Journal of Power Sources 300 (2015) 460–471

Contents lists available at ScienceDirect

Journal of Power Sources

journal homepage: www.elsevier.com/locate/jpowsour

Analyzing system safety in lithium-ion grid energy storage

David Rosewater [a, *], Adam Williams [b]

[a] Sandia National Laboratories, 1515 Eubank, Albuquerque, NM, USA
[b] Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA, USA

HIGHLIGHTS

- Reviews li-ion: voltage, arc-flash, fire, and vent gas combustion and toxicity.
- Reviews Probabilistic Risk Assessment (PRA) for safety engineering li-ion systems.
- Presents Systems-Theoretic Process Analysis (STPA) as alternative to PRA.
- Presents research applying STPA to a li-ion grid energy storage system.
- Concludes STPA may be more cost effective than PRA for li-ion systems.

ARTICLE INFO

Article history:
Received 1 July 2015
Accepted 16 September 2015
Available online 8 October 2015

Keywords:
Energy storage
Battery
Safety
Lithium-ion
STAMP
STPA

ABSTRACT

As grid energy storage systems become more complex, it grows more difficult to design them for safe operation. This paper first reviews the properties of lithium-ion batteries that can produce hazards in grid scale systems. Then the conventional safety engineering technique Probabilistic Risk Assessment (PRA) is reviewed to identify its limitations in complex systems. To address this gap, new research is presented on the application of Systems-Theoretic Process Analysis (STPA) to a lithium-ion battery based grid energy storage system. STPA is anticipated to fill the gaps recognized in PRA for designing complex systems and hence be more effective or less costly to use during safety engineering. It was observed that STPA is able to capture causal scenarios for accidents not identified using PRA. Additionally, STPA enabled a more rational assessment of uncertainty (all that is not known) thereby promoting a healthy skepticism of design assumptions. We conclude that STPA may indeed be more cost effective than PRA for safety engineering in lithium-ion battery systems. However, further research is needed to determine if this approach actually reduces safety engineering costs in development, or improves industry safety standards.

1. Introduction

Controlling the potential hazards that lithium-ion batteries can pose has been a challenge since their market introduction by Sony in 1991 [1]. Lithium-ion batteries, while inert and non-hazards in most contexts, have the following properties that can develop hazardous conditions: voltage [2], arc-flash/blast potential [2], fire potential [1,3], vented gas combustibility potential [4], and vented gas toxicity [3]. While this is not a comprehensive list, for example weight could also produce a hazard, these are properties that are somewhat unique to lithium-ion batteries and become more challenging to manage in large stationary energy storage systems. This list will be used to perform the safety analysis in Section 3. Each property is capable of producing a hazard if and only if specific contextual requirements are met. Section 1.1 will introduce the circumstances necessary for lithium-ion batteries to produce a hazard and briefly discuss commonly applied controls for each property. It then discusses the potential for hazard combinations and why safety engineering in systems with lithium-ion batteries has been historically difficult. Section 1.2 then reviews the most prevalent of the conventional techniques used in safety engineering and discusses its limitations in complex systems.

The aim of this paper is to propose an alternate perspective for designers to engineer safe lithium-ion battery systems. This perspective is developed and explored through the robust, non-quantitative hazard analysis method Systems-Theoretic Process

* Corresponding author.
E-mail addresses: dmrose@sandia.gov (D. Rosewater), adwill@mit.edu (A. Williams).

http://dx.doi.org/10.1016/j.jpowsour.2015.09.068

Nomenclature

Accident	an undesired or unplanned event that results in a loss
CESS	Community Energy Storage System
Hazard	a system state, or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident
Loss	any unacceptable outcome (loss of life or injury, damage to property, loss of mission, loss of data, loss of investment, damage to reputation, etc.)
PRA	Probabilistic Risk Assessment
Risk	the effect of uncertainty on outcomes
Safety	freedom from accidents (loss events)
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
System	a set of components, including mechanical; electrical; computer; human; organizational; and societal elements, along with the connections between components that together form a complex whole

Analysis (STPA) and its application to a lithium-ion battery system. We argue that framing hazard analyses to emphasize uncertainty, in the ways that component interactions violate safety constraints, can help to overcome costly systematic biases which are enforced by the conventional perspective. Systematically identifying and eliminating the ways that can hazards develop allows for safety to be ensured more efficiently than trying to prove safety through the collection and analysis of historical data. A brief discussion is also included on how this perspective could impact the way safety is represented, and therefor publicly perceived, promoting a better understanding of uncertainty and a more rational approach to risk management.

1.1. Hazardous properties in lithium-ion battery systems

1.1.1. Voltage

The number of battery cells per string in grid energy storage can be higher than in mobile applications, resulting in higher DC voltage and a need for additional precautions. In the voltage range 100–1000 V DC, the National Fire Protection Agency's (NFPA) standard 70E on electrical safety in the workplace establishes a limited approach boundary for unqualified workers at 1.0 m [2]. This boundary is to prevent those who are unable to avoid hazards from coming within arms reach of the exposed electrical conductors. An additional boundary is established for those personnel who are aware of the hazard to restrict what tasks they can perform. NFPA 70E sets the restricted approach boundary for qualified workers to the distance "avoid contact" for exposed conductors between 100 and 300 V DC, and a more precise 0.3 m for exposed conductors between 300 and 1000 V [2]. This boundary is to prevent even qualified workers from working on or around live circuits with dangerous voltage. If the circuit can be deenergized, a Lock-Out-Tag-Out (LOTO) procedure is required to remove the dangerous voltage, apply a lock to prevent its return, and verify its absence before work. For LOTO to be possible in a battery system, the design must include isolation points that allow a worker to divide the string into segments each less than 100 V DC without being exposed to dangerous voltage. An exception to the requirement for LOTO exists for systems that are impossible to deenergize but this requires that qualified workers must have high level work authorization in addition to adequate shock Personnel Protective Equipment (PPE), and insulated tools.

1.1.2. Arc-flash/blast

High string voltage affects both the potential for shock and the potential for arc-flash/blast. Equations (1) and (2) show the maximum power point method for calculating the incident energy in DC arc-flash [2]. Indecent energies calculated by this equation are described as "conservatively high" [2] and other methods are being explored for calculating and classifying the potential harmful energy in a DC arc-flash [5]. Arc-blast results from explosive components of an electric arc (e.g., vaporized copper) and depends greatly on the equipment and environment involved in the arc. Common controls to prevent arc flash include increasing separation between positive and negative conductors, regular maintenance to prevent equipment failure, and arc-rated PPE for electrical workers.

$$I_{arc} = 0.5 I_{bf} \tag{1}$$

$$IE = 0.01 V_{sys} I_{arc} T_{arc} \Big/ \left(D^2\right) \tag{2}$$

Where:

I_{arc} = Arcing current (amps)
I_{bf} = System bolted fault current (amps)
IE = incident energy at a given working distance (cal cm^{-2})
V_{sys} = System voltage (volts)
T_{arc} = Arcing Time (sec)
D = working distance (cm)

1.1.3. Fire

Thermal runaway is chemical process where self-heating in a battery exceeds the rate of cooling causing high internal temperatures, melting, off-gassing/venting, and in some cases, fire or explosion. Causes of thermal-runaway include mechanical, electrical, and thermal abuse; internal short circuit from manufacturing defects; and the development of metallic dendrites that form an internal short over time [1,6,7]. "Reactivity[1] level" is measured on a scale between 0 and 7, shown in Table 1. The reactivity[1] level in thermal runaway can vary greatly depending on chemistry, concentrations, additives, cell design, cell conditions (such as its state of charge (SOC) or state of health (SOH)) and environmental conditions [1,6,8]. At very high reactivity[1] levels (5–7) the cells can produce heat rapidly enough to catch fire, rupture or explode.

Controls for lithium-ion battery fires can be divided into three classes: abuse testing, battery management design, and emergency systems. Abuse testing exposes a representative sample of cells to the worst case environmental conditions they would expect to see during both use and foreseeable misuse; thereby establishing the limits of safe operation [8]. Many abuse testing standards exist [9–17], each with different intended environments and use conditions. Designers then impose these limits in products, often through the application of a Battery Management System (BMS). There exist many challenges in BMS design to detect and respond to the violation of environmental or use limits [18]. When fires do occur, emergency systems use warnings, alarms, fire suppression, or other response mechanisms to mitigate the scope of damage from the fire. Fire detection and suppression systems are used in

[1] The term "Reactivity" is used in place of "Hazard" as source uses a conflicting definition of hazard.