RISK QUANTIFICATION FRAMEWORK OF HYDRIDE-BASED HYDROGEN STORAGE SYSTEMS FOR LIGHT-DUTY VEHICLES

Y. F. Khalil, Ph.D., Sc.D.

Physical Sciences Department, United Technologies Research Center, 411 Silver Lane,
MS 129-30, East Hartford, Connecticut, 06108, U.S.A, khalilyf@utrc.utc.com

ABSTRACT

This study aims to develop a quantitative risk assessment (*QRA*) framework for on-board hydrogen storage systems in light-duty fuel cell vehicles, with focus on hazards from potential vehicular collision affecting hydride-based hydrogen storage vessels. Sodium aluminum hydride (NaAlH_4) has been selected as a representative reversible hydride for hydrogen storage. Functionality of *QRA* framework is demonstrated by presenting a case study of a postulated vehicle collision (*VC*) involving the onboard hydrogen storage system. An event tree (*ET*) model is developed for *VC* as the accident initiating event. For illustrative purposes, a detailed *FT* model is developed for hydride dust cloud explosion as part of the accident progress. Phenomenologically-driven *ET* branch probabilities are estimated based on an experimental program performed for this purpose. Safety-critical basic events (*BE*) in the *FT* model are determined using conventional risk importance measures. The Latin Hypercube sampling (LHS) technique has been employed to propagate the aleatory (i.e., stochastic) and epistemic (i.e., phenomenological) uncertainties associated with the probabilistic *ET* and *FT* models. Extrapolation of the proposed *QRA* framework and its core risk-informed insights to other candidate on-board reversible and off-board regenerable hydrogen storage systems could provide better understanding of risk consequences and mitigation options associated with employing this hydrogen-based technology in the transportation sector.

Keywords: Event tree; fault tree; on-board reversible; off-board regenerable; dust cloud explosion; importance measures

Nomenclature

BC: Base case

BE: Basic event

CAFTA: Computer-added fault tree analysis software

CBA: Cost-to-benefit analysis

CNG: Compressed natural gas

CS: Cutset

EPRI: Electric Power Research Institute

ETA: Event tree analysis

FMEA: Failure mode and effects analysis

FTA: Fault tree analysis

F-V: Fussell-Vesely importance measure

GTPROB: Gate probability calculator in *CAFTA*

HAZOP: Hazard and operability analysis

IE: Initiating event
LD-FCV: Light-duty fuel cell vehicle
LHS: Latin Hypercube sampling
MCS: Monte Carlo sampling
MECE: Mutually exclusive and collectively exhaustive
MIE: Minimum ignition energy of the dispersed hydride dust in air
NRC: Nuclear Regulatory Commission
PEM: Proton exchange membrane
PoF: Physics of failure
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
RB: Risk-based decisions
RAW: Risk achievement worth importance measure
RI: Risk-informed decisions
SAPHIRE: Systems analysis programs for hands-on integrated reliability evaluations
UNCERT: a *CAFTA*-based program to perform uncertainty analysis on cutset files using *CAFTA* database

1. Introduction

For hydrogen fueled light-duty fuel cell vehicles (*LD-FCV*) to attain a significant market penetration, it is imperative for automotive manufacturers to demonstrate that all potential risks associated with this hydrogen-based technology are well-understood and controlled within acceptable levels. To achieve this goal, *LD-FCV* with on-board solid-state hydrogen storage systems should undergo comprehensive quantitative risk analysis (*QRA*) during their concept development and early design phases. Risk-informed decisions that aim to “*eliminate by design*” all potential safety-critical failure mechanisms can guide design and safe implementation of the on-board hydrogen storage systems in *LD-FCV*.

The objective of this study is twofold: a) propose a *QRA* framework that could be adopted for quantifying the risks associated with on-board reversible and off-board regenerable hydrogen storage systems and b) demonstrate functionality of the proposed *QRA* framework using a case study of a postulated vehicular collision (*VC*). The on-board hydrogen storage medium is assumed to be a reversible complex metal hydride, and sodium aluminum hydride (NaAlH_4) has been selected as the candidate reversible hydride in this case study. Again, the focus of this investigation is on the hazards from a potential vehicular collision affecting the on-board hydride-based hydrogen storage vessel. Moreover, hydrogen auto ignition phenomenon is out of scope of the proposed risk quantification framework as the focus is on NaAlH_4 related safety events.

The remainder of this paper is organized as follows: Subsection 1.1 presents the elements of *QRA* and subsection 1.2 discusses the fundamental differences between risk-informed (*RI*) and risk-based (*RB*) decision-making processes. Section 2 describes the proposed *QRA* framework for on-board hydrogen storage. Results and discussion are presented in Section 3. Finally, Section 4 summarizes the study's key conclusions and suggested recommendations for future work.

1.1 Elements of quantitative risk assessment (*QRA*)

A well-structured *QRA* should start by conducting qualitative risk analysis (*QLRA*) such as design failure mode and effects analysis (*d-FMEA*) or hazard and operability (*HAZOP*) analysis.¹ In this study, *d-FMEA* methodology (SAE J1739, 2002; MIL-STD-1629, 1980) is deemed more appropriate since on-board hydrogen storage systems design is still in its conceptual stage. Khalil's application of *d-FMEA* to a conceptual/baseline design of an on-board reversible storage system yielded the following risk information (Khalil, 2011):

- Identification of critical failure modes and safety hazards, their root causes and their system-level consequences. This information is useful for formulating the dominant accident initiating events (*IE*) and accident progression pathways that can be represented by probabilistic event tree (*ET*) and fault tree (*FT*) models.
- Down-selection of candidate mitigation strategies for the identified risk-significant failure modes and safety hazards. The risk mitigation task typically requires consideration of *risk-to-risk* tradeoffs where designing out a given risk could, unintentionally, introduce one or more new risks that should be addressed. In some cases, the proposed risk mitigation method may involve additional testing or developing physics-of-failure (*PoF*) models to better understand the failure mechanism and how it can be mitigated.
- Quantification of risk reduction ($\Delta Risk$) associated with each proposed risk mitigation strategy. This information is useful in evaluating cost effectiveness of each mitigation strategy.

After completing *QLRA*, the remaining *QRA* elements are: a) developing probabilistic event tree (*ET*) model for each accident initiating event and fault tree (*FT*) models for the top events of each *ET* model, b) linking and solving *ET/FT* models to quantify the accident sequences, c) quantifying the aleatory and epistemic uncertainties associated with *ET* and *FT* models, d) quantifying the risk importance measures of basic events (*BE*) in the *FT* models,

¹ *HAZOP* analysis focuses on identifying deviations of process parameters from desired operating set points.

and e) conducting economic consequence analysis for the identified dominant accident initiators. It should be noted that *QLRA/d-FMEA* and *QRA* should be treated as living risk models to be periodically updated to reflect the latest relevant state-of-knowledge as it evolves over time (Khalil, 2009).

1.2 Risk-based (RB) versus risk-informed (RI) decisions

When the decision-making process to design out sources of system risks is solely based on insights derived from *QLRA* and *QRA*, the process is referred to as a risk-based (*RB*) decision [5]. The main shortcoming of *RB* decisions is the exclusion of deterministic insights that can be gained from performing engineering calculations and experimental studies. These additional insights could be critical to the decision-making process. To avoid this inherent shortcoming, the present study adopts a risk-informed (*RI*) decision-making process (Khalil, 2000) whereby the *QLRA*- and *QRA*-based insights are blended with insights from physics-based models and experimental observations. As demonstrative examples on the use of the *RI* approach, Khalil conducted dust cloud explosion tests to determine the explosibility of several candidate solid-state hydrogen storage materials including NaAlH_4 and performed material reactivity tests (Khalil, 2010a; 2013a; 2013b; 2013c) to determine the degree of pyrophoricity of hydride powder when it comes in contact with water or humid air. As discussed in subsection 3.1, these experimental insights are used for estimating realistic probabilities of occurrence of key phenomenological events that describe progression of accident sequences triggered by postulated initiating events.

2. Quantitative Risk Assessment (*QRA*) Framework for On-Board Hydrogen Storage

Section 2 introduces the proposed *QRA* framework (Fig. 1) and presents a case study to demonstrate its functionality. The case study postulates a collision of a light-duty PEM² fuel cell vehicle with an on-board hydrogen storage system that contains sodium aluminum hydride (NaAlH_4) as a representative reversible hydrogen storage material. To discuss the details of the proposed *QRA* framework, Section 2 is structured into five subsections as follows: Subsection 2.1 describes the development of a probabilistic *ET* model using the *ETA-II* Program which is part of EPRI Risk & Reliability Workstation (ETA-II, 2007). The *ET* model is applied to the postulated vehicular collision (*VC*) as the accident initiating event (*IE*). Subsection 2.2 discusses the development of a probabilistic *FT* structure that models hydride dust cloud explosion based on the postulated *VC*. The *CAFTA* program developed by EPRI (CAFTA, 2007) is utilized to construct and quantify this *FT* model. Subsection 2.3 presents the methodology for *ET/FT* linking and shows how the mutually exclusive and collectively exhaustive (*MECE*) accident sequences contained in the *ET* model can be converted into equivalent *FT* models. Subsection

² Proton exchange membrane.

2.4 deals with uncertainty treatment in the probabilistic *ET* and *FT* models. Subsection 2.5 presents the methodologies used for determining the risk importance measures of basic events (*BE*) contained in the *FT* models.

Fig. 1. Proposed *QRA* framework for on-board hydrogen storage systems.

2.1 Probabilistic event tree (*ET*) model for a postulated vehicular collision (*VC*) as the accident initiating event

As shown in Fig. 2, the probabilistic *ET* model contains a set of mutually exclusive and collectively exhaustive (*MECE*) accident sequences. The model describes a chronological ordering of key top events that are postulated to occur during the accident progression following occurrence of the vehicular collision (*i.e.*, the accident initiating event). As shown in Fig. 2, there are six top events as follows: The first top event, on the far-most left of the diagram, is the vehicle collision (*VC*) triggering event that is assumed to occur with some finite frequency (*i.e.*, probability/year). The second top event is rupture of the on-board hydride storage vessel (*R*). The third top event is dispersal of the hydride dust in air (*D*). The fourth top event is dust cloud explosion in air (*E*). The fifth top event is dust contacts water in any form (rain, humidity in air, etc.) and chemically reacts to produce H_2 gas (*W*) and the sixth top event is hydrogen fire breakout (*F*). For this particular accident initiator, the *ET* logic contains 11 *MECE* sequences and 27 branches (or split fractions). Each branch represents the probability with which the corresponding top event occurs. Each branch represents a Bernoulli distribution with a binary outcome (success / failure) with the upward path (*i.e.*, the success side of the branch) representing the negation of occurrence of the corresponding top event and a downward path (*i.e.*, the failure side of the branch) representing the occurrence of the top event with some finite probability. In general, each branch probability is conditional on the previous *ET* branch probabilities. However, it is also possible that the branches can be independent of each other and in such case; marginal probabilities are used instead of conditional probabilities.

The end state (*i.e.*, outcome) of each of the 11 accident sequences is characterized by four identifiers as shown on the far right side of the *ET* model in Fig. 2. These identifiers are:

- (1) Sequence class: it describes the damage state (*DS*) or severity of outcome. For example, *DS-1* signifies that in Seq-01, the hydride storage vessel did not rupture as a result of the vehicular collision. Hence, the subsequent top events *D*, *E*, *W*, and *F* did not occur. Seq-11, however, represents the worst case scenario since the hydride storage vessel is assumed to be ruptured (top event *R*) as a result of the collision and both top events *E* and *F* have occurred.
- (2) Sequence path: it describes the failure paths of the *ET* branches along the sequence. For example, Seq-04 has a failure path represented by *VC*, *R*, and *W*.

- (3) Sequence frequency: it is the probability of occurrence (per unit time) of the accident sequence. Since the *ET* accident sequences are mutually exclusive and collectively exhaustive, only one of the *ET* accident sequences can occur with some likelihood as shown in this column of the *ET* structure (Fig. 2).
- (4) Sequence ID: it is an identifier used by *CAFTA* in order to convert each *ET* accident sequence into an equivalent *FT* model. The sequence ID becomes the name of the top gate in the equivalent *FT* model.

Fig. 2. Probabilistic event tree (*ET*) model for a vehicular collision (*VC*) as an accident initiator.

As discussed in subsection 3.1, assigning realistic probabilities for the *ET* top events *D*, *E*, *W*, and *F* are based on experimental insights. With respect to estimation of likelihood of rupture of the hydride storage vessel (*R*), it is worth mentioning that Type-III and Type-IV vessels have been proposed for storing the reversible hydride material in on-board systems for the light-duty vehicular application. The main difference between these types is that Type-III vessel has an inner stainless steel liner with a full composite overwrap. In Type-IV vessels, the inner liner is made of a polymeric material such as high-density polyethylene, *HDPE*, while the outer full overwrap is made of a composite material. In both vessel designs, the inner liner provides the barrier to prevent hydrogen gas leakage and the composite overwrap provides the structural strength of the vessel. Type-III vessel design has a couple of advantages over Type-IV design; firstly, because the metal liner offers more resistance to hydrogen leakage and secondly, because it eliminates the concerns about the liner-boss interface. For the purpose of this research and due to the absence of specific catastrophic rupture data for Types III and IV vessels, the assigned probability of rupture of the hydride storage vessel (*R*) in the *ET* model, Fig. 2, is extrapolated from published data of a surrogate vessel used for compressed natural gas (*CNG*) storage (Chamberlain, 2004). In his study, Chamberlain (2004) limited his estimate of catastrophic rupture probability on *CNG* Type-I (made of AISI 4130X alloy steel) vessels, as this design represents about 90% of *CNG* storage vessels currently in use in the U.S. transportation sector.³ He reported a lifetime (assumed to be 15 years) probability of catastrophic rupture of the inner surface of the *CNG* vessel side wall of 5.09E-3 and a lifetime probability of 4.45E-3 for the catastrophic rupture of the side wall's outer surface. These probabilities are based on a predictive model for cyclic fatigue which causes wall crack growth leading to catastrophic rupture of the *CNG* vessel (Chamberlain, 2004). Undoubtedly, use of failure data of the *CNG* surrogate vessel does not provide an accurate estimation for a representative on-board reversible hydride storage vessel due to many sources of uncertainty including the vessel type (namely, Type-III or IV versus Type-I) and the pressure loading pattern (between 250 bar when full and 20 bar at empty

³ The majority of *CNG* vessels are of Type-I design (all metal) and the rest are Type-II vessel (has a metallic liner with hoop-wrapped composite matrix).

for a CNG vessel and between 100 bar when NaAlH_4 vessel is fully charged and ≈ 6 bar when discharged).

2.2 Probabilistic fault tree (FT) model for hydride dust cloud explosion

For hydride dust cloud explosion (E), which is the fourth top event in the probabilistic ET model (Fig. 2), there are five conditions that must be simultaneously present for this event to occur, namely: 1) an explosible dust (*i.e.*, fuel), 2) an oxidizer (*e.g.*, oxygen in air), 3) an ignition source with energy $\geq$ the dust minimum ignition energy (MIE), 4) suspension of the dispersed dust in air forming a dust cloud, and 5) some degree of confinement in which dust is dispersed. The first three conditions are the commonly known requirements for fire occurrence. Combustible dust explosion, however, requires two additional conditions (#4 and #5) beyond the three conditions required for causing a fire event. Figures 3a and 3b show a probabilistic fault tree (FT) model for the hydride dust cloud explosion event (E). Fig. 3b depicts the subtree logic of the transfer gate G008 (identified by the triangular symbol shown in Fig. 3a). As displayed in Fig. 3a, the FT model contains four of the aforementioned five conditions required for dust cloud explosion to occur and these four conditions are represented by the following FT basic events:

G001: this basic event represents the probability of occurrence of an ignition source with energy $\geq$ the dust minimum ignition energy (MIE).

G002: this basic event represents the probability that dust is dispersed in a confined space.

G003: This basic event represents the probability of presence of a combustible hydride dust.

G004: This basic event represents the probability of presence of an oxidizer (air).

The fifth condition for dust cloud explosion to occur is explicitly included in the ET model (Fig. 2) by the top event D which signifies dispersal of hydride dust in air. Moreover, the FT model (Figs. 3a and 3b) contains one top gate (E), nine basic events, four gate events (two AND gates and two OR gates), and five cutsets.

Fig. 3a. Probabilistic fault tree (FT) model for hydride dust cloud explosion (E) (Subtree of transfer gate G008 shown in Fig. 3b).

Fig. 3b. Subtree of gate G008 (*i.e.*, the transfer gate shown with the triangle symbol in the probabilistic fault tree (FT) model in Fig. 3a).

2.3 Event tree (ET) / fault tree (FT) linking methodology

The *ETA-II* program is used for development of the probabilistic *ET* model for the vehicle collision (*VC*) accident initiator (Fig. 2). The *ET* editor stores *FT* options in its database for use by the *ET/FT* linking algorithm called *PRAQUANT* that reads the logic directly from the *ET* editor in the *ETA-II*. When *ET* branches refer to the top gates of separate *FT* models, *PRAQUANT* combines all the fault trees across the sequence under one *AND* gate of a new master *FT* logic. This master *FT* logic can then be solved to generate the sequences' end-state probabilities, thereby accounting for dependencies among the *ET* branches in a single quantification step. In order to use the *ET/FT* linking feature, the end-state probability calculation function of the *ET* editor must be turned off because enabling this function assumes that the *ET* branches are independent (*i.e.*, each branch is not conditionally dependent on previous branches in the *ET* model).

2.4 Treatment of uncertainty in the probabilistic models

Understandably, the *ET* and *FT* probabilistic models as proposed in subsections 2.1 and 2.2, respectively, contain sources of uncertainty (Khalil & Mosher, 2008) that include: a) shear randomness of some events, b) phenomenologically-driven events, and c) model completeness which reflects the degree to which a proposed probabilistic model could accurately represent the physical system or phenomenon being modeled. The first source of uncertainty is called aleatory uncertainty which, unfortunately, cannot be reduced by improving the state of knowledge about the event. The second source is called epistemic uncertainty, which can be reduced as the state of knowledge about the event increases through the use of physics-based models or by drawing insights from dedicated experimental procedures. The *ET* top events (Fig. 2) contain a combination of aleatory and epistemic events triggered by the vehicular collision (*VC*) as the accident initiator. Aside from the stochastic/ aleatory top event (*R*), *i.e.*, rupture of the hydride storage vessel, the remaining top events *D*, *E*, *W*, and *F* represent a chain of phenomenologically-driven events, namely: a) hydride dust dispersal as a cloud of fine particles that may remain suspended in air or possibly coagulate into coarser particles (clumps) that settle by gravitational force to form a dust pile on the ground beneath or near the crashed vehicle, b) all, or part of, the ejected hydride dust could contribute to the cloud explosion, and c) the ejected hydride dust may come in contact with water of any source (*e.g.*, wet ground, rain, or just the moisture in air) and chemically react, and d) hydrogen fire breakout that may occur; given dust cloud explosion or hydride reaction with water leading to hydrogen gas release.

The aleatory and epistemic sources of uncertainty can be propagated through the risk models by assigning appropriate probability distributions to the basic events (*BE*) in the *FT* models and to the *ET* top events. For example, the *ET* top event (*D*) which represents dust dispersal in air can be modeled by a lognormal distribution with some shape parameter, while a Gaussian distribution (with some mean and a standard deviation) could be used for the *ET* top event (*R*) that models the hydride storage vessel rupture. Other types of probability distributions that are commonly used in *PRA* include Beta (β), Gamma (γ), and the exponential distributions.

Additionally, most statistical software packages can be used to generate best fit probability distributions from experimental or field failure data. In cases where field failure data are scarce or even non-existent, use of probabilities based on expert judgment elicitation (Khalil & Mosher, 2008) or surrogate data would be acceptable as initial estimations to be revised as more representative data become available.

To perform the uncertainty analysis, *PRAQuant* in *CAFTA* is used to convert each accident sequence in the *ET* model into an equivalent *FT* model where the sequence end-state becomes the top gate of an equivalent *FT* logic. *CAFTA* applies DeMorgan's theorem for the negation of a given *ET* top event along the accident progression path (Fig. 2) using a *NOT* gate/ *NAND* gate within the equivalent *FT* model. The DeMorgan's theorem can be expressed by equations (1) and (2) as follows below:

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

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

Where:

E_i = Probability of occurrence of event (i).

$\overline{E_i} = 1 - E_i$ = Complement of event (i) = Probability of event (i) not occurring.

The symbols $\cup$ and $\cap$ in the set theory refer to the union and intersection, respectively, of probabilistic events (where $i = 1, 2, \dots n$).

Fig. 4 shows the equivalent *FT* mode for Seq-11 in the *ET* model (Fig. 2). This sequence contains only failure paths signifying that *ET* top events *VC*, *R*, *D*, *E*, and *F* have occurred. The straight vertical line between gates SEQ-11 and SEQ-11P represents equivalence of gates in *CAFTA*'s terminology. The equivalent *FT* model has one *AND* gate, one accident initiator *VC* (shown by the arrow symbol), and three basic events representing the *ET* top events *R*, *D*, *E*, and *F*, respectively.

Fig. 4. An equivalent *FT* model for Seq-11 shown in the *ET* model in Fig. 2.

An example of how an accident sequence containing failure and success paths is converted into an equivalent *FT* model is depicted in Fig. 5. In this example, an equivalent *FT* model is generated from Seq-09 in the *ET* model (Fig. 2). The *FT* model shows the equivalence of SEQ-09 and SEQ-09P gates and contains one *AND* gate, one *NOT* gate (*N_E*) signifying the negation of top event (*E*), one accident initiator (*VC*), and four basic events, *R*, *D*, *W*, and *F*.

Fig. 5. An equivalent *FT* model for Seq-09 shown in the *ET* model in Fig. 2.

The *CAFTA* platform employs two commonly used techniques for uncertainty analysis, namely, Monte Carlo Sampling (*MCS*) and the Latin Hypercube Sampling (*LHS*), respectively. Besides the *CAFTA* platform, other software packages that contain *MCS* and *LHS* capabilities include the Oracle Crystal Ball⁴ and SAPHIRE.⁵

In the present study, the *LHS* technique has been deliberately selected for uncertainty analysis in order to avoid the concern about potential clustering of the sampled data when the *MCS* technique is employed. Clustering occurs when sampled data does not cover the entire basic event probability distribution. The *LHS* technique averts data clustering by using a stratified sampling method where the basic event probability distribution is divided into equal intervals and the stratification algorithm forces the sampling process to randomly draw probabilities from within each interval of the probability distribution. In this study, the *UNCERT* program has been employed for the uncertainty analysis using *LHS* technique (based on 30,000 samples) and the results are discussed in subsection 3.3 and reported in Table 2 as the upper bound (95th percentile) probabilities of occurrence.

Triangular probability distributions are assumed for the *ET* top events *R*, *D*, *E*, *W*, *F*, *F1*, and *F2* (Fig. 2). Each triangular distribution has a lower bound probability (LB), mean probability, and an upper bound probability (UB). These *ET* top events are also shown as basic events in the equivalent *FT* models (Figs. 4 and 5). Because event *R* is stochastic in nature and, thus, expected to have the highest uncertainty as discussed in Subsection 2.1, its mean probability was assumed to increase by a factor of 10 to produce an UB value and to decrease by a factor of 10 to produce a LB value. Events *D*, *E*, *W*, *F*, *F1*, *F2* are epistemic and, thus, expected to have less uncertainty around their mean probability values. In each of these epistemic events, an UB value was generated by assuming a 10% increase in its mean value and a LB value was generated by reducing its mean value by 10%. Table 3 summarizes the triangular probability distributions of events *R*, *D*, *E*, *W*, *F*, *F1*, and *F2*, respectively.

⁴ Oracle® Crystal Ball, release 11.1.2.3, Oracle Inc., Redwood City, CA.

⁵ Developed by Idaho National Engineering Laboratory (INEL) for the Nuclear Regulatory Commission (NRC).

2.5 Risk importance measures of basic events (BE) in the FT model

As depicted in the *ET* model (Fig. 2), the end states of some of the accident sequences may involve one type of risk such as the occurrence of hydride dust cloud explosion or hydrogen fire breakout. Other accident sequences may involve the occurrence of both types of risks, namely, dust cloud explosion and hydrogen fire breakout. As discussed in subsection 2.4, these accident sequences are converted into equivalent *FT* models for the purpose of uncertainty analysis. To rank order the risk contribution of basic events that constitute any cutset within the *FT* model, the *CAFTA* platform allows calculation of two risk importance measures, namely, Fussel-Vesely (*F-V*) and the risk achievement worth (*RAW*). Table 1 summarizes the risk importance measures commonly employed in the probabilistic risk assessment (*PRA*) field.

Table 1

Risk importance measures of components and events.

It should be noted that $Risk_{BC}$ signifies the risk associated with the base case (*i.e.*, mean) probabilities, $Risk_{P_i=0}$ signifies the risk associated with the case where the probability of occurrence of basic event *i* is set to zero, and $Risk_{P_i=1}$ signifies the risk associated with the case where the probability of occurrence of the basic event *i* is set to 1. Accordingly, for the base case risk, *F-V* should equal to 0, *RRW* should equal to 1, *RAW* should equal to 1, and *BI* should equal to zero. Moreover, a correlation between *F-V* and *RRW* can be derived as shown by equation (3):

$$F - V = 1 - \frac{Risk_{P_i=0}}{Risk_{BC}} = 1 - \frac{1}{RRW} \quad \dots \dots (3)$$

Again, for the base case where $Risk_{P_i=0} = Risk_{BC}$, then $RRW = 1$ and from Eq. (5), $F-V = 0$.

3. Results and Discussion

3.1 ET model quantification

As discussed in subsection 2.1, Fig. 2 depicts the *ET* model for the postulated vehicular collision (*VC*) as the accident initiating event. Table 2 lists the 11 *MECE* accident sequences and their Boolean equations. The *ET* model is quantified using the *ETA-II* software (part of the *CAFTA* program) for the base case where the mean probability values of the *ET* top events (*R*, *D*, *E*, *W*, and *F*) are used. The quantification results of this base case are shown in the third column of Table 2. Each of these *MECEs* has the opportunity to occur alone with some mean probability as depicted in the third column of Table 2. In the Boolean equations shown in the second column of

Table 2, $\bar{P}_i$ represents the complement probability of P_i (*i.e.*, $\bar{P}_i = 1 - P_i$) where *i* represent one of the *ET* top events *R*, *D*, *E*, *W*, and *F* (Fig. 2). Moreover, the summation of the sequence probabilities in the third column of Table 2 should equal to 1.0, which is the normalized value of the *VC* initiating event probability. It should be noted that in sequences Seq-02, Seq-03, Seq-04,

and Seq-05, dispersal of the hydride dust in air (D) does not occur (which is one of the five conditions required for dust cloud explosion to occur) and, hence, ET top event “ E ” becomes irrelevant for these sequences (Fig. 2). The probabilities assigned to top events R , D , E , W , and F , respectively, are provided in Table 3.

Table 2
Accident sequences of the event tree (ET) model.

Table 3
Probabilities of top events in the ET model (Fig. 2).

In this study, it should be noted that the VC conditional probability (i.e., $P_{VC} = 1$) has been deliberately used (compared to using a VC marginal probability) since accident collision statistics of fuel cell powered vehicles with on-board hydrogen storage systems is nonexistent. The sequence probabilities shown in Table 2 should be multiplied by VC IEF value when such statistical data become available in the future.

The probabilities of the ET branches/ split fractions (associated with D , E , W , and F as depicted in Fig. 2) are estimated based on insights generated from a comprehensive experimental program performed by Khalil (2010a; 2013a; 2013b; 2013c). To estimate a realistic probability for the dispersal of the hydride dust in air (D), Khalil (2010b; 2011a; 2011b) fabricated a test rig that mimics fast depressurization (blowdown) of a 15-ml stainless steel vessel containing 30 grams of $NaAlH_4$ power. To perform this test, the vessel (containing the hydride powder) is initially pressurized to 100 bar using nitrogen gas. Fast depressurization to about 10 bar occurs in about 50 msec and is achieved by the sudden opening of a rupture disk that mimics vessel rupture. The results of this series of replicated tests show that the probability of dust dispersal is about 16.5 % where portions of the hydride mass are dispersed into a receiving powder collection vessel (located downstream of the rupture disk) upon fast depressurization of the hydride storage vessel. Fig. 6 shows the fast depressurization test rig. It should be noted that due to safety requirements in our test laboratory, pressurized nitrogen gas has been used in the lowdown tests instead of pressurized hydrogen gas.

Fig. 6. Fast depressurization (blowdown) test rig to mimic rupture of the hydride storage vessel (Khalil, 2010a; 2011a; 2011b).

To estimate a reasonable probability for the hydride dust cloud explosion (E), Khalil (2013a; 2013b; 2013c) conducted a series of dust cloud explosion tests on several candidate hydrogen storage materials including $NaAlH_4$. These tests follow ASTM standardized test protocols (ASTM, 2005; ASTM, 2006; ASTM 2007; ASTM, 2008). Fig. 7 shows a schematic diagram of

the Kühner 20-liter spherical apparatus used for the dust cloud explosion tests for NaAlH_4 powder as the representative candidate of the reversible hydrides.

Fig. 7 - Schematic diagram of the Kühner 20-liter spherical explosion test apparatus (Khalil, 2013a; 2013b; 2013c).

Furthermore, a series of tests were conducted to investigate the degree of pyrophoricity of NaAlH_4 powder upon contacting water (Khalil, 2010a; Khalil, 2011b). Fig. 8 shows the vigorous hydride powder chemical reactivity upon contact with water and the observed hydrogen flames. Again, these experimental observations provided the basis of the assigned probabilities of the ET branches “W”, and “F,” respectively.

Fig. 8. Pyrophoricity of NaAlH_4 powder upon contacting water (Khalil, 2010a; Khalil, 2011b).

With respect to estimating the probability of occurrence of *ET* top event (*R*), rupture of the hydride storage vessel, this study assumes 50% of the geometric mean of the two probabilities $5.09\text{E-}3$ and $4.45\text{E-}3$ reported by Chamberlin (2004) for *CNG* Type-I vessel rupture. Furthermore, the derived probability is slightly adjusted to account for the fact that the maximum operating pressure for the reversible hydride is lower than that of the *CNG* vessel, namely, 100-bar versus 250-bar (Wong, 2009). While the estimated probability of hydride storage vessel rupture may not be accurate, it however provides an initial estimation which could be further refined as more specific catastrophic rupture failure data for Type-III and Type-IV hydride storage vessel become available.⁶ Additionally, a bounding analysis has been conducted in the present study to reduce the impact of the uncertainty caused by using the *CNG* Type-I vessel as a surrogate for the proposed Type-III or Type-IV vessel for on-board reversible hydrogen storage systems.

Using the *ET* structure shown in Fig. 2 and data in Table 2, the end states mean probabilities of accident sequences that lead to hydride dust cloud explosion (Seq-10), hydrogen fire breakout (Seq-03, Seq-05, Seq-07, and Seq-09), or both dust cloud explosion and hydrogen fire breakout (Seq-11) are summed up. The percent contribution of each of these six mutually exclusive

⁶ The new data could be field/ in-service failure data, experimental observations, or physics of failure (*PoF*) predictions.

accident sequences is calculated by dividing each end state probability by the summation value⁷ and the results are summarized in Fig. 9.

Fig. 9. Base case percent contributions of mutually exclusive accident sequences leading to hydride dust explosion, hydrogen fire breakout, or both dust explosion and fire breakout.

3.2 FT models quantification

As discussed in subsection 2.2, *CAFTA* software is used to develop the *FT* model and assign the basic events probabilities as shown in Figures 3a and 3b. The *GTPROB* subroutine in *CAFTA* is used to calculate the probability of each gate in the *FT* model such as G001, G002, and others. The contribution of each cutset to the *FT* top gate (*E*) probability is calculated using *CAFTA*'s cutset generator subroutine. Fig. 10 shows the percent contribution of each of the five cutsets (as described in Subsection 2.2) to the *FT* top gate (*E*). Cutset #1 which represents the product of the basic events G002, G003, G004, and G005 has the dominant contribution (46.1%) to the *FT* top gate (*E*) probability followed by cutset #2 which represents the product of the basic events G002, G003, G004, and G006. Cutset #2 contributes 36.4% to the *FT* top gate probability.

Fig. 10. Percent contributions of cutsets to the *FT* top gate (*E*) shown in Figs. 3a and 3b.

3.3 Uncertainty analysis

Table 2 summarizes the upper bound (95th percentile) probabilities of occurrence of the *MECE* accident sequences shown in the *ET* model (Fig. 2). The *LHS* methodology has been used to propagate events' uncertainty through the accident sequences after being converted into equivalent fault trees.

The same approach used for generating the results displayed in Fig. 10 has been applied to show the results for the upper bound (95th percentile) case as depicted in Fig. 11. As is clear from Fig. 11, the probability of occurrence, shown as a percentage of the total, of each of the six mutually exclusive sequences (Seq-03, Seq-05, Seq-07, Seq-09, Seq-10, and Seq-11) follow the same trend shown in Fig. 10; however, the percentages are different for the upper bound case compared to the base case.

⁷ From Table 2, the sum of end states mean probabilities of Seq-03, Seq-05, Seq-07, Seq-09, Seq-10, and Seq-11 = 1.475E-3

Fig. 11. Upper bound (95th percentile) percent contributions of mutually exclusive accident sequences leading to hydride dust cloud explosion, hydrogen fire breakout, or both dust cloud explosion and hydrogen fire breakout.

3.4 Sequence outcome and safety implications

Table 4 summarizes the safety implications of each outcome of the 11 accident sequences identified in the event tree model (Fig. 2), with probabilities of occurrence as reported in Table 2. From Table 4, it is clear that Seq-01 represents the safest outcome where the on-board hydrogen storage vessel did not rupture as a result of the postulated vehicular collision. The worst case sequence is represented by Seq-11 where the on-board storage vessel ruptured as a result of the collision leading to dust cloud explosion and hydrogen fire breakout. Sequence Seq-10 is less severe than Seq-11 as dust cloud explosion occurred without hydrogen fire breakout.

Table 4
Safety implications of the identified accident sequences (Fig. 2).

4. Conclusions and Recommendations

The focus of this study was on the hazards from a potential vehicular collision affecting the on-board hydride-based hydrogen storage vessel. A probabilistic framework has been proposed for conducting quantitative risk analysis (*QRA*) of on-board reversible hydrogen storage systems. The functionality of the *QRA* framework has been demonstrated by presenting a case study of a postulated vehicular collision as the accident initiator and an event tree (*ET*) model has been developed for this initiator. The *ET* model contains 11 mutually exclusive and collectively exhaustive accident sequences. A detailed fault tree (*FT*) model has been developed for the *ET* top event (*E*) that represents hydride dust cloud explosion. The end states of the *ET* accident sequences are quantified using *ET/FT* linking methodology. Each *ET* sequence is converted to an equivalent *FT* model to enable performance of uncertainty analysis of the *FT* top gate using the Latin Hypercube sampling technique. The risk importance measures of basic events in the *FT* model are determined and ranked using *F-V* and *RAW* methods.

The key conclusions and recommendations for future work can be summarized as follows:

- (a) In this study, the proposed *QRA* framework was applied to on-board reversible hydrogen storage systems using NaAlH_4 as a candidate solid-state storage medium. For future work, the proposed *QRA* framework should be applied to off-board regenerable hydrogen storage system with storage media like alane (AlH_3) and ammonia borane (NH_3BH_3).
- (b) The proposed *QRA* framework should also be extended in the future to include other failures of components (such as piping, valves, etc.) and subsystems (such as PEMFC stack) in addition to the on-board hydrogen storage vessel.
- (c) The study showed the risk-significance of the on-board hydride containing vessel and the importance of maintaining its structural integrity under worst case scenarios such as a

vehicular collision leading to vessel rupture, hydride dust explosion, and hydrogen fire breakout. Hence, further research to better understand the vessel's structural response to high-energy mechanical impact would be highly recommended. Future research in this area could include physics-of-failure (*PoF*) modeling and experimentation (above and beyond the standardized gunshot test (Wong, 2009). Moreover, testing the integrity of the vessel when subjected to high-energy mechanical impact should be done not only for a new vessel (i.e., at beginning of life), but also after repeated cycles of pressurization and depressurization as the induced cyclical fatigue weakens the vessel's structural integrity over time.

- (d) Additional empirical studies are recommended to better understand the physical phenomena associated with hydride dust dispersal, suspension in air, or agglomeration and deposition following rupture of the pressurized hydride vessel. Also, it would be informative to better understand safety implications of compounding/ interaction effect when a mixture of hydride dust and hydrogen gas is suddenly exposed to air.
- (e) Due to the non-existence of historical failure data and field operating experience to support risk quantification of on-board hydrogen storage systems, expert opinion pooling and use of available data for surrogate components could be leveraged as initial estimates with the understanding that as more reliable and relevant data become available, the risk models could be refined accordingly.
- (f) Event tree accident sequences with end states representing hydride dust cloud explosion, hydrogen fire, or both should be further developed to quantify potential safety and property damage consequences.

Acknowledgements

This material is based upon work supported by the Department of Energy under Award Number DE-FC36-07GO17032.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Technical support provided by Mr. Ronald Brown and Dr. Fanping Sun (of the United Technologies Research Center) during the fast depressurization (blowdown) tests are very much appreciated.

References

SAE J1739 (2002, August). Potential failure mode and effects analysis in design (Design FMEA), potential failure mode and effects analysis in manufacturing and assembly processes

(Process FMEA), and potential failure modes and effects analysis for machinery (Machinery FMEA). *SAE International*, Warrendale, PA.

MIL-STD-1629 (1980, November 24). Procedures for performing a failure modes and effects analysis. Military Standard, Department of Defense, Washington, DC. Retrieved from: <https://src.alionscience.com/pdf/MIL-STD-1629RevA.pdf>

Khalil, Y. F. (2011). Reciprocity of safety insights between risk analysis and codes and standards of vehicular hydrogen storage. *Proceedings of Risk Management*, American Nuclear Society (ANS), ISBN 978-0-89448-074-4, pp. 277-283.

Khalil, Y. F. (2009). Risk assessment and safety analysis for commercial nuclear reactors. Chapter 16 in *Nuclear Engineering Handbook*, Chapter 16: CRC Press, Taylor and Francis Group, ISBN/ISSN 1420053906.

Khalil, Y.F. (2000, April 2-6). Risk-informing the management of nuclear assets. *Proceedings of 8th International Conference of Nuclear Engineering*, Paper # ICONE-8683, Baltimore, MD.

Khalil, Y.F. (2010a). Selected risk mitigation tests and failure mechanisms of on-board vehicle hydrogen storage systems. Invited Paper, Hydrogen Safety Task 31, International Energy Agency, Rome, Italy, October 4–6. <http://iea.hia.net/Task31/default.aspx>

Khalil, Y.F. (2013a). Experimental determination of dust cloud deflagration parameters of selected hydrogen storage materials: complex metal hydrides, chemical hydrides, and adsorbents. *Journal of Loss Prevention in the Process Industries*, 26, 96-103.

Khalil, Y.F. (2013b). Experimental investigation of the complex deflagration phenomena of hybrid mixtures of activated carbon dust/hydrogen/air. *Journal of Loss Prevention in the Process Industries*, 26, 1027-1038.

Khalil, Y.F. et al. (2013c). Experimental and theoretical investigations for mitigating NaAlH₄ reactivity risks during postulated accident scenarios involving exposure to air and water. *Process Safety and Environmental Protection, IChemE*, 91, 463-475.

Event tree analysis (ETA-II) software package (2007, December 21). *Risk and Safety Management Program*, Electric Power Research Institute (EPRI), Palo Alto, CA, 94304.

Computer aided fault tree analysis (CAFTA 5.3) software package (2007, December 21). *Risk and Safety Management Program*, Electric Power Research Institute (EPRI), Palo Alto, CA, 94304.

Chamberlain, S. S. (2004). Development of a physics of failure model and quantitative assessment of fire fatality risks of compressed natural gas bus cylinders. *Doctoral Dissertation*, University of Maryland, College Park, MD.

Khalil, Y. F. and D. A. Mosher, (2008, September 7-11). 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, Knoxville, TN.

Khalil, Y.F. (2010b). Quantification & addressing the DOE material reactivity requirements with analysis and testing of hydrogen storage materials and systems. *FY 2010 Annual Progress Report*. http://www.hydrogen.energy.gov/pdfs/progress10/IV_e_4_Khalil.pdf

Khalil, Y. F. (2011a). Quantifying and addressing the DOE material reactivity requirements with analysis and testing of hydrogen storage materials and systems. *FY 2011 Annual Progress Report IV.E.1*, DOE Hydrogen and Fuel Cells Program, 538-543.
http://www.hydrogen.energy.gov/pdfs/progress11/iv_e_1_khalil_2011.pdf

Khalil, Y.F. (2011b, September 14-16). Reactivity characterization tests for selected solid-state hydrogen storage materials. In: *Proceedings of the 4th World Hydrogen Technologies Conference (WHTC2011)*, Glasgow, Scotland. [http://www.whtc2011.org.uk/WHTC programme.pdf](http://www.whtc2011.org.uk/WHTC_programme.pdf)

ASTM. (2005). Standard test method for pressure and rate of pressure rise for combustible dusts - E-1226-05. West Conshohocken, PA: ASTM International.

ASTM. (2006). Standard test method for minimum autoignition temperature of dust clouds - E-1491-06. West Conshohocken, PA: ASTM International.

ASTM. (2007). Standard test method for minimum explosible concentration of combustible dusts - E-1515-07. West Conshohocken, PA: ASTM International.

ASTM. (2008). Standard test method for minimum ignition energy of a dust cloud in air - E-2019-03. West Conshohocken: ASTM international.

Wong, J. (2009, December 10). CNG & hydrogen tank safety, R&D, and testing. Powertech Labs Inc. Retrieved from:
http://energy.gov/sites/prod/files/2014/03/f10/cng_h2_workshop_8_wong.pdf

Table 1

Risk importance measures of components and events.

Risk Importance Measure ^a	Definition
Fussell-Vesely (<i>F-V</i>)	$\frac{Risk_{BC} - Risk_{P_i=0}}{Risk_{BC}}$
Risk reduction worth (<i>RRW</i>)	$\frac{Risk_{BC}}{Risk_{P_i=0}}$
Risk achievement worth (<i>RAW</i>)	$\frac{Risk_{P_i=1}}{Risk_{BC}}$
Birnbaum importance (<i>BI</i>)	$Risk_{P_i=1} - Risk_{BC}$

^a *CAFTA* calculates only two importance measures, namely, *F-V* and *RAW*. However, *RRW* can be calculated using Eq. (5) derived in this study.

Table 2
Accident sequences of the event tree model.

Accident Sequence	Boolean Equation	Sequence Mean Probability	Upper Bound Probability (95 th Percentile)
Seq-01	$P_{VC} \cap \bar{P}_R$	9.98E-1	9.99E-1
Seq-02	$P_{VC} \cap P_R \cap \bar{P}_D \cap \bar{P}_W \cap \bar{P}_F$	4.55E-4	4.93E-3
Seq-03	$P_{VC} \cap P_R \cap \bar{P}_D \cap \bar{P}_W \cap P_F$	1.14E-4	1.47E-3
Seq-04	$P_{VC} \cap P_R \cap \bar{P}_D \cap P_W \cap \bar{P}_{F1}$	3.32E-4	4.38E-3
Seq-05	$P_{VC} \cap P_R \cap \bar{P}_D \cap P_W \cap P_{F1}$	9.95E-4	8.16E-3
Seq-06	$P_{VC} \cap P_R \cap P_D \cap \bar{P}_E \cap \bar{P}_W \cap \bar{P}_F$	4.49E-6	4.23E-4
Seq-07	$P_{VC} \cap P_R \cap P_D \cap \bar{P}_E \cap \bar{P}_W \cap P_F$	1.12E-6	1.16E-4
Seq-08	$P_{VC} \cap P_R \cap P_D \cap \bar{P}_E \cap P_W \cap \bar{P}_{F1}$	3.28E-6	3.67E-4
Seq-09	$P_{VC} \cap P_R \cap P_D \cap \bar{P}_E \cap P_W \cap P_{F1}$	9.83E-6	6.69E-4
Seq-10	$P_{VC} \cap P_R \cap P_D \cap P_E \cap \bar{P}_{F2}$	5.34E-5	1.16E-3
Seq-11	$P_{VC} \cap P_R \cap P_D \cap P_E \cap P_{F2}$	3.02E-4	2.49E-3

Table 3
Probabilities of top events in the ET model (Fig. 2).

Top Event	Assigned Probabilities (Mean, LB, UB)
Rupture of hydride storage vessel (R)	(0.00227, 0.000227, 0.0227)
Dispersal of hydride dust in air (D)	(0.165, 0.149, 0.182)
Dust cloud explosion (E)	(0.95, 0.855, 0.998)
Dust contacts water and chemically reacts (W)	(0.70, 0.63, 0.77)
H ₂ fire breakout (F) in Seq. 03 and Seq-07	(0.20, 0.18, 0.22)
H ₂ fire breakout (F1) in Seq. 05 and Seq-09	(0.75, 0.675, 0.825)
H ₂ fire breakout (F2) in Seq. 11	(0.85, 0.765, 0.935)

UB = upper bound probability

LB = lower bound probability

Table 4
Safety implications of the identified accident sequences (Fig. 2).

Accident Sequence	Sequence Outcome Safety Implications
Seq-01	Safe outcome – no vessel rupture
Seq-02	Vessel ruptured but no H ₂ fire occurred
Seq-03	Vessel ruptured and H ₂ fire occurred
Seq-04	Vessel ruptured, hydride dust chemically reacted with water but no H ₂ fire occurred
Seq-05	Same as Seq-04 but H ₂ fire occurred
Seq-06	Vessel ruptured, hydride dust dispersed in air, but no H ₂ fire occurred
Seq-07	Same as Seq-06 but H ₂ fire occurred
Seq-08	Vessel ruptured, hydride dust dispersed in air, but no H ₂ fire occurred
Seq-09	Same as Seq-09 but H ₂ fire occurred
Seq-10	Vessel ruptured, dust cloud explosion occurred, but no H ₂ fire occurred
Seq-11	Same as Seq-10, but H ₂ fire occurred

Fig. 1. Proposed *QRA* framework for on-board hydrogen storage systems.

Fig. 2. Probabilistic event tree (ET) model for a vehicular collision (VC) as an accident initiator.

Fig. 3a. Probabilistic fault tree (FT) model for hydride dust cloud explosion (E) (Subtree of transfer gate G008 shown in Fig. 3b).

Fig. 3b. Subtree of gate G008 (*i.e.*, the transfer gate shown with the triangle symbol in the probabilistic fault tree (FT) model in Fig. 3a).

Fig. 4. An equivalent *FT* model for Seq-11 shown in the *ET* model in Fig. 2.

Fig. 5. An equivalent *FT* model for Seq-09 shown in the *ET* model in Fig. 2.

Fig. 6. Fast depressurization (blowdown) test rig to mimic rupture of the hydride storage vessel (Khalil, 2010b; 2011a; 2011b).

Fig. 7 - Schematic diagram of the Kühner 20-liter spherical explosion test apparatus (Khalil, 2013a; 2013b; 2013c).

Fig. 8. Pyrophoricity of NaAlH_4 powder upon contacting water (Khalil, 2010a; 2011b).

Fig. 9. Basecase percent contributions of mutually exclusive accident sequences leading to hydride dust explosion, hydrogen fire breakout, or both dust explosion and fire breakout.

Fig. 10. Percent contributions of cutsets to the *FT* top gate (*E*) shown in Figs. 3a and 3b.

Fig. 11. Upper bound (95th percentile) percent contributions of mutually exclusive accident sequences leading to hydride dust cloud explosion, hydrogen fire breakout, or both dust cloud explosion and hydrogen fire breakout.