

Application of System Safety Engineering Processes to Advanced Battery Safety

2011-01-1369

Published
04/12/2011Galen Ressler
General Motors Company

Copyright © 2011 SAE International

doi:[10.4271/2011-01-1369](https://doi.org/10.4271/2011-01-1369)

ABSTRACT

The battery system in the Chevrolet Volt is very complex and must balance a variety of performance criteria, including the safety of vehicle occupants and other users. In order to assure a thorough approach to battery system safety, a system safety engineering process was applied and found to provide a useful framework. This methodical approach began with the preliminary hazard analysis and continued through requirements definition, design development and, finally, validation. Potentially hazardous conditions related directly to functional safety (for example, charge control) and primary physical safety (for example, short circuit conditions) can all be addressed in this manner. Typical battery abuse testing, as well as newly defined limit testing, supported the effort. Extensive documentation, traceability and peer reviews helped to verify that all issues were addressed. A description of the process which was followed, specific examples of its application and recommendations for future refinement of the approach are provided.

INTRODUCTION

Expansion of electrical drive in more and more automobiles brings with it different considerations to assure occupant and public safety. In addition to high voltage electrical energy considerations, batteries may also include consideration for new thermal and material performance characteristics. All of this takes place in the context of automotive markets which have ever increasing expectations for comfort, style, performance, and safety. The introduction of the Chevrolet Volt takes a significant step forward in all these areas. Achieving the necessary safety performance for this large battery required an expanded application of known system safety process elements, as well as use of existing battery safety approaches.

The Chevrolet Volt battery system is made up of 288 lithium ion battery cells configured as 96 sets of 3 parallel cells connected in series. This results in a nominal pack voltage of 370 V. In order to achieve a driving range of 25 - 50 miles in all-electric mode (depending on terrain, driving techniques and temperature), the battery must provide approximately 10 kW-hr of usable energy. In addition, the battery must provide up to 115 kW discharge power (10 seconds) to achieve the necessary vehicle performance. The battery system is configured in a T shape and is located outside of the passenger compartment, beneath the vehicle tunnel and rear seat. It has a mass of 198 kg. See Matthe, et al [1] for more details on the configuration and development of the Volt battery system.

BATTERY SAFETY BACKGROUND

Battery safety is not a new consideration. Hazards associated with batteries, such as corrosive electrolyte and hydrogen gas generation are well known [2]. Over the past decade, as advanced battery technologies have developed for vehicle applications, battery safety testing methods have been developed and refined. See references [3, 4, 5] for examples. However, in nearly all cases, these standards either do not have specific criteria to be met for safety or they are primarily applicable to batteries with an aqueous electrolyte (such as lead acid or nickel metal hydride). So, when considering the safety of a lithium ion battery system, such as the case for Volt, no existing battery safety standards provide a complete definition of what is required.

Battery system hazards have a variety of forms and sources. One way to categorize these hazards is to consider how they relate to functional safety. These categories are:

- Hazards which are caused and mitigated by battery control systems. These are clearly functional safety conditions. An example is battery pack over-charge.

**Documents**
Document Sharing Hub

- Hazards which are detected and mitigated by battery control systems. These also are clearly functional safety conditions. An example is loss of high voltage electrical circuit isolation.
- Hazards which are detected and communicated by battery control systems. These are not functional safety conditions since the control system cannot take any mitigating actions. An example is excessive battery pack temperature caused by a source external to the battery.
- Hazards which are unrelated to the battery control systems. These are referred to as primary safety conditions. An example is a pack short circuit.

Prior work has proposed a framework for performing a comprehensive safety analysis on battery systems. Ashtiani [6], in 2007, proposed a method utilizing hazard severity level assessments and probability of occurrence as a method to complete an overall analysis. It incorporated aspects of existing test methodologies (specifically, the hazard severity level as defined in SAE J2464 [4]) but required estimates for probabilities which are unavailable. It is also largely based on qualitative criteria, making it difficult to clearly define acceptable safety limits.

An alternative method, capable of providing specific criteria and addressing all of the potential hazard causes, was needed for the Volt battery system. The alternative method selected was the GM system safety engineering process which helps address both random and systematic failure concerns.

VOLT BATTERY SYSTEM SAFETY PROCESS

System safety engineering is a specialized application of the system engineering process which has been documented for a variety of industries [7, 8, 9]. It applies the process of defining requirements, creating a design which meets those requirements, and verifying those requirements to the area of safety. In automotive applications, many vehicle manufacturers have applied this process to functional safety behavior, including electronic throttle control and active safety systems. In the case of advanced batteries, though, this methodology must be applied beyond functional safety to also include primary physical safety, such as high voltage access or short circuit behavior. Functional safety relates to safety issues which are due to malfunction of electrical/electronic devices while primary physical safety refers to intrinsic safety issues. The Chevrolet Volt battery system safety engineering process utilized an approach which addressed both functional and primary safety concerns.

The process as applied to the Volt battery system consisted of four phases. These are concept phase, requirements phase, design phase, and verification phase. See Figure 1. These phases necessarily correspond to similar development activities for the vehicle as a whole. In addition, they are

iterative in nature, particularly between the requirements and design phases and between the design and verification phases. The following sections detail the activities which were included in each phase for the Volt battery system safety development.

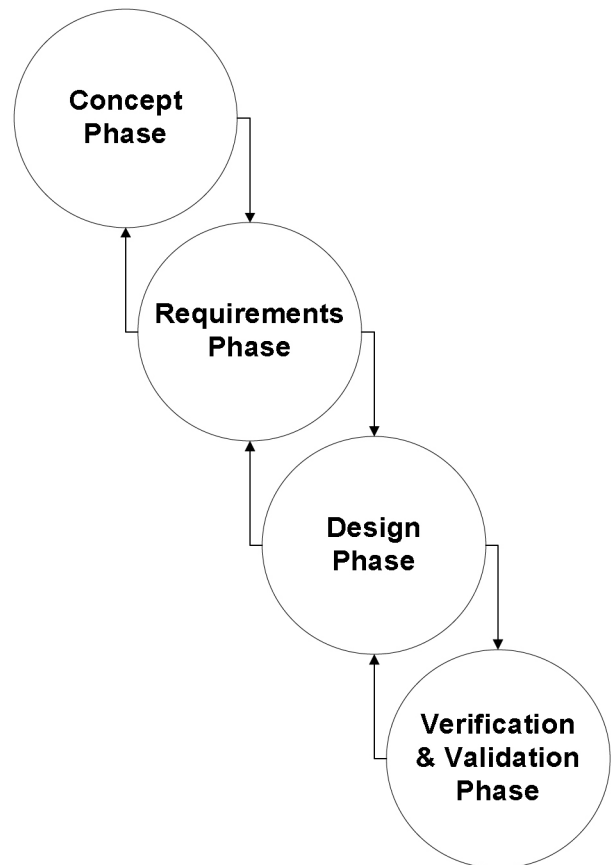


Figure 1. System Safety Process Overview

CONCEPT PHASE

The initial phase of the system safety process can be referred to as the “concept phase.” During this phase, the potential hazards of the system are identified and a strategy, or concept, is generated to mitigate those hazards. Preliminary hazard analysis (PHA) is the tool utilized to identify potential hazards. It is a simple, yet powerful, spreadsheet analysis which lists the potential hazards of the system, their possible causes, “worst case” scenario descriptions, mitigating conditions and, ultimately, a safety goal intended to mitigate the hazard in the final design. In order to support the subsequent analysis and define requirements, a ranking is assigned.

Risk classification was based on GM hazard and risk methodology which is consistent with the evolving ISO/DIS 26262 guidelines. Accordingly, an ASIL (Automotive Safety Integrity Level) value, adapted from ISO/DIS 26262 [7], was

assigned to each hazard, based on an assessment of the severity, exposure condition, and controllability. For the battery system, a total of 9 separate hazards were identified in [Table 1](#). An example analysis is shown below. These are similar to those identified in other battery safety analyses [2, 6].

In accordance with ISO/DIS 26262, severity is measured on a scale of S1 to S3, with S3 being the most severe. The hazards associated with batteries have the potential of severe injury which corresponds to a severity of S3 as shown in [Table 1](#). The only exception on this list is related to skin burn which would lead to a moderate injury level, S1.

Controllability is also assessed on a scale from C1 to C3. Guidance provided in the DIS, which describes the ability of a driver to control a vehicle to safe location and condition, does not apply directly to battery hazards. Instead, controllability was interpreted to relate to the ability of a person to control their exposure to the condition. In the case of the service environment, a service technician is trained and, therefore, has greater control over their exposure to high voltage. Flammable and toxic liquids would exist in locations which require an intentional act on the part of an individual in order to be exposed, due to the pack location outside of the passenger compartment. This was interpreted into a C1 assessment. Because the battery location is outside of the passenger compartment and the only portion potentially accessible to passengers is a manual disconnect device located beneath the center storage console, in the case of skin burn, a person would need to, again, take an intentional act to be exposed to the hazard.

Exposure is assessed on a scale of E1 to E4, with E4 being possible each time the vehicle is driven. In this case, all hazards except those related to the less frequent conditions of a vehicle crash or vehicle service, are possible in each drive situation. The exposure value was reduced in the case of a crash and battery service, consistent with the direction in the DIS, as these are less frequent.

It is important to note that the hazard assessment shown above is specific to the configuration and location of the Volt battery system. A battery system located completely inside the vehicle passenger compartment for example, may have a different assessment. This assessment also presumes little or no knowledge of specific details of the battery system design. For example, toxic and flammable gases are listed as these are theoretically possible to exist. However, later work may show that a particular cell does not emit sufficient flammable gas to actually generate a hazardous condition, or that a particular number of cells are required to vent in order to generate a hazardous condition. This consideration is taken into account during a later phase of development.

Table 1. Battery System Preliminary Hazard Analysis

Hazard	Severity	Control	Exposure	ASIL
High voltage exposure during normal operation	S3	C3	E4	D
High voltage exposure during/following a vehicle crash	S3	C3	E2	B
High voltage exposure during service	S3	C2	E3	B
Exposure to flammable gas	S3	C3	E4	D
Exposure to toxic gas	S3	C3	E4	D
Exposure to flammable liquid	S3	C1	E4	B
Exposure to toxic liquid	S3	C1	E4	B
Exposure to high temperature components (skin burn)	S1	C2	E4	A
Exposure to fire or ignition source	S3	C3	E4	D

In order to develop the appropriate system and component requirements, potential causes of these hazards must be determined. This creates a better understanding of the system and forms the basis for developing requirements. For example, exposure to flammable gas could be caused by over charging the pack, an internal cell failure or an external short. Each of these can lead to cell venting which may generate flammable gas.

The other primary task during the concept phase creates the safety concept document which describes both the physical and controls features intended to mitigate or prevent the various potential causes for each of the identified hazards. Key features of the safety concept include a system description, a definition of safe states for the system, and the hazard mitigation strategy which incorporates a degradation strategy to allow the system to transition to a safe state depending upon the type of fault. Considering the overcharge example listed above, pack voltage is monitored to make sure that it doesn't exceed acceptable values. If an over voltage condition is detected to be imminent, the battery system transitions to a safe state, either a reduced power condition or shutdown. The ASIL ranking for the associated safety goal to mitigate the underlying hazard (in this case, ASIL D) places integrity requirements on the sensors, processors, actuators and software involved in this system. A diagram of the safety concept for over charge is shown in [Figure 2](#). This shows the