Battery Hazard Modes and Risk Mitigation Analysis

Cyrus N. Ashtiani

Introduction

The safety of the on-board battery in electric, hybrid, and plug-in vehicles is of paramount importance to the U.S. automakers. Several high profile Li-Ion battery fire incidents in 2006 that resulted in recall of millions of laptop computers provided further evidence that even the estimated hazardous failure rates of 1 in tens of million cells could be potentially devastating to the nascent HEV industry.

In early 2006, The United States Advance Battery Consortium (USABC) took the task of developing a methodology for assessment of Rechargeable Energy Storage Systems (RESS) safety. A review of the existing battery safety and abuse tolerance test procedures used by FreedomCAR(1), USABC(2), EUCAR(3), and SAE(4), and Sandia National Lab(5), reveals that these procedures essentially subject the battery to various abuse conditions and then monitor and characterize the battery behavior. The abuse conditions often include disabling pack, module, and cell protection devices, depending on whether they are active or passive. An active protection device relies on an external system for protection or control of the device. An example is a contactor which can break the current path based on a control signal from the battery management system. At the cell and module level, the contactor is an active protection device. At the battery pack level, even though the contactor is part of the battery system, it could still be considered an active protection device for the fact that it needs a 12V supply from outside the pack. An example of passive protection is a cell built-in Current Interrupt Switch (CIS) which is being activated by the internal gas pressure or a bimetal switch which is activated by the internal temperature of the cell.

The abuse tests, while providing a lot of information about battery behavior during abusive conditions, fall short of putting the wealth of this data into a practical procedure for the design engineers to utilize. It lacks the system perspective and does not include the likelihood of the hazards, the risks posed by them, and more importantly, a systematic methodology to find and assess the most effective ways of reducing the risks.

This document describes a methodology named Hazard Modes & Risk Mitigation Analysis or HMRMA which is based on three principles:

1. Risk assessment & mitigation require quantifying risk
2. Should include all the sensing, control, & protection devices, and their effect all the way to the highest system level
3. Should serve as a tool in the design process at all levels - cell, module, pack, and finally the whole vehicle development level

HMRMA methodology involves two major steps. The first step is identification of hazards and calculation of the associated risks. The next major step, after identifying the hazards and risks, is called detection and control. These are the subjects of the next two sections in this paper.

Hazard Identification and Calculation of Risk

The first step in the HMRMA is identification of the hazards and calculation of the associated risks. Before we proceed further, we need to clearly define some of the key concepts beginning with hazard modes.

Hazard Modes

A hazard is defined as an externally or internally activated event that could potentially lead to material or at worse life threatening conditions. The hazards are pre-described and, in the case of RESS, fall into four categories:

i. Electrical Hazards Such as short-circuit, or overcharge are examples of externally activated hazards. The soft-short, i.e., an internal short resulting from often a locally compromised separator, is an example of an electrical hazard which is internally induced.
ii. Thermal Hazards Such as elevated temperatures, fire, etc. A thermal hazard could be activated externally or internally.
iii. Mechanical Hazards Representing conditions such as crush, nail-intrusion, drop, etc.
iv. System Hazards Result from events that initiate in the external system of which the battery is a part. Examples of this category are loss of high voltage line continuity, a chassis fault.

The hazard modes are summarized in table 1.

TABLE 1. Hazard Modes (Examples)

Electrical	Thermal	Mechanical	System
Short-Circuit	Fire	Crush	Contactor Fails Closed
Overcharge	Elevated Temp.	Nail Intrusion	Loss of HV Continuity
Soft Short		Drop	Chassis Fault

Severity

Each hazard is assigned an integer number in the range of [0, 7] representing, in the increasing order, the severity of the hazard. For a given hazard, the respective severity is judged based on the observed reactions or effects, when the test article is subjected to standard abusive tests devised to simulate that hazard (1). These effects, in the extreme include explosion, and release of toxic substances in excess of OSHA exposure limits (level 7), to simply a reversible loss of function (level 1).

Table 2 summarizes the severity levels, denoted by S, and the effect-based criteria for determining the severity of hazard. This table was, for the most part, adopted from EUCAR existing standards (2) to avoid confusion as well as creating a more broadly-accepted standard for safety analysis.

Table 2 . Severity Levels (Adopted and modified from EUCAR)

S	Description	Criteria for Severity Classification & Effects
0	No effect	No effect. No loss of functionality.
1	Reversible Loss of Function	No defect; no leakage; no venting, fire, or flame; no rupture; no explosion; no exothermic reaction or thermal runaway. Temporary loss of battery functionality. Resetting of protective device needed.
2	Irreversible Defect/Damage	No leakage; no venting, fire, or flame; no rupture; no explosion; no exothermic reaction or thermal runaway. RESS irreversibly damaged. Repair needed.
3	Leakage Δ mass < 50%	No venting, fire, or flame; no rupture; no explosion. Weight loss <50% of electrolyte weight. Light smoke (electrolyte = solvent + salt).
4	Venting Δ mass >= 50%	No fire or flame; no rupture; no explosion. Weight loss >=50% of electrolyte weight. Heavy smoke (electrolyte = solvent + salt)
5	Fire or Flame	No rupture; no explosion (*i.e.,* no flying parts).
6	Rupture	No explosion. RESS could disintegrate but slowly without flying parts of high thermal or kinetic energy
7	Explosion	Explosion (*i.e.,* disintegration of the RESS with externally damaging thermal & kinetic forces). Exposure to toxic substances in excess of OSHA limits

This EUCAR rating system was originally designed for determination of hazard severity at the cell level. In the context of HMRMA, however, it is extended with some minor adjustments, to serve at all levels of cell, module, pack, as well as the whole system design and development. Furthermore, even though terms like explosion, fire, venting, etc., might seem intuitively obvious, a more technically sound description of these terms could be found in (6).

Likelihood Level

Each hazard is assigned a number between [1, 10] representing the Rate of Occurrence (ROO) of the hazard over the life of the article. In hybrid and electric vehicles, the life of the battery pack is between 10 to 15 years, depending on the emission classification of the vehicle, and a load cycle life equivalent of 100k to 150k miles.

It should be noted that determination of the ROO in strict statistical sense, with a given margin of error and a certain confidence level, is prohibitively costly and time consuming. The likelihood numbers, denoted here by L, have a relative meaning very similar to the practice of Failure Modes & Effects Analysis (FMEA), widely used in the auto and aerospace industries (7). Often, historic data are available that help selection of the likelihood level. For instance, in the case of mechanical hazard "Crush", statistics exist to support the number crash incidents over the life of a vehicle. These numbers can be used to select the appropriate likelihood levels. In other occasions where statistical data are not available, an educated engineering guess should suffice to start the HMRMA process. Over the time, as more data become available, the HMRMA should reflect a revised likelihood level in accordance with the new data. Table 3 shows the likelihood levels as a function of the ROO in ppm or in %, over the life.

Table 3. Likelihood Levels

L n/u	ROO ppm - (%)	Description
10	100,000 (10%)	Extremely High
9	50,000 (5%)	Very High
8	20,000 (2%)	High
7	10,000 (1%)	Above Average
6	5000 (0.5%)	Average
5	2000 (0.2%)	Below Average
4	1000 (0.1%)	High Low
3	500 (0.05%)	Average Low
2	100 (0.01%)	Low
1	10 (0.001%)	Very Low

The likelihood levels, unlike severity levels, do not need to be an integer. If the ROO happens to fall between the two integers, use of fractional numbers are allowed. The likelihood level of L=0 corresponding to ROO=0 means the hazard is not likely to occur and does not need to be considered for risk analysis.

.

Hazard Risk Number and the Risk Space

The product of a hazard severity S, times the likelihood level of the hazard L, is a number called Hazard Risk Number and abbreviated as HRN:

$$HRN = S * L \qquad [1]$$

As the severity of a given hazard increases, the likelihood of the hazard has to be reduced to generate an acceptable HRN. If such an acceptable HRN is designated by R_0 then the constant-risk contour is defined by a hyperbola:

$$S * L = R_0 \qquad [2]$$

The constant risk counter [2] is represented by a hyperbolic curve that divides the two-dimensional space of "Severity vs. Likelihood", also referred to as the Risk Space, into a low risk and a high risk zones as shown in Fig. 1.

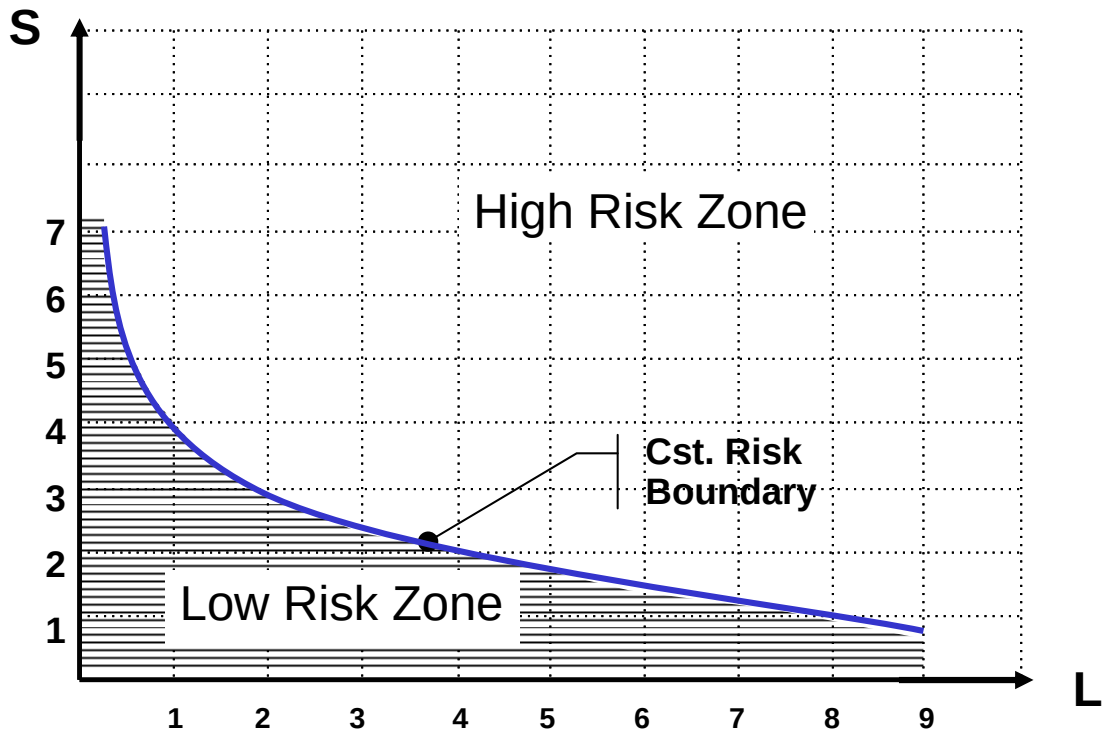

Figure 1. The Risk Space

Risk Space Boundaries

In addition to the boundary separating low and high risk zones in the risk space, there are usually other constraints that impose further limits on the area where the risk associated with all probable hazards should fall. For instance, an unacceptably high-severity hazard even though at low likelihood levels, may not be acceptable and impose a severity cut-off limit $S = S_L$. Likewise, a high rate of occurrence of an hazard with very low severity, as low as 1, points to an unreliable product and consequently imposes a likelihood cut-off limit $L = L_L$. These two limits along with a constant risk boundary of [2], enclose the low risk space as shown in Fig.2 by the shaded area.

The high severity cut-off and high-likelihood cut-off limits can be interpreted as zero-risk tolerance in these regions of the risk space. In reality, what it points out to is that the risk tolerance in these regions is much lesser than R_0 as represented by [2].

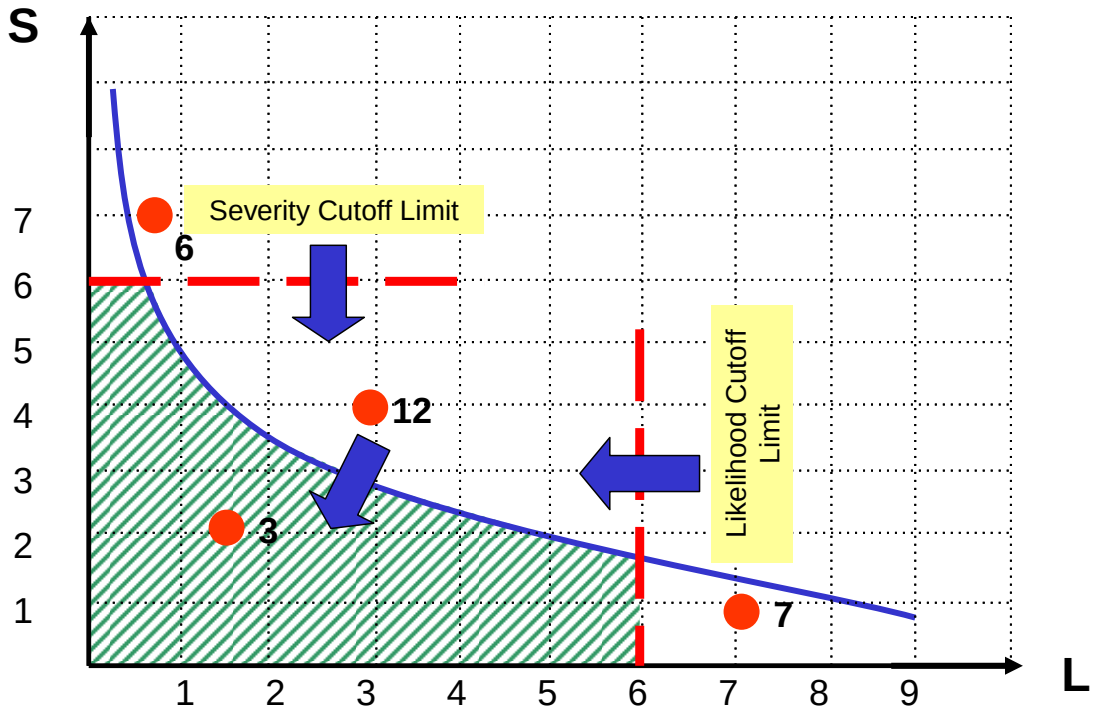

Figure 2. Risk Space Boundaries

Figure 2 shows the risk representations of four hazards on the risk space along with their respective risk numbers. In this hypothetical case, the remaining tasks are to bring the risk points associated with 6, 12, and 7 within the shaded area shown in this figure. This is the subject of the next section.

Hazard Detection and Control

So far we have focused on identifying the hazards and calculating the associated risks. In the following sections we will turn our focus on mitigating risks in terms of both implementation and calculation of the reduced risks. These concepts are collectively called hazard detection and controls which will be explained in the following:

Indicators

Indicators are referred to observable or detectable signs, signals, or in general information preceding occurrence of a hazard. The keyword here is preceding the on-set of the hazard, but it could also be extended to during a hazard and before one leads to another hazard, usually, of a higher severity. Indicators can be of different natures, such as hardware, software, or both. Examples of indicators are:

- A temperature sensor to detect overheating conditions
- An algorithm for predicting State-of-Charge used to detect overcharge condition
- An interlock wire to detect continuity of high power wiring

Indicators are used as feedback to pre-empt a hazardous condition either automatically by triggering an event interruption mechanism, or manually such as providing feedback to operators for manual intervention or avoidance of a hazardous situation.

Controls

Controls are referred to the means of reducing the occurrence or likelihood of a hazard by pre-emption or at best by prevention (L=0). The concept of controls are closely tied to indicators in the sense that often indicators provide the signals that point to a potential hazardous conditions and then the controls act in response to interrupt the sequence of events.

The controls can be put in two general categories:

I. Means to interrupt the sequence of events leading to a hazardous condition, examples of this category are:
   i. A pressure relief vent at the cell level. Such a vent will relieve the pressure buildup inside the cell before it reaches dangerous levels that could potentially lead to an explosion.
   ii. A contactor switch that could break the high power circuit during an event, such as a short-circuit, hence pre-empting a potential exothermic event.
   iii. A different type of control is locating the battery pack in the vehicle in a crush-protected zone. Such a control strategy will prevent battery from crushing in the event of an accident.
II. The second category of controls includes procedures and personnel & public training in dealing with, prevention and avoidance of hazardous conditions.

The Hazard Control Number The impact of a control is represented by a number in the range of [0 1] called the Hazard Control Number (HCN). When a control is devised, the original hazard likelihood level is reduced by a factor equal to HCN. As a result, the subsequent Hazard Risk Number in equation [1] will be reduced correspondingly:

$$HRN = S * L * HCN \quad [3]$$

Obviously an HCN=1 means no control scheme has been utilized and an HCN=0 means the control scheme has ultimately succeeded in preventing the associated hazard. For practical purposes, it is suggested that HCN values to be used in the increments of 0.1 as proposed in Table 4.

Table 4. Hazard Control Numbers (HCN)

HCN	Description
0.9	Modest Risk Reduction
0.8	
0.7	Above Average Risk Reduction
0.6	
0.5	
0.4	Notable Risk Reduction
0.3	
0.2	
0.1	Significant Risk Reduction
0.0	Prevention

Hazard Modes & Risk Mitigation Analysis; An Example

An example will help to illustrate how the HMRMA technique maybe employed to reduce risk associated with a given hazard. Suppose an overcharge abuse test to 200% SOC on a given cell resulted in venting, flames, and fire (5). Based on the effects from this abuse test, and referring to table 2, this hazard gets a severity rating of S=5. Further, assume we expect an event like this, i.e. cell overcharge to 200% SOC, to occur about 500 times total over the age of the vehicle in a fleet of 100,000 cars. This puts the rate of occurrence in the fleet at 5,000 ppm, which according to table 3 corresponds to a likelihood level of L=6. The initial Hazard Risk Number from equation [1] will then be calculated as HRN_0=30. Table 5 shows these numbers in the first three data columns, respectively. To mitigate this risk, several approaches can be considered. The very first possibility is to start at the cell fundamental electrochemical level. Examples of this kind are, introducing flame-retardant additives to the electrolyte, or even more fundamentally using different positive and/or negative active material. These approaches that change the cell at the very fundamental level are typically too time-consuming and require extensive work to test and validate. They also require repeating the steps mentioned in the above to identify hazard modes and the new severity levels, but won't affect the likelihood levels as long as their causes are external to the cell (such as the likelihood of overcharge).

A different approach is to leave the cell intact but use higher level system detection and controls to reduce the likelihood of the event. Such approaches could turn out to be much more effective and often less costly. For instance, if one adds several temperature sensors in critical locations within the pack to provide information on the cell temperatures and rate of rise of temperatures to the Battery Management System (BMS), then the BMS would be able to detect potential for overcharge and preemptively break the contactors or circuit-breakers. Depending on the system design and maturity, and characteristics of the cell in the event of overcharge, this will reduce cell O/C likelihood level by a modest factor, from table [4] by $HCN_1 = 0.7$ and the new hazard risk number will be reduced to:

$$HRN_1 = HRN_0 * HCN_1 = 21$$

This information regarding indicators, controls, and generally detection scheme #1 are captured in the subsequent columns in table 5. If the HRN of 21 is still above the target risk number, a second mitigation scheme will be devised as shown in the table, this time by adding voltage sensors to detect other indicators of O/C such as cell imbalance, voltage roll-over, or high rate of rise, whichever applies to the case, and the process is repeated to generate a lower risk number of

$$HRN_2 = HRN_1 * HCN_2 = 12.6$$

Table 5. Hazard Modes & Risk Mitigation Analysis (HMRMA)

Status	**0**			**Mitigation Scheme #1**		**1**		**Mitigation Scheme #2**		**2**	
Potential Hazard	**sev**	**lhd**	**hrn**	**I**	**C**	**hcn**	**hrn**	**I**	**C**	**hcn**	**hrn**
Overcharge	5	6	30	Add temp. sensors to detect overheating	T-Sensors w/feedback to BMS & contactor switch	0.7	21	Add voltage sensors to detect imbalance, voltage roll-over	V-Sensors w/feedback to BMS & contactor switch	0.6	12.6
Short-Circuit											
Crush											

The link below provides a template for HMRMA spreadsheet.

C:\Documents and Settings\t1654ca\My

Safety Gap Analysis

The USABC currently has several performance requirement tables for various automotive applications, EV, HEV, and most recently PHEV's. These tables are provided to help the battery manufacturers to properly design and develop for their target industry in the automotive propulsion applications. More recently, in July 2007, the USABC approved a similar safety requirement target as a minimum safety requirement for batteries. Table 6 below shows these requirements which are commonly referred to as the battery "Safety Gap Analysis" since it is used to measure various battery technology hazard risk numbers vs. the USABC target values.

Table 6. USABC Battery Safety Gap Analysis

Hazard Severity	Hazard Risk Numbers		
	USABC Target	Marginal	Unacceptable
1	< 7	≥ 7 < 8	≥ 8
2	< 12	≥ 12 < 14	≥ 14
3	< 15	≥ 15 < 18	≥ 18
4	< 16	≥ 16 < 20	≥ 20
5	< 15	≥ 15 < 20	≥ 20
6	< 12	≥ 12 < 18	≥ 18
7	< 7	≥ 7 < 14	≥ 14

Acknowledgments

This work has been completed with the support of the USABC and has benefited from input and many valuable discussions and comments from experts and colleagues at Chrysler, Ford, GM, Sandia National Lab, and SAE.

References

1. D. H. Doughty and C. C. Crafts, Sandia National Labs, June 2005, *FreedomCAR Electrical Energy Storage System Abuse Test Manual for Electric and Hybrid Electric Vehicle Applications*
2. D. Doughty, *First International Symposium on Large Lithium Ion Battery Technology and Application* (2005) ---- General USABC Test Proc
3. A. Schmolz, *EUCAR Safety Test Procedures for Modules of EV-Batteries* (May 1999)
4. SAE J2464, *Electric Vehicle Battery Abuse Testing* (1999)
5. T. Unkelhaeuser & D. Smallwood, *Sandia Laboratories Report* SAND99-0497, Electrochemical Storage System Abuse Test Procedure Manual, V 1.0 (1999)
6. Levy, S.C., Bro, P.: Battery Hazards and Accident Prevention Plenum Press, New York and London, 1994 ISBN 0-306-44758-4
7. DaimlerChrysler, Ford Motor Company, General Motors Corp., *Potential Failure Modes and Effects Analysis (FEMA)*, Reference Manual, Third Edition, July 2001.