RISK QUANTIFICATION OF HYDRIDE BASED HYDROGEN STORAGE SYSTEMS FOR AUTOMOTIVE APPLICATIONS

Khalil, Y. F.[1] and Mosher, D. A.[2]

[1] Physical Sciences Department, United Technologies Research Center, 411 Silver Lane, MS 129-30, East Hartford, Connecticut, 06108, U.S.A, khalilyf@utrc.utc.com
[2] UTC Power Program, United Technologies Research Center, 411 Silver Lane, MS 129-21, East Hartford, Connecticut, 06108, U.S.A, mosherda@utrc.utc.com

ABSTRACT

For hydrogen fueled vehicles to attain significant market penetration, it is essential that any potential risks be controlled within acceptable levels. To achieve this goal, on-board vehicle hydrogen storage systems should undergo risk analyses during early concept development and design phases. By so doing, the process of eliminating safety-critical failure modes will help guide storage system development and be more efficient to implement than if undertaken after the design-freeze stage. The focus of this paper is the development of quantitative risk analyses of storage systems which use on-board reversible materials, such as conventional AB_5 metal hydrides, the complex hydride $NaAlH_4$ or other material candidates currently being researched. Collision of a vehicle having such a hydrogen storage system was selected as a dominant accident initiator and a probabilistic event tree model has been developed for this initiator. The event tree model contains a set of comprehensive, mutually exclusive accident sequences. The event tree represents chronological ordering of key events that are postulated to occur sequentially in time during the accident progression. Each event may represent occurrence of a phenomenon (e.g., hydride chemical reaction and dust cloud explosion) or a hardware failure (e.g., hydride storage vessel rupture). Event tree branch probabilities can be quantified using fault tree models or basic events with probability distributions. A fault tree model for hydride dust cloud explosion is provided as an example. Failure probabilities assigned to the basic events in the fault tree can be estimated from test results, published data, or expert opinion elicitation. To account for variabilities in the probabilities assigned to fault tree basic events and, hence, to propagate uncertainties in event tree sequences, Monte Carlo sampling and Latin Hypercube sampling were employed and the statistics of the results from both techniques were compared.

NOMENCLATURE

BE: Basic Event
CAFTA: Computer-Added Fault Tree Analysis software
CBA: Cost-to-Benefit Analysis
EF: Error Factor which reflects the span of the probability distribution
CS: CutSet
EPRI: Electric Power Research Institute
ETA: Event Tree Analysis
FMEA: Failure Mode and Effects Analysis
FTA: Fault Tree Analysis
GTPROB: GaTe PROBability calculator in CAFTA
HAZOP: HAZard and OPerability analysis
IE: Initiating Event
LHS: Latin Hypercube Sampling
MC: Minimum Cutset
MCS: Monte Carlo Sampling
NRC: Nuclear Regulatory Commission
PRA: Probabilistic Risk Assessment
PRAQuant: A CAFTA-based program to link and evaluate integrated event tree and fault tree models
QLRA: QuaLitative Risk Analysis

QRA: Quantitative Risk Analysis
UNCERT: a CAFTA-based program to perform uncertainty analysis on cutset files using CAFTA database
SAPHIRE: Systems Analysis Programs for Hands-on Integrated Reliability Evaluations

1.0 INTRODUCTION

1.1 Elements of Quantitative Risk Analysis (QRA)

The path to a sound quantitative risk analysis should start with qualitative methods (QLRA) such as hazard checklists, failure mode and effects analysis (FMEA), and hazard and operability analysis (HAZOP). With respect to an on-board reversible storage system, the FMEA methodology was deemed to be more appropriate compared to HAZOP since the application is still in its early design stage. Unlike FMEA, the primary focus of HAZOP is on deviations of process parameters from set operating conditions. In addition, FMEA has the advantage of being semi-quantitative [1, 2, 3, 4].

The insights to be obtained from the QLRA methods set the stage for the conduct of quantitative risk analyses. For the application of interest to this work, the key insights derived from applying FMEA to a conceptual/baseline design of an on-board reversible storage system [5] were:

- Identification of critical failure modes, safety hazards and their outcomes. This information was used for formulating the dominant accident initiating events (IE) and sequences that can represented by event tree models for those initiators.

- Identification of both component-level and system-level consequences of failure modes and safety hazards. This information is useful for supporting the conduct of economic consequence analysis.

- Down-selection of risk mitigation options for the identified critical hazards and failure modes. The risk mitigation task typically requires consideration of risk-to-risk tradeoffs as in some cases when one risk is designed out from the system, another type of risk could be unintentionally introduced. Risk mitigation may also be associated with identifying information gaps and conducting additional material and system testing. The knowledge of risk mitigation options supports the quantification of risk reduction magnitude and conducting cost-to-benefit analysis (CBA) for each proposed option.

After conducting QLRA, the remaining elements of QRA include: a) developing fault tree and event tree models, b) linking and solving these models to quantify the risk, c) conducting economic consequence analysis, d) quantifying model uncertainties and conducting sensitivity studies, and finally e) evaluating the risk significance of new data (such as field data, test results, model predictions, and industry operating experience) as they become available. The risk analyses should be revised accordingly in light of the new data. In summary, the risk models should be treated as living models subject to being updated and improved in accuracy to reflect the state-of-knowledge as it evolves over time [4].

1.2 Risk-Informed versus Risk-Based Analyses

Within the context of system design, when the risk insights derived from qualitative and quantitative risk analyses are used as the sole basis for justifying design for safety, the approach is considered risk-based [6].

For the on-board reversible storage system, however, the authors of this work do not recommend the risk-based approach to demonstrate design for safety as this approach uses risk insights as the sole input for making engineering decisions to design out critical safety hazards and failure modes. Contrary to the risk-based approach, the authors recommend the adoption of a risk-informed approach where QLRA and QRL probabilistic insights are blended with other physics-based deterministic analyses.

2.0 RISK ANALYSIS FOR ON-BOARD HYDROGEN STORAGE

This section is organized into three subsections as follows:

Subsection 2.1 describes the development and quantification of an accident sequence or Event Tree using the ETA-II Program which is part of EPRI Risk & Reliability Workstation [7]. A detailed example is provided using vehicle collision as an accident initiator.

Subsection 2.2 presents a fault tree structure that models hydride dust explosion based on a vehicle collision as the accident initiator. The CAFTA program developed by EPRI [8] is utilized to construct and solve this fault tree model.

Subsection 2.3 discusses how accident sequences generated by an event tree can be converted to fault tree models that account for the failure paths and the success paths using the DeMorgan theorem. PRAQuant, part of CAFTA, can be used for linking and solving event tree and fault tree models [7, 8].

2.1 Event Tree Model for Vehicle Collision (VC) as an Accident Initiating Event

The event tree (ET) model shown in Fig. 1 contains a sequence of six top events arranged in chronological order. The first top event on the far-most left of the diagram is the vehicle collision (VC) as the accident initiating event (IE) that could occur with some finite frequency. The progression of the remaining five top events that follow the accident initiator are: rupture of the hydride storage vessel (R), dispersal of the hydride dust in air (D), dust cloud explosion (E), dust contacts water and chemically reacts (W), and hydrogen fire breakout (F). With respect to top event (R), FMVSS 303 [13] and SAE J2579 [14] examine the likelihood for storage vessel rupture as part of the crashworthiness test. The ET in Figure 1 also contains several branches and each branch represents the probability with which the corresponding top event may occur. Each branch has a binary outcome (success / failure) with the up path (also called the success side of the branch) representing the negation of the top event and down path (also called the failure side of the branch) representing the occurrence of the top event with some finite probability. PRA practitioners refer to the branch by a node or a split fraction. In general, each branch probability is conditional on the previous branch probabilities of the tree. If appropriate, however, a simplifying assumption can be made where the event tree top events and, thus, the associated branches are assumed to be independent of each other.

A specific accident sequence is commonly referred to as a cutset. The end state of each cutset is provided on the far right side of the ET in terms of four characteristic cells, namely:

(1) Sequence class which describes the damage state (DS) of each specific sequence in the tree. For example DS-4 describes the progression of events for sequence #4 where the hydride containing storage vessel ruptured as a result of the vehicle collision, the spewed hydride material did not disperse into the air to form a dust cloud, no dust explosion occurred, however, the spewed hydride from the ruptured storage vessel came in contact with water and chemically reacted, and there was a hydrogen fire in this sequence. Each of the other damage states in the event tree of Fig. 1 can be described following a similar logic.

(2) Sequence path which describes the failure paths along the sequence. Again for sequence #4 as an example, the path would be represented by VC, R, W.

(3) Sequence probability as quantified by the ETA-II software. Since the accident initiator is expressed as a frequency and the probabilities of the branches are dimensionless, then the sequence end state is calculated as an annual probability (i.e., frequency).

(4) Sequence ID.

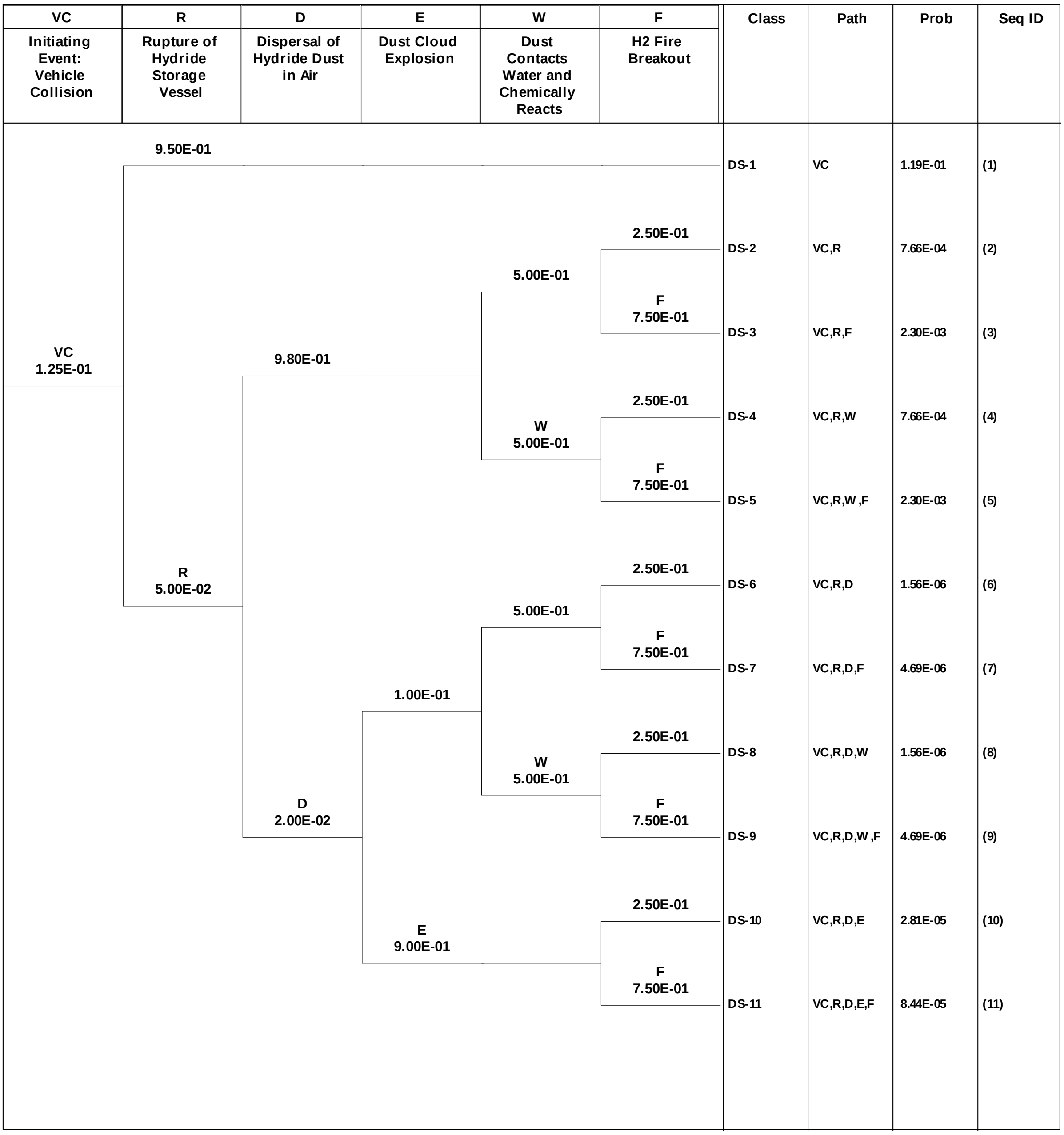

Figure 1. Event tree model for vehicle collision as an accident initiating event

2.2 Fault Tree (FT) Model for Hydride Dust Explosion

There are five conditions that must simultaneously occur for a dust explosion event to occur. The conditions are: 1) presence of an explosible dust (i.e., fuel), 2) an oxidizer (e.g., oxygen in air), 3) an ignition source, 4) mixing of dust with the oxidizer / air through sufficient turbulence leading to dust cloud suspension, and 5) some degree of confinement. The first three conditions are the commonly known requirements for fire initiation. Combustible dust explosion, however, requires two additional conditions beyond those required for a conventional fire initiation.

Figure 2a, which is continued in Figure 2b through the transfer gate G011, shows a fault tree model for an explosion event of a combustible dust such as a metal hydride. The fault tree logic covers all of the five conditions required for the explosion to occur. The fault tree model contains one top gate, nine basic events (including the accident initiator), and five gate events (including the top gate). The shown fault tree logic contains five cutsets and each represents a set of basic events that lead to failure of the fault tree top gate (NEWTOP). The CAFTA software was used to develop the fault tree model and best estimate probabilities were assigned to the basic events as shown in Figures 2a and 2b. The GTPROB subroutine in CAFTA was used to calculate the probability of each gate in the fault tree such as G001, G002, and others. The contribution of each cutset in the fault tree to the top gate (NEWTOP) probability was calculated using the cutset generator subroutine in CAFTA.

Uncertainty analysis for the quantified top gate (NEWTOP) of the fault tree model can be performed by propagating the basic event uncertainties through the five cutsets of this fault tree. This can be done by assigning appropriate probability distributions for the basic events rather than assigning best estimate values. The statistics of uncertainty analysis of the top gate "Hydride Dust Cloud Explosion," given the dry air condition and basic event probability assumptions are as follows:

Mean = 1.13E-4, median = 1.11E-4, standard deviation = 4.33E-5, lower bound (5th percentile) = 1.67E-5, and upper bound (95th percentile) = 2.71E-4. The uncertainty calculations were performed using the Monte Carlo sampling technique in Crystal Ball software. Section 3.2 discusses treatment of data uncertainties in more detail.

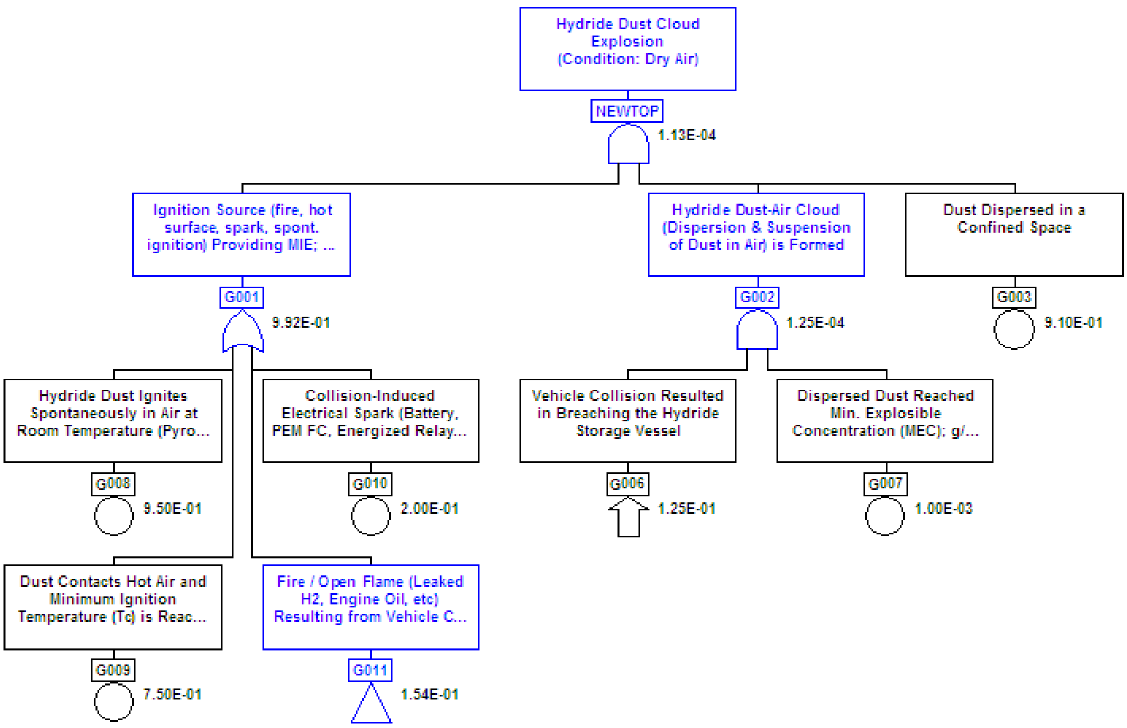

Figure 2a. Fault tree model for hydride dust explosion (Transfer Gate G011 developed in Fig. 2b)

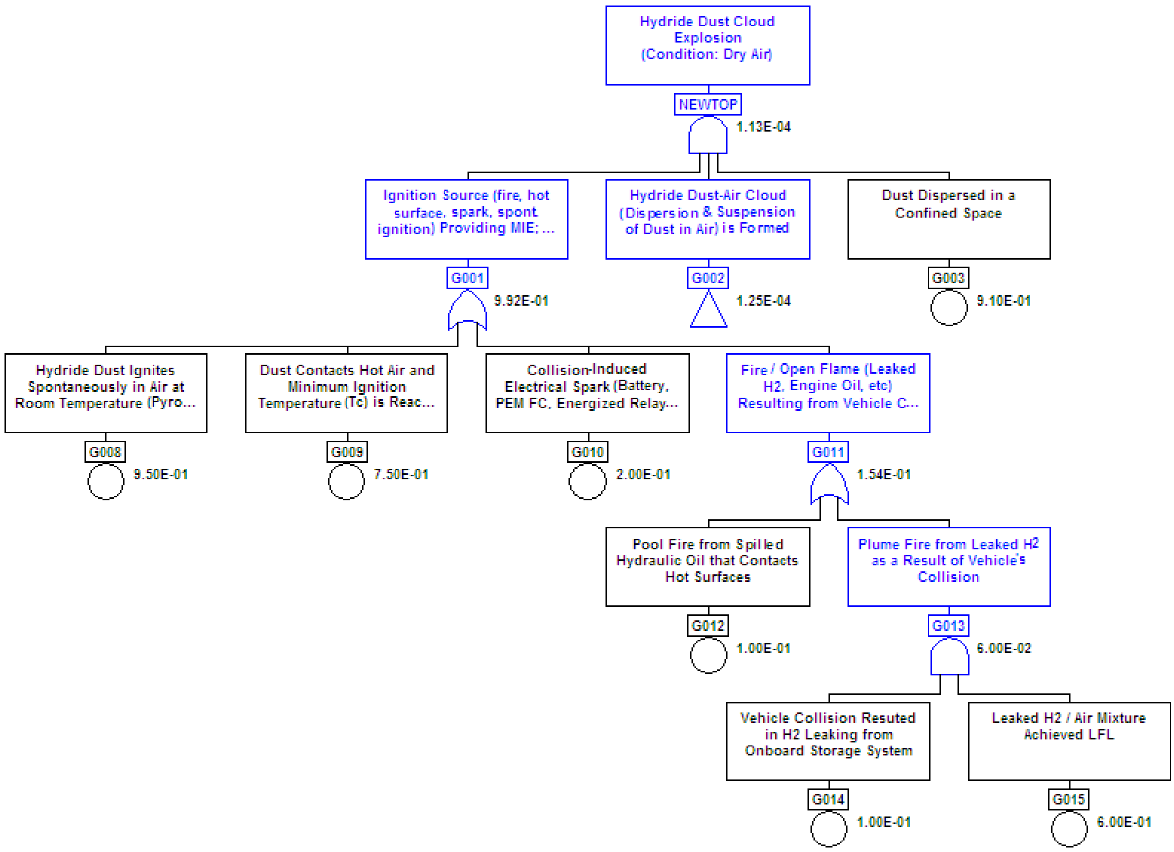

Figure 2b. Fault tree model for hydride dust explosion (Transfer Gate G002 developed in Fig. 2a)

2.3 Event Tree / Fault Tree Linking

The ETA-II program [7] was used to develop the event tree model for the vehicle collision accident initiator (Fig. 1). The event tree editor stores fault tree options in its database for use by the fault tree linking tool called PRAQUANT that reads the logic directly from the event tree editor (ETA-II). Using PRAQuant, each accident sequence in the event tree model was converted into a fault tree where the sequence end-state becomes the top gate of the fault tree logic.

When event tree branches refer to top gates in separate fault tree models, PRAQuant combines all the fault trees across the sequence under one AND gate of a new fault tree logic. This new fault tree logic can then be solved to generate the sequence end-state probability, thereby accounting for dependencies among the event tree branches in a single quantification step. In order to use the fault tree linking feature, the end-state probability calculation function of the Event Tree Editor must be turned off since this function assumes that the branches are independent (i.e., each branch is not conditionally dependent on previous branches in the event tree). Finally, the negation of some events along an accident progression path (such as sequence #9 in Fig. 1) is handled in CAFTA by applying DeMorgan's theorem [9] which can be represented as follows:

$$\overline{\left\{\bigcup_{i=1}^{n} E_i\right\}} = \bigcap_{i=1}^{n} \overline{E_i} \qquad (1)$$

$$\overline{\left\{\bigcap_{i=1}^{n} E_i\right\}} = \bigcup_{i=1}^{n} \overline{E_i} \qquad (2)$$

Where: E_i = Prob. of occurrence of event (i) and $\overline{E_i} = 1 - E_i$ = Complement of event (i)

In Fig. 1, for each accident sequence that contains failure paths as well as success paths, two fault tree gates are created. The first is an AND gate of the failure paths of the sequence. The second gate is an OR Gate of the success paths in the sequence, where this gate has the same name as the sequence, with an "N" appended. The fault tree logic would then be the first AND gate and not the second gate (referred to as a NAND gate). Fig. 3 shows an example of an accident sequence with only failure paths (sequence #11 in Fig. 1) that is converted into a fault tree model. Fig. 4 shows an example of an accident sequence with both failure and success paths and how it is converted into a fault tree model. Accident sequence #9 in Fig. 1 was used as a demonstration of how De Morgan's theorem was applied to account for the negation of some events along the sequence progression path.

3.0 UNCERTAINTY ANALYSIS

3.1 Sources of Uncertainties

Understandably, there are many sources of uncertainties, some of which could be phenomenologically driven while others could be due to shear randomness, associated with events that could be triggered by different accident initiators. For example, with some finite probabilities, the following events may occur after an on-board storage vessel breach as a result of a vehicular collision: a) the hydride dust may disperse in the air as a cloud of fine particles or may form coarser particles (clumps) that settle by gravitational force to form a pile on the ground beneath the vehicle, b) all, or a percentage of, the ejected hydride dust may contribute to dust explosion, and c) the ejected hydride dust may come in contact with water of any source (e.g., wet ground, rain, or just humid air) and chemically react, d) the dispersed dust may fall on a hot surface of temperature ≥ the minimum ignition temperature (T_c) of the dust cloud, or may come in contact with an electric spark capable of providing the minimum ignition energy (MIE) for the dust cloud.

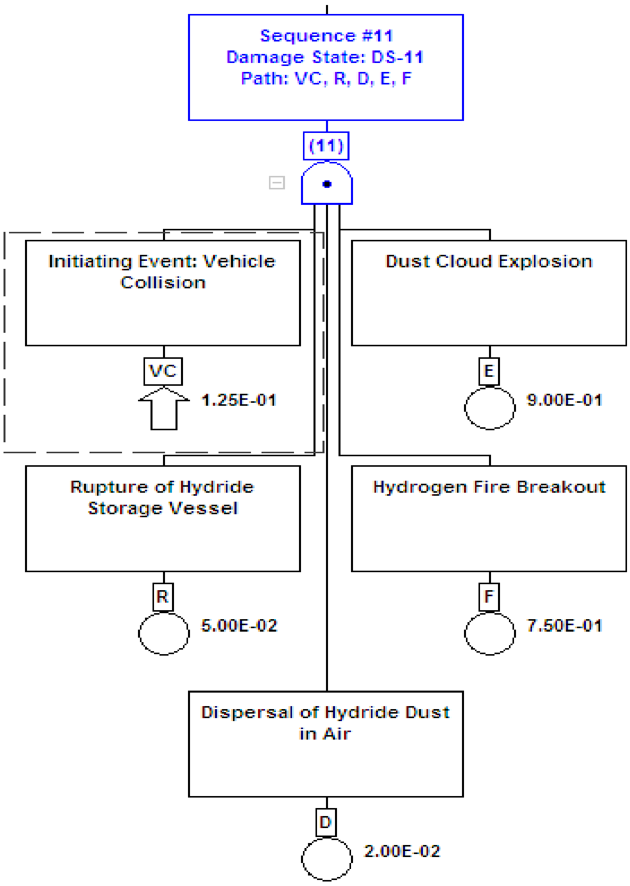

Figure 3. Fault tree model for sequence #11 of event tree model shown in Fig. 1

These uncertainties can be addressed by assigning appropriate probability distributions to the fault tree basic events. For example, the basic event that models dust dispersal can be represented by a lognormal distribution with some risk factor while a Gaussian distribution (with some mean and a standard deviation) could be used for the basic event that models vessel breach. Other probability distributions that are commonly used in PRA include the Beta, Gamma, and the exponential distributions. Most statistical software packages can be used to generate best fit probability distributions from experimental results, field failure rate data, or from expert judgment elicitation [10].

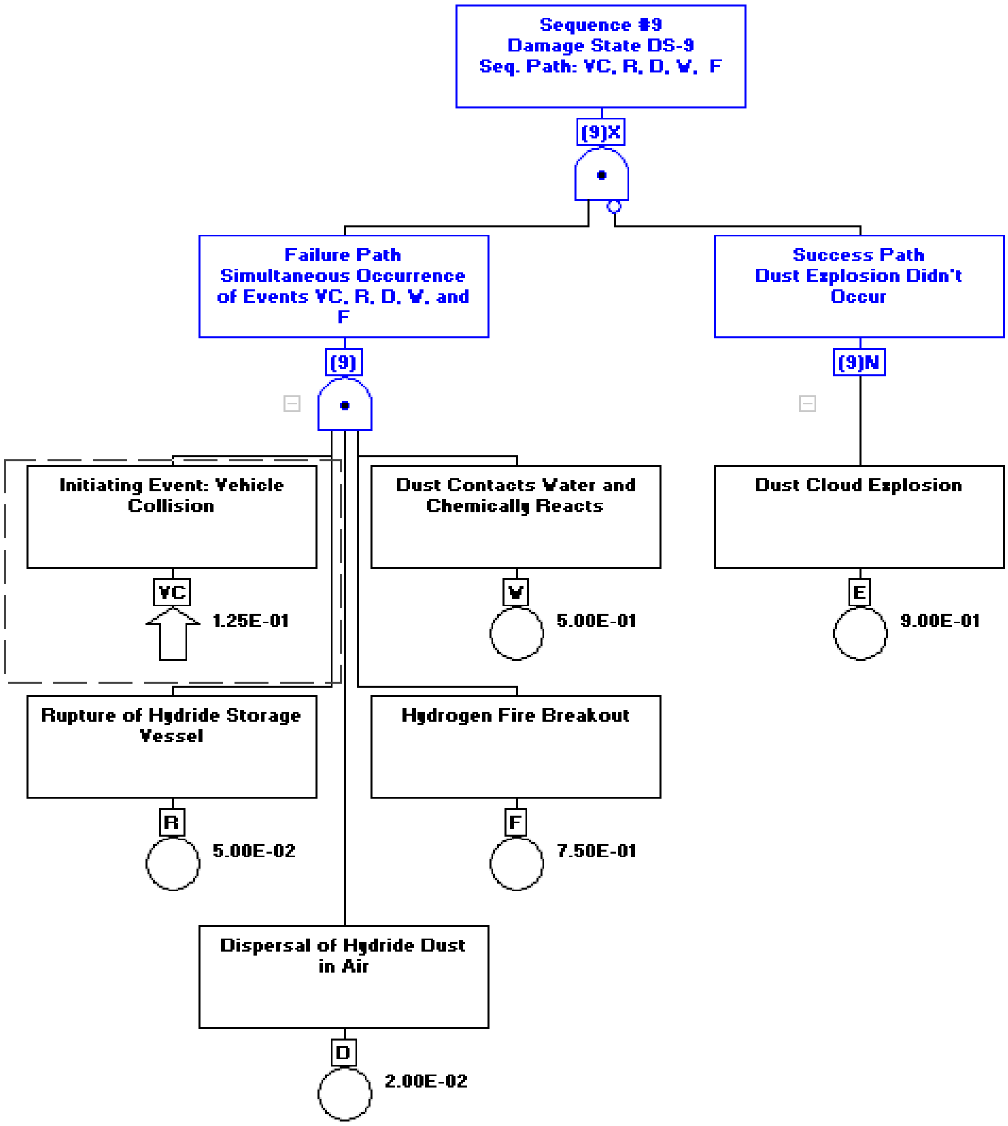

Figure 4. Fault tree model for sequence #9 of the event tree model shown in Fig. 1.

3.2 Treatment of Data Uncertainties

The two methodologies for uncertainty analysis that are commonly used in PRA are the Latin Hypercube Sampling (LHS) and Monte Carlo Sampling (MCS), respectively [10].

The Crystal Ball software, developed by Decisioneering Inc., contains MCS and LHS capabilities in an Excel platform [11]. Other specialized software packages with both MCS and LHS capabilities include UNCERT [7] developed by EPRI and SAPHIRE [12] developed by INEL for the Nuclear Regulatory Commission (NRC).

Other approaches that could be used to treat uncertainties in addition to the rigorous methods discussed in the section include applying the defense-in-depth (DID) philosophy commonly used in nuclear PRAs. The DID philosophy can be implemented in a system design by requiring component redundancy, component diversity, and allowing sufficient safety margins in the design calculations. These requirements add layers of defense-in-depth to the system design.

The Boolean polynomial for accident sequence #11 can be described as follows:

$$VC \cap R \cap D \cap E \cap F = DS - 11 \tag{3}$$

Where:
VC = Vehicle Collision as the accident initiating event (annual probability or frequency)
R = Probability of Rupture of the hydride storage vessel given a vehicle collision. This event represents an aleatory uncertainty
D = Probability of Dispersal of the hydride dust in air given a vehicle collision and rupture of the hydride storage vessel
E = Probability of dust cloud Explosion given vehicle collision, rupture of the hydride storage vessel, and dispersal of the dust in air
F = Probability of hydrogen Fire breakout given vehicle collision, rupture of the hydride storage vessel, dispersal of the hydride dust in air, and dust explosion.
$\cap$ = Boolean symbol for intersection of events.
DS-11 = damage state for sequence #11 in the vehicle collision event tree

Each of the events in Equation (3) can be represented by a probability distribution with a mean (or median) and an error factor (EF). When the medians of these events are entered into Equation (3), a single point estimate of the sequence (cutset) end-state probability can be calculated as follows:

$$(1.25E-1)*(5.0E-2)*(2.0E-2)*(9.0E-1)*(7.5E-1) = 8.44E-5 \tag{4}$$

The end-state frequency of sequence #11 is also shown in the vehicle collision event tree, Fig. 1.

Example of Event Tree Sequence (Cutset) End-State Uncertainty Calculation

The following subsections, 3.2.1 and 3.2.2, illustrate the MCS and LHS methods, respectively, for the accident sequence #11 of the vehicle collision event tree. The resulting end-state (DS-11) probability distribution is calculated for each sampling technique and the statistics are compared.

3.2.1 MCS Technique

To perform the Monte Carlo Sampling, a series of quantifications of an event tree end-state needs to be performed using random samples from each basic event uncertainty distribution. To avoid clustering potential, the MCS technique may require more sampling than LHS for the same level of accuracy. Based on the authors' experience, to generate reliable results with MCS, the number of sampling points or trials from the probability distribution should be at least 1000.

Table 1 shows the statistics of the calculated frequency of sequence #11 end-state. The MCS technique required 100,000 trials in order to achieve reliable uncertainty calculations with 95% confidence level. Fig. 5 shows the end-state probability density function as predicted by MCS.

3.2.2 LHS Technique

LHS is a stratified sampling technique where the probability distribution of the random variable is divided into equal intervals. The LHS algorithm forces the sampling process to randomly select probabilities from within each interval for each basic event. Hence, LHS avoids clustering (where samples are taken from some parts of the distribution and, thus, the distribution is not fully sampled) which could potentially happen when MCS is used. LHS generally requires fewer samples than the MCS for a similar accuracy level. Because of the stratification method used in LHS, however, it takes a longer computational time per sample to propagate uncertainties compared to MCS.

Table 1. Statistics of Sequence #11 end-state (DS-11) frequency using MCS and LHS.

	MCS	**LHS**
Mean	8.45E-5	8.44E-5
Standard Deviation	1.91E-5	1.91E-5
5^{th} Percentile (lower bound)	4.65E-5	4.52E-5
95^{th} Percentile (upper bound)	1.61E-4	1.52E-4

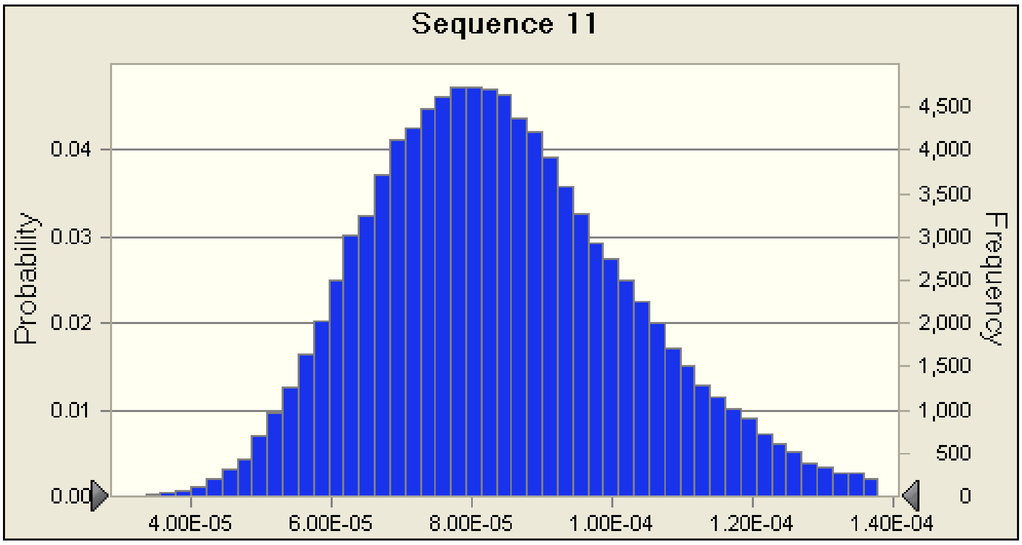

Figure 5. Probability density function of end-state frequency for sequence #11 using MCS

The Latin Hypercube Sampling technique required 100,000 trials in order to achieve reliable uncertainty calculations with 95% confidence level. Within each interval of the stratified probability distribution 500 samples were taken. Table 1 shows the statistics of the accident sequence #11 end-state frequency as predicted by LHS.

Comparison of the two uncertainty propagation methods indicates that they both give similar statistical results. Minor differences do exist with the general trend that LHS produces frequency values which are slightly lower than those predicted by the MCS method.

4.0 CONCLUSIONS

The primary focus of this work has been quantitative risk analysis of on-board reversible hydrogen storage systems. Vehicle collision was selected as one of the dominant initiating events as evidenced by a previous study of the authors on using design failure mode and effects analysis for a conceptual baseline design of an on-board reversible storage system [5]. The ETA-II software [7] was used to develop an event tree model for this accident initiator. Each sequence or cutset in the event tree model was converted to a fault tree model and the sequence end-state was quantified using the event tree / fault tree linking methodology supported by PRAQuant [8]. Finally, the uncertainties associated with probabilities assigned to the basic events in the fault tree models were evaluated using Monte Carlo sampling and Latin Hypercube sampling techniques supported by the Crystal Ball software and the statistical results were compared.

Key insights gained and recommendations:

(a) Vehicle collision is the dominant accident initiating event which could lead to rupturing the on-board hydride storage vessel with some finite probability depending on the impaction energy. Hence, further understanding of the vessel structural integrity through modeling, experimentation and field data would be of value.

(b) Additional experimental studies are motivated to better understand the physical phenomena of hydride dust spillage behavior and the compounding effect when a mixture of hydride dust and hydrogen gas is suddenly exposed to air.

(c) Since the epistemic uncertainties associated with basic events that represent physical phenomena (such as dust dispersion) and the aleatory uncertainties related to hardware failure (such as hydride storage vessel rupture) could be large, risk quantification should include uncertainty propagation from basic events to fault trees top gates and across each accident sequence to the end-state probability. Other methods that could be used to offset the impact of large uncertainties include applying the defense-in-depth philosophy and considering sufficient safety margins.

(d) Due to the scarcity and sometimes non-existent field data to support risk quantification, expert opinion solicitation should be applied with the understanding that as more reliable data become available, the risk models could be refined accordingly. In a previous work by the authors, the mechanism of expert opinion elicitation was comprehensively discussed [10].

5.0 REFERENCES

1. Khalil, Y. F., Failure Mode and Effects Analysis & Hazard Analysis and Critical Control Points: FMEA & HACCP Training Workshop sponsored by California Safety Compliance Corporation (CSCC), 1122 W. Washington Blvd., December 10-11, 2003, Los Angeles, CA 90015.
2. SAE J1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), August 2002.
3. MIL-STD-1629, Procedures for Performing a Failure Modes and Effects Analysis, Military Standard, Department of Defence, Washington, DC.
4. Khalil, Y. F., ASME Nuclear Engineering Handbook, Chapter 16: Risk Assessment and Safety Analysis for Commercial Nuclear Reactors, CRC Press, Taylor and Francis, (In Press, 2009).
5. Khalil, Y. F. and D. A. Mosher, Risk Assessment for On-Board Reversible Hydrogen Storage: Conceptual Baseline Design and FMEA Worksheet, Internal Document, United Technologies Research Center (UTRC), January 2009.
6. Khalil, Y.F., Risk-Informing the Management of Nuclear Assets. Proceedings of 8th International Conference of Nuclear Engineering, Paper # ICONE-8683, April 2-6, 2000, Baltimore, MD.
7. ETA-II software, EPRI Risk and Reliability Workstation, EPRI, Palo Alto, CA, 94304.
8. CAFTA software, EPRI Risk and Reliability Workstation, EPRI, Palo Alto, CA, 94304.
9. Khalil, Y.F. and R. Anoba, Modeling Characteristics of an Operational Probabilistic Safety Assessment (PSA). Proceedings of the 10th International Conference on Nuclear Engineering, Paper # ICONE 10-22010, April 14-18, 2002, Arlington, VA.
10. Khalil, Y. F. and D. A. Mosher, Probabilistic Treatment of Expert Judgment on Aleatory and Epistemic Uncertainties Associated with On-board Vehicle Hydrogen Storage Systems. Proceedings of the International Conference on Probabilistic Safety Assessment, PSA 2008 Topical Meeting, September 7-11, 2008, Knoxville, TN.

11. Crystal Ball software package (Rev. 7.2.2.), Decisioneering, Inc., Denver, CO, 80202.
12. SAPHIRE for Windows (Rev. 6.0), prepared for the Nuclear Regulatory commission by the Idaho Nat. Eng. Lab., Idaho Falls. ID 83415.
13. FMVSS 303 (FMVSS 49 CFR 571.303), Fuel System Integrity of Compressed Natural Gas Vehicles.
14. SAE J2579, Technical Information Report for Fuel Systems in Fuel Cell and Other Hydrogen vehicles, January 2009.

Acknowledgement: This material is based upon work supported by the U.S. Department of Energy under contract # FG36-07GO17032. The authors would like to acknowledge the guidance provided by Dr. Ned Stetson at DOE, Dr. Donald Anton at Savannah River National laboratory and Dr. Daniel Dedrick at Sandia National Laboratories for their technical collaboration is this area.