injury. Because maintenance activities occur with personnel in close proximity, this hazard should not be ignored when facilities develop their site-specific training and procedure requirements.

The HAZOP resulted in the identification of 27 credible hazard scenarios for the CNG locomotive involving a potential release of NG, although many were applicable to multiple maintenance states. The CNG locomotive, which has the CNG cylinders onboard, requires that the CNG cylinders be brought inside the facility for all maintenance activities. The potential for the CNG cylinders to be filled with CNG exists depending on site specific procedures and on actual defueling capability, so the HAZOP was performed anticipating charged CNG cylinders during maintenance activities. None of the scenarios identified resulted in a High risk priority due to the predominant Low probability class for these events. Nine scenarios were identified with a Medium risk priority and are shown in Table 9.

Table 9: Medium Risk Priority Scenarios for CNG Locomotive Maintenance

Hazard Scenario and Maintenance State	Causes	Consequences	Risk
Over pressurization of cylinder (L2-out, L-2 in, L-3, L-4, L-5, L-6, L-7)	External fire AND failure of PRD to operate	Explosive vessel rupture	M

Over pressurization of cylinder (L2-in, L-3, L-4, L-6, L-7)	External fire AND successful operation of PRD	Potential release of total volume of cylinders	M
Outlet or fitting on tank fails open (L-2 in, L-3, L-4, L-6, L-7)	Mechanical defect, material defect, installation error, maintenance error	Mechanical defect, material defect, installation error, maintenance error	M
CNG tank rupture (L-2 in, L-3, L-4, L-6, L-7)	Mechanical damage, tool or equipment impingement	Potential release of total volume of cylinders	M
Leakage from the cylinder (L-2 in, L-3, L-4, L-6, L-7)	Accident, Vandalism or sabotage	Potential release of total volume of cylinders	M
Premature activation of PRD, failure in open position (L-2 in, L-3, L-4, L-6, L-7)	Mechanical defect, material defect, installation error, maintenance error	Potential release of a portion of the cylinder(s) contents	M
PRD leak of CNG (L-2 in, L-3, L-4, L-6, L-7)	Mechanical defect, material defect, installation error, maintenance error	Potential release of a portion of the cylinder(s) contents	M
Improper venting, premature termination of venting (L-1)	Mechanical defect, material defect, installation error, maintenance error	Potential release of total volume of cylinders	M
Over pressurization of engine fuel line (L-3, L-7)	Failure of regulator to properly restrict downstream pressure to the engine	Potential release of a portion of the cylinder(s) contents	M

The base assumption for the LNG locomotive maintenance was that the LNG tender will be decoupled and the locomotive will be run on diesel or towed. This means that there is very little natural gas onboard the locomotive during maintenance activities. If the natural gas lines from the point of coupling to the dual-fuel engine are vented to atmosphere, only a de minimis amount of natural gas would remain in the lines. The only hazard scenario identified involves the failure of the system to vent completely. This may occur because of blockage or constriction due to debris or contaminants in the system. The consequences class and probability class of this scenario are both Low so this scenario is not captured in a HAZOP table.

HUMAN FACTORS ASSESSMENT ON LNG TENDER FILL EXAMPLE PROCEDURE

The human factors assessment documented a methodology to assess a procedure for the LNG tender fill process. The example procedure evaluated was an industry one-page tender fill procedure. The procedure was not intended to represent all possible variations of LNG tender fill procedures. Instead, this procedure was used as an example to illustrate general improvements. A more thorough investigation would include a direct observation of the procedure with the actual equipment and operators and a discussion with more subject matter experts involved in performing this operation. The investigation of the training and expertise of the operator are outside the scope of this assessment.

Documents were reviewed to provide information and guidance for procedure design and development. The most appropriate for guidance for this application is the Department of Energy (DOE), “Writer’s Guide for Technical Procedures” [9]. According to the DOE Guide, a technical procedure “prescribes precisely how to accomplish various technical tasks associated with starting up, testing, operating, and maintaining the facility’s equipment and systems. These procedures specify fixed tasks and define activities in a way that ensures operations are safe, efficient, and practiced with the appropriate margins of safety” [9]. Important items to consider when writing a procedure:

- Mark warnings or cautions clearly by putting them in **bold**.
- Warnings must come before action steps.
- Separate steps so they are visible. Avoid placing multiple steps in a paragraph form.
- Break up multiple steps that call out several pieces of equipment into separate steps or action to avoid confusion of equipment/numbers.
- Font and size of typeface should be a minimum of 12-point font and should be readable under the worst conditions anticipated.
- Emergency steps should be clear so the reader can locate them under stress.
- Do not require calculations to use the procedure.

Other items were identified for consideration with regard to potential error and safety concerns:

- Procedure mentions that “only properly trained and site authorized personnel shall perform the tender fill,” but does not provide guidance for who or what ‘properly trained and site authorized personnel’ are.
- The procedure indicates that proper personal protective equipment (PPE) should be worn, but does not indicate the proper PPE for the procedure.
- The procedure indicates “tender must be properly cooled and ready to accept LNG before use of the procedure.” There is no indication of how ‘properly’ or ‘ready to accept’ is determined or who is responsible.

Procedures should be reviewed every few years to ensure that the procedures remain current and up-to-date with industry best practices as well as any changes in controls, operations, or technologies. If a known change in controls, operations, or technology occurs, the procedure should be reviewed immediately to ensure that it is consistent with the changes. A team consisting of practitioners, operators, and trainers should be formed when reviewing an existing procedure or designing a new procedure. This will ensure that those who are closest and most knowledgeable can input into the procedure design.

NEXT STEPS

Appropriate next steps involve conducting a detailed FMEA for the OEM-specific system as their designs are finalized and implemented. An additional operating mode that needs to be addressed is the Refueling mode. The Refueling mode involves transfer of LNG and CNG. Although a human factors review was performed on a procedure, a quantitative analysis such as an FMEA or HAZOP could be used to analyze additional natural gas release scenarios and hazards. As the railroads move close to natural gas implementation, details on the procedures and locations of the refueling process will be defined better and then can be better analyzed. High pressure fuel (CNG) and cryogenic (LNG) materials are new to the railroad industry so transition and change management activities are important to minimizing the risks.

ACKNOWLEDGMENTS

The authors would like to thank the Federal Railroad Administration/US Department of Transportation for funding and support of this analysis. Sandia staff conducted site visits to collect information on typical processes associated with railroad maintenance and all site personnel were cooperative and actively supported the data gathering. Their engagement was crucial to this analysis and their support is appreciated.

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

REFERENCES

[1] SAE ARP 5580. Aerospace Recommended Practice-Recommended Failure Modes and Effects Analysis Practices or Non-Automobile Application. SAE International. Updated May 2012.

[2] MIL-STD-1629 A. Procedures for Performing a Failure Mode, Effects and Criticality Analysis. 1980.

[3] Reliability Information Analysis Center (RIAC), *Nonelectronic Parts Reliability Data (NPRD).*Electronic database, U.S. Department of Defense. 2011.

[4] Reliability Information Analysis Center (RIAC), *Failure Mode/Mechanism Distributions (FMD).* Electronic database, U.S. Department of Defense. 2013.

[5] *Recommended Practices for LNG Powered Heavy Duty Trucks,* ATA Foundation Alternative Fuels Task Force, Manufacturer's LNG Technical Subcommittee. 1995.

[6] Qualitative Risk Assessment for an LNG Refueling Station and Review of Relevant Safety Issues, Idaho National Engineering Laboratory, INEEL/EXT-97-00827-Rev. 2. 1998.

[7] Woodward, J. L., and Pitblado, R. M., "LNG Risk Based Safety: Modeling and Consequence Analysis." [New York]; Hoboken, N.J.: AIChE; Wiley. 2010.

[8] *Railroad Safety Statistics 2010 Annual Report*, U.S. Department of Transportation Federal Railroad Administration. 2012.

[9] United States Department of Energy (DOE), "*Writer's Guide for Technical Procedures,"* DOE-STD-1029-92, December 1998.