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 xxx

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
0378-7753/© 2015 Published by Elsevier B.V.

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.

Table 1
Reactivity[1] levels and descriptions (adapted from Ref. [8]).

Reactivity[1] level	Description	Classification criteria
0	No effect	No effect. No loss of functionality.
1	Passive protection activated	No defect; no leakage; no venting, fire, or flame; no rupture; no explosion; no exothermic reaction or thermal runaway. Cell reversibly damaged. Repair of protection device needed.
2	Defect/Damage	No leakage; no venting, fire, or flame; no rupture; no explosion; no exothermic reaction or thermal runaway. Cell irreversibly damaged. Repair needed.
3	Leakage mass less than 50%	No venting, fire, or flame; no rupture; no explosion. Weight loss less than 50% of electrolyte weight (electrolyte = solvent + salt).
4	Venting mass greater than 50%	No fire or flame; no rupture; no explosion. Weight loss greater than 50% of electrolyte weight (electrolyte = solvent + salt).
5	Fire or flame	No rupture; no explosion (i.e., no flying parts).
6	Rupture	No explosion, but flying parts of the active mass.
7	Explosion	Explosion (i.e., disintegration of the cell).

many stationary systems [19] though, current life safety provisions for their design and installation do not hold provisions specific to lithium-ion batteries [20–26]. Increasing separation of cells within a pack, use of different electrical configurations, active external cooling, and containment within certain plastics have also been shown to mitigate the need for emergency systems by preventing thermal runaway from propagating [27–29].

1.1.4. *Vented gas combustibility*

Gasses can vent from a cell in thermal runaway at lower reactivity[1] levels (3–7). These gases include carbon dioxide, carbon monoxide, hydrogen, and methane and if they are allowed to reach a critical concentration in an enclosed space, a spark can cause an explosion [30]. Marr, Somandepalli, and Horn investigated this phenomena with a cell test chamber, gas analysis and, combustion test chamber apparatus [30]. Marr and colleagues analyzed the makeup and explosiveness of gasses emitted during the thermal runaway of 7.7 Wh lithium-ion cells with graphite anode and a $LiCoO_2$ cathode [30]. Tests performed at 100% SOC produced an estimated 2.5 L of gas with a Lower Explosive Limit (LEL) of 6.3% and explosion severity index K_g = 65 m-bar/s (comparable to methane at 46 m-bar/s, or propane at 76 m-bar/s) [30]. To provide a better understanding of how these conditions may occur, Equation (3) shows an expression for estimating the minimum kWh of lithium-ion batteries required to reach the LEL in a room with no ventilation. Using this equation and the values derived by Marr and colleagues, E_{LEL} can be estimated for a 50 m^3 room. $V_{room} = 50{,}000$ L, $LEL = 6.3\%$, $E_{cell} = 7.7$ Wh, and $V_{runaway} = 2.5$ L, results in $E_{LEL} = 9.7$ kWh. This result is sensitive to the assumptions of room size, gas composition and LEL, cell chemistry, design, SOC and the average volume of vented gas produced during thermal runaway. This potential hazard can be controlled through preventing thermal runaway, ventilation of the space sufficient to prevent gas concentrations from reaching the minimum combustion threshold, deflagration venting [31], and explosion suppression [32].

$$E_{LEL} = \frac{V_{room} * LEL * E_{(cell)}}{V_{runaway}} \tag{3}$$

Where:

E_{LEL} = Minimum energy of lithium-ion batteries required to reach LEL (Wh)
V_{room} = Volume of the room (liters)
LEL = Low explosive limit of vent gas (concentration by volume %)
E_{cell} = Energy of tested cell (Wh)
$V_{runaway}$ = Volume of gas produced by one cell at 100% SOC in thermal runaway (liters)

1.1.5. *Vented gas toxicity*

Gases vented during thermal runaway can be toxic in high concentrations. Ribiere et al. evaluated toxicity levels based on combustion tests of lithium manganese oxide cells [3]. Table 2 shows the estimated battery energy (Wh) needed to reach concentrations in a 50 m^3 room that could, after 60 min, lead to exposure exceeding the Irreversible Effects Threshold (IET) and the First Lethal Effects Threshold (FLET) [3]. The gases listed are hydrogen fluoride (HF), carbon monoxide (CO), nitrogen oxide (NO), sulfur dioxide (SO_2), and hydrogen chloride (HCl). In addition to preventing thermal runaway through abuse testing and the applications of a BMS, this hazard can be controlled through sufficient ventilation, access control, and use of a positive pressure breathing apparatus.

1.1.6. *Combinations of hazards*

These five properties, in addition to the hazards they can lead to individually, have the potential to interact and make individually designed controls less effective or even counterproductive. Experiments performed by the Federal Aviation Administration (FAA) demonstrate one example where the suppression of a thermal runaway fire in a shipment of lithium-ion batteries allowed vent gasses to buildup and explode in the test compartment [28]. Perhaps a higher profile example of emergent hazards is that of the fire that occurred in a Boeing 787 Auxiliary Power Unit (APU) in 2013. According to the NTSB report, experimentation had been performed at standard temperatures and pressures to demonstrate that a thermal runaway event in a single cell would not propagate to adjacent cells in the APU [33]. After the accident, this experiment was repeated at a temperature near the high end of the operational range which demonstrated the potential for propagation [33]. Neither mechanical abuse alone nor elevated temperature alone produced the hazardous propagation of fire observed when both these conditions were applied to the APU. A combination of factors spanning design, manufacturing, testing, shipment, installation,

Table 2
Estimated battery energy to reach the IET and FLET values for the NO, CO, HCl, SO_2 and HF toxic gases (exposure time of 60 min, fire occurring in a 50 m^3 room) (adapted from Ref. [3]).

(Wh)	HF	CO	NO	SO_2	HCl
IET	60	290	280	530	1320
FLET	110	1140	2080	4710	7880

oversight, regulation, operation, and environment can lead to real world accidents in all types of energy storage systems [34–37,33]. Because of the complex nature of the controls needed in each of these areas, safety in lithium-ion battery systems is a complex problem. The next section will review the conventional perspectives and techniques applied to analyze hazards in complex systems.

1.2. Conventional safety engineering practices

Risk can be described as the effect of uncertainty on objectives [38] and current practices in safety engineering are built from a foundation of managing such uncertainties. Risk management seeks to 1. Ensure that adequate measures are taken to protect people, the environment, and assets, and 2. Balance different concerns (e.g., safety and cost) through analytic methods [39]. One foundational principle of current risk analysis is a focus on observable quantities (e.g., failure occurrence rate) that describe the states of the system in question [40]. Such observable quantities can be predicted through design and historical data analysis, with the related mathematical uncertainties expressed as probabilities [40]. One specific risk management and analysis tool Probabilistic Risk Assessment (PRA) (also called Quantitative Risk Assessment – QRA) is commonly used in safety engineering across domains (e.g., aviation [41] and nuclear [42]), as well as in electrical and energy storage specific applications [43,44]. PRA attempts to capture and mathematically express the current state of knowledge about a system including uncertainties [39]. It identifies hazards, their deterministic causes and consequences, and provides a way of describing uncertainty [39]. PRA enables the calculation of expected risk values (defined as probability of an event multiplied by the severity of its consequences) so that alternatives can be compared on a similar numerical basis [39]. Where there is insufficient data to directly predict behavior, and therefore risk, PRA relies on Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) to deconstruct a system into components which can be more readily quantified. Total risk is then calculated through a mathematical function of the system's architecture and risk identified at the component level [39]. PRA logic suggests that for safety engineering, risk reduction is equated with improved safety.

Despite a history of successful (and useful) application in across safety domains, PRA encounters several problems when applied to safety of complex systems. These problems stem from the structural assumptions and underlying biases inherent in PRA logic. Performing PRA assumes that there is sufficient input/output data and knowledge of the underlying mechanisms to make accurate predictions of system behavior. But there exist many factors effecting safety that are difficult or impossible to measure, quantify and therefore observe. These factors challenge the assumptions of PRA and call into question the accuracy of the safety predictions it makes. Minute manufacturing variations, untracked environmental conditions (including during shipping and installation), imperceptible chemical side-reactions, digital errors whose records and effects are erased, biological sensory perception, human understanding, and organizational safety culture are all factors known to affect safety in ways that are difficult or impossible to directly observe and predict. Software performance in automated systems can also be difficult to observe in a safety context due to the complexity of system requirements and interactions across organizations involved in its development.

Even when quantities are technically observable, predictions can be inaccurate if input/output data are sparse, if data cannot be collected under realistic conditions, or if the model of the system is flawed. The conditions where this can occur are varied. While describing its application to reliability engineering, Zio documented that PRAs generally have four assumptions, adapted for a safety context, which lead to underestimation of risk in complex systems: a system has fixed interface boundaries, observations of past system behavior are sufficient to allow accurate prediction of future behavior, actuarial data are available and accurate for all system components and system behavior can be understood based on element behavior and cause-and-effect links [45]. Each of these assumptions is rendered invalid in complex systems which tend to display a highly dynamic structure, nondeterministic and interdependent links and insufficient data to bound uncertainty. Researchers hold significant criticism for PRA performed under these conditions. For example, in reference to the precautionary principal, Sterling describes the use of reductive risk management methods (including PRA) in cases with poor knowledge about probabilities and outcomes as irrational, unscientific and potentially misleading [46].

When system risk is calculated based on system architecture and component risk values, risk management assumes system interactions can be combined in deterministic or predictable ways. But today's complex systems increasingly include social and organizational influences that can invalidate this assumption. For this reason, Leveson cites the fast pace of technological change, new types of hazards, increasing complexity and coupling, decreasing tolerance for single accidents, more complex relationships between humans and automation, and changing regulatory and public views on safety as factors in society that are ubiquitously stretching the limits of safety engineering [47]. These factors that continue to create cases with poor knowledge about probabilities and outcomes are especially prevalent in energy storage technologies. Similarly, Taleb frames these factors as the misuse of statistics in cases where the underlying type of probability distribution is unpredictable. He argues that out-of-sample risk estimation in systems governed by low-probability events with extreme outcomes the Black Swan domain are especially vulnerable to the fragility of our knowledge about these systems [48]. Knowledge of the system is generated by analyzing the sparse available data to produce probability distributions (e.g., Gaussian) for events. Because of the low rates of occurrence of these events, risk calculations possess high error relative to their absolute probabilities. As the severity of outcomes in these systems is inversely proportional to their probabilities, even small errors in the estimation of probability are magnified dramatically in the calculation of risk. In such systems, Taleb advocates a philosophy that includes a healthy skepticism of our knowledge [48]. However PRA, as it is described above, relies on the strength of our knowledge to predict underlying risk. If grid scale energy storage is an industry where extremely rare accidents can have wide economic impacts, designers should be keenly aware of the inability of PRA to accurately calculate this kind of risk.

To explore whether lithium-ion energy storage systems possess sufficiently observable risk and/or predictably compounded risk amenable to PRA, two examples from Section 1.1 are revisited in the context of PRA. These examples come from the aviation industry on account of the rich data available in this field; however similar cases exist for the use of PRA in grid energy storage. First, FAA experimentation on fire suppression showed how a fire in a shipment of lithium-ion batteries could be suppressed using oxygen starvation but that doing so could produce the conditions for a combustible gas explosion [28]. The calculated PRA probability of this accident scenario is the number of lithium-ion batteries that catch fire during shipment divided by the number total number of batteries shipped. In a 2013 FAA study, expected probability of an accident was estimated by using Equation (4). The mean result of this equation predicts approximately OR = 4.1 battery fire accidents in the 10 year period from 2012 to 2021 prior to mitigation interventions [49]. Severity of an accident was calculated by taking the numerical sum of the estimated costs associated with crew injuries, airplane damage, cargo damage, collateral damage [49].

$$OR = BAR*B_{ton-miles} \tag{4}$$

Where:

OR = Occurrence Rate (Accidents per 10 year period 2012–2021)
BAR = Battery Accident Rate ($1.99 * 10^{-9}$: historical battery accidents per ton shipped, per mile)
$B_{ton-miles}$ = Battery Ton-Miles (2,063,769,370: Estimated tons of batteries to be shipped × estimated miles through the air in 10 year period 2012–2021)

While such calculations do produce an estimate of risk, this mathematical reduction could be misleading given the magnitude of the uncertainty in both probability and severity observations. As the designs of lithium-ion batteries continue to evolve, manufacturing processes change, and shipping regulations are applied; the underlying risk will change and historical observations may no longer predict future occurrence rates. Also, the costs directly associated with an accident do not begin to capture the reputation and confidence damage to the airline, the battery manufacture, and the shipping and battery industries. The uncertainty inherent in these quantities is clouded by the apparent clarity of calculated risk.

Second, the NTSB reported on the fire in the Boeing 787 APU battery in 2013. According to the report, designers calculated that the likelihood of occurrence of a cell venting was 1 in 10 million flight hours. This estimate was based partly on the available data from the battery supplier that 14,000 similar cells had been used in industrial applications for significant time without incident [33]. At the time of the 2013 fire, the actual occurrence of venting in the APU design was 2 in 52,000 flight hours [33]. As previously discussed, the causes for thermal runaway fire can be a complex combination of factors spanning materials, manufacturing, shipping, installation, and use environment. The effect of each of these factors is difficult to account for in new applications as they can combine in non-linear and unanticipated ways. Not only is the calculation of risk made more difficult by the intricacies of thermal runaway in lithium-ion batteries, organizational complexities can make the mechanisms that compound risk in system design more difficult to predict. Indeed, the NTSB cited manufacturing defects as the root-cause of the fire, but also identified the effects of integration, thermal management, testing, design reviews, and regulatory oversight [33]. Boeing's observation and subsequent calculation of risk may have been fully accurate based on the available information at the time but this metric may not have adequately represented the underlying effects of uncertainty on the real-world system.

In these examples contextual factors make some observations of risk quantities inaccurate and the ways that it compounds in systems difficult to predict. While PRA may be robust enough to distinguish between these different types and qualities of risk, as humans we are subject to the "anchoring" and "what you see is all there is" heuristics of risk estimation described by the psychologist and Nobel laureate Daniel Kahneman [50]. These cognitive biases make invalidating/ignoring available but inaccurate data and seemingly-deterministic mechanisms especially difficult. This happens because it is cognitively easier to trust available information than ignore it or look for where the information is incomplete. The conformation bias also effects how risk data are interpenetrated in that it is cognitively easier to accept new data that confirms, rather than conflicts with, what we already believe [50]. As PRA is structured around available data and deterministic mechanisms, it can be inferred that its use enforces the biases that may, in complex systems, lead to mischaracterization of uncertainty.

Instead of focusing on the potential for mischaracterization, PRA can perhaps be better assessed on the basis of its claim of cost-effective usefulness, that it improves safety even without accuracy, for which there is some support [51]. It could be argued however that the cost-effective usefulness of risk management generally could benefit from a lack of probability and severity calculations where any such figures would be more misleading than helpful. Indeed Aven and Zio write that "the motivation for the qualitative analysis is the acknowledgment and belief that the full scope of the risks and uncertainties cannot be transformed to a mathematical formula" and in such systems "Numbers can be generated but would not alone serve the purpose of the risk assessment" [52]. This suggests that for lithium-ion energy storage systems, where risk quantities are difficult to observe/compound, a robust and non-quantitative method for safety engineering could be more useful or less costly than PRA. Such a method could encourage a healthy skepticism of our knowledge, help us to overcome our cognitive biases, and enable us to make design decisions informed by all that we do not know. This paper presents the application of a non-quantitative safety engineering method to a lithium-ion battery system in order to assess the plausibility of this claim.

2. A systems perspective on safety

System-Theoretic Accident Model and Process (STAMP) provides a new model of causality for analyzing (and designing against) accidents, especially those involving complex, socio-technical systems [47]. This model has been applied successfully to complex problems in many high consequence industries including aviation [53,54], space [55,56,54], automotive [57,58], medical [59,60], security [61,62], and nuclear power [61,63]. STAMP argues that in today's complex world safety is best understood in terms of interrelated components needing to maintain dynamic equilibrium. In order to prevent accidents, the system must enforce safety constraints by adapting to changes in itself or its environment [47].

As such, safety can be described and analyzed as an emergent system property that results from adequate system-wide enforcement of design constraints through control actions. In this causality model, losses are considered the result of flawed interactions between physical components, engineering activities, operational mission, organizational structures and social factors [64]. Further, losses occur when the system enters a hazardous state (e.g., buildup of explosive vent gases) and experiences an additional challenge external to the hardware system, such as an environmental or human event scenario (e.g., technician opens the door and causes a spark) [47]. Rather than focus on estimating risk of such external scenarios or events (like PRA-based analyses), STAMP emphasizes identifying and manipulating the elements of a system's design that can be controlled. This model shifts the analytical paradigm from preventing failures to enforcing safety control actions [47].

This paradigm shift has its origins in systems and control theory. Systems theory introduces two concepts useful for battery system safety: hierarchy and emergence. Hierarchy refers to understanding the fundamental differences and relationships between levels of complexity within a system, including identifying what generates, separates and links each level. Emergence refers to the phenomenon by which behaviors at a given level of complexity are irreducible to the behavior or design of its component parts. Such emergent properties act as constraints on the actions of components at the lower levels [47]. Hierarchy and emergence help explain the observation that a system can have a "safe" (or reliable) component, but that the same component can exhibit unsafe behavior in the context of a different design or environment (e.g., batteries that are safe for use in industrial applications but not in aviation or aerospace). Taken together, hierarchy and emergence suggests that safety emerges at each level of complexity, depending on the enforcement of constraints on components at lower levels to determine the movement of the system away from or toward hazardous system states.

Likewise, control theory is founded on two principles useful to battery system safety: control (actions and loops) and communications (between components and levels of a hierarchy). If the emergent properties within a hierarchy act as constraints on component interactions, then a set of control actions can be designed to enforce these constraints. Control theory introduces the concept of a control loop to describe this process. A typical loop (an example of which is presented later in Section 3.2, shown in Fig. 2) follows an action command from a controller (the initiator) to the actuators (the controlled variables) to the controlled processes (the components or systems that need to change) to the sensors (the measured variables) and back. Movement of information around this loop also highlights the importance of communication within systems. Regardless of whether the system is open or closed, control presupposes a need for components within and across levels to communicate the pertinent information in a timely manner [47]. This suggests that if safety is an emergent systems property, then safety constraints can be enforced through a network of safety control actions that need be provided (communicated) effectively.

Considering safety through the lenses of hierarchy, emergence, control and communication suggests a redefinition of battery system safety that replaces a focus on probabilistic risk and redundancy with a larger perspective aimed at identifying and imposing safety constraints to avoid hazardous system states. Safety for energy storage, then, is an emergent property recast as a control problem regarding appropriate responses to: component failures (e.g., malfunctioning batteries, inoperable battery management systems or installation errors), external disturbances (e.g., natural disasters, reduction of maintenance resources or changing modes of operation), or dysfunctional interactions among system components (e.g., confusion over maintenance responsibility, pore coordination between components that charge or discharge a battery or competing objectives between the manufacturer and electric utility) [64].

STAMP is not alone in promoting a systems perspective on safety [65]. Per the description of STAMP above, 'safety' can be further described as the ability of an energy storage system to maintain a state that eliminates losses related to disruption of its services. Rather than relying on defense-in-depth reliability intended to minimize the chance of a series of random, independent component failures leading to a loss, this framework analyzes energy storage safety as the avoidance of hazardous states in terms of three fundamental concepts: (1) safety control actions, (2) control structures and (3) process models.

2.1. Safety control actions

Control actions act as constraints or set points by which higher levels within a hierarchy exercise control of activities at lower levels based on the current understanding of the system being controlled [47,64]. For example, a control computer provides setpoints to a energy storage system's inverter based on data received from battery telemetry. The presence (or lack) of safety at one level imposes constraints on the behaviors of the components at a lower level to ensure that unsafe system states are avoided.

2.2. Control structures

Hierarchical organizational structures help visualize the entire socio-technical system and understand safety constraints to avoid unsafe states. A control structure, such as the one showed in Fig. 1, illustrates how constraints and commands are communicated from the top down via reference channels, as well as operational experience from the bottom up via feedback channels [47]. The accurate and timely communication of safety control actions through this control structure enables a socio-technical system (such as a battery energy storage system) to avoid hazardous states.

2.3. Process models

In order to ensure that appropriate controls are being applied to manage the constraints at lower levels of the system, the controller (human or automation) uses a model of the process being controlled ("mental map" or digital abstraction) to make decisions. Process models must contain information regarding relationships between variables, the current system state, and the mechanisms to employ changes in the system state. This model is used by the controller to determine which safety control actions need to be issued and when each should be applied. For example, a system controller must have a model for restricting a battery's charge and discharge current based on voltage, temperature, state of charge, etc. Accurate process models are needed at all levels of the control structure to enforce adherence to safety requirements [47].

In summary, STAMP combines hierarchy, emergence, constraints and communications to reframe the concept of safety for complex energy storage systems as an emergent system property. In other words, losses result from interactions between system components (e.g., the batteries and the BMS) that violate safety design constraints (e.g., batteries exceed temperature limits and BMS does not detect it or respond). Understanding how control actions are issued though a control structure in response to process models can help mitigate these component interactions and enhance the safety of energy storage systems. This perspective, along with a rigorous non-quantitative method for hazard analysis, is anticipated to make risk management in design more effective and/or less costly.

3. Safety analyses of a battery system using STAMP

The following analysis serves as an illustrative example of how a systems perspective on safety can be applied. The vender's name and the identifying details of the system have been removed to retain ability for this example to widely apply across many venders and systems. A small, grid connected, lithium-ion battery system (between 3 and 30 kWh) was selected to illustrate how both system details and environmental/use characteristics are important for a safety analysis. Referred to here as a Community Energy Storage System (CESS), devices similar to this one are being considered for wide deployment in residential applications. Such systems can provide improved service reliability to home owners and may enable a higher penetration of distributed renewable generation assets [66].

Based on a systems perspective of safety, Systems Theoretic Process Analysis (STPA) is a tool to systematically analyze the safety constraints of a design. It consists of two broad steps: Step 1. Identify potentially hazardous control actions, and Step 2. Determine how unsafe control actions could occur [47]. STPA refines a designer's view of safety control by analyzing a series of integrated control loops within a system's safety control structure. In the next

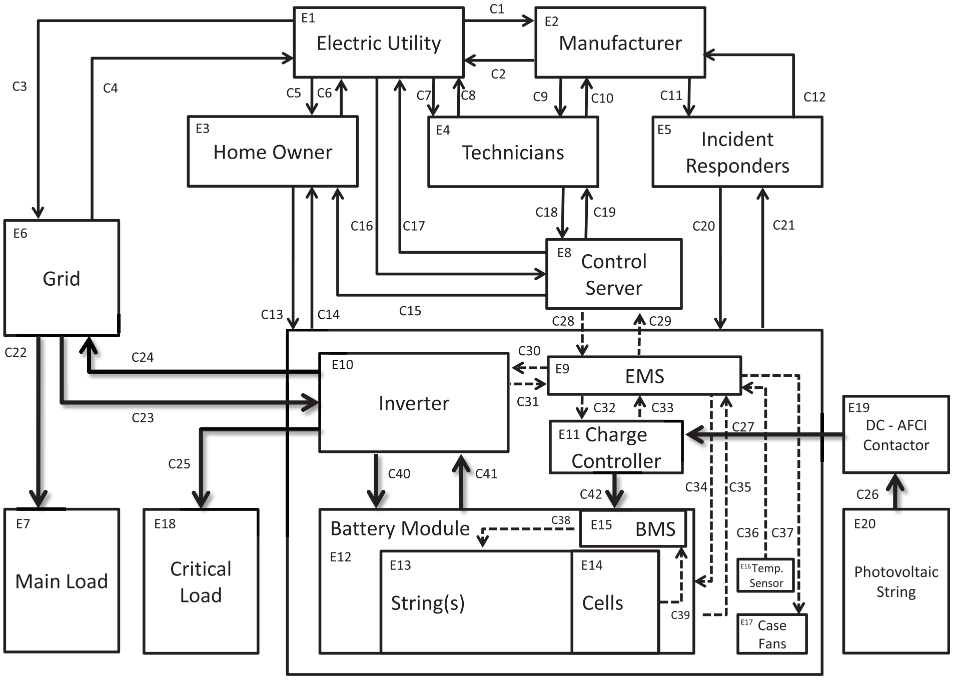

Fig. 1. CESS control structure diagram.

sections, a CESS will be prepared for STPA by establishing the system accidents, hazards, and control structure. Then one control loop within this structure will be analyzed in detail to exemplify the application of STPA Steps 1 and 2. The discussion section will then provide an assessment of the positive and negative attributes of the analysis approach.

3.1. System characterization

Before STPA can be performed the system level losses to prevent must be clearly defined. Working with the vender, three unacceptable losses were identified: injury or death, damage to property, and cost overruns and damage to reputation with costumers. Table 3 shows these accidents along with descriptions detailed enough to establish pass/fail criteria. While these criteria are helpful for the system in question, pass/fail criteria are not necessary for STPA. Unacceptable losses can often be unique to a specific organization or project so it is important to capture them each time the analysis is performed.

With the accidents to prevent clearly defined, the system's hazardous states can be derived. These hazards are developed by tracing the losses in Table 3 to the five properties of lithium ion batteries that can develop a hazard as discussed in the introduction: voltage, arc-flash/blast potential, fire potential, vented gas combustibility potential, and vented gas toxicity. This process promotes a complete list of hazardous states but does not, by itself, ensure comprehensiveness. It is vital to be skeptical of seemingly firm knowledge of how each of these losses could come about and all assumptions that limit the scope should be documented. For example: “While injury may result from through the mechanical properties of a CESS (e.g., sharp corners, tipping and failing over) it is assumed that the CESS does not posses anything that would set it apart from similar electrical equipment (washing machine, HVAC, etc.) in this regard. Differences include a lockable door, heavier in weight, and labeled as a battery. This assumption may not hold in cases where the physical differences are significant in the associated manufacturing/installation standards and inspection process (e.g., developing countries, or areas where prevalent seismic activity is poorly represented in local codes).” This documentation tracking what is not known or poorly understood is vital to the completeness of an hazard analysis.

Table 4 lists the systems states that, under certain external conditions, could lead to a loss. This is to say that a buildup of vented gasses to combustible concentrations (H5) is not a loss in and of itself but given a spark, it could be. Each hazard could lead to one or more losses and a loss can develop out of one or more hazards. For example: if a home owner is exposed to voltage potential (H1) it may lead to injury (L1), which could in turn lead to reputation damage with costumers (L3). Likewise, if conditions are present to lead to thermal runaway (such as a manufacturing defect) (H3) and people are in proximity to the device, the potential exists for human exposure to vented gasses (H5) which may lead to Injury from smoke inhalation (L1). Note that hazards H4, H5, and H6 can develop out of the conditions leading to thermal runaway of installed cell(s) (H3), which include both internal conditions (e.g., shipping damage) or external conditions (e.g., building fire). These

Table 3
STAMP unacceptable losses for CESS safety.

Losses	Description
L1	Injury or death (Shock, electrocution, burn, smoke inhalation, or any other event related to life safety in excess of that expected for similar electrical equipment installed in one- or two-family dwellings)
L2	Damage to property (Fire that spreads, explosion, or any other event or condition that causes damage property outside of the unit itself)
L3	Cost overruns and damage to reputation with costumers (No more than 10% of the initial distribution require service by a technician within the first year)

Table 4
STAMP potential hazardous states of CESS.

Hazard	Description
H1	Human exposure to dangerous voltage potential
H2	Human exposure to dangerous arc-flash/blast potential
H3	Conditions leading to thermal runaway of installed cell(s)
H4	Conditions allowing propagation of thermal runaway or fire
H5	Conditions allowing human exposure to vented gasses
H6	Conditions allowing the buildup of vented gasses to combustible concentrations

hazards will be used to help define safety constraints in later steps.

A hierarchical control structure can be established to describe the system that is expected to avoid these hazardous states. Control structures help to define and communicate functional component interactions and hierarchy. The development of a control structure can be iterative; allowing it to evolve as a design or the understanding of a real system grows. Working with the vender, the control structure in Fig. 1 was developed. The highest level controllers established in this control structure are the electric utility and the CESS manufacture. Higher level controllers would be regulators and perhaps even congress but as the vender will have little influence on these interactions they can be modeled as environmental factors. It is important to recognize that this control structure is an open system with many external influences such as weather, insurance policies, and legislative environments many of which will have unknown effects on the assumed structure. For example: if local regulations were to require regular inspections by the county electrical inspector, that inspector may need to be included in this structure such that their interactions could be analyzed in detail. This promotes the documentation and critical assessment of the assumptions about how components interact.

3.2. Representative control loop

While an analysis of the whole system is needed to ensure safe operation, a condensed analysis of a single control loop is sufficient to capture the effectiveness of the method. Fig. 2 shows the control loop used to enforce limits on battery operation in the CESS. STPA allow a designer to assess the effectiveness of this control loop within the constraints provided by higher levels in the control structure. A controller (e.g., the Energy Management System (EMS)) issues a safety control action based on its current process model to an actuator (e.g., inverter). This actuator then implements a controlled process (e.g., adjust DC current). The completion of this controlled process is registered by a sensor (e.g., Battery Management System (BMS)). This sensor information becomes feedback upon which the controller updates its process model. Proceeding around each control loop in a systematic fashion allows for a holistic STAMP-based analysis of the safety control actions designed to help the system enforce its safety constraints.

3.3. Safety control actions

Each entity in the hierarchical control structure has system safety responsibilities. The interactions of safety responsibilities must enforce safety constraints in order to avoid hazardous systems states. Each constraint is enforced by a safety control action and so the two terms are often used interchangeably. The connections in Fig. 2 represent how control actions are communicated from one element to another. While these control actions can range from a conversation, to digital communication, to a direct mechanical force, each has a set of safety constraints. Table 5 lists each of the control actions for battery cell voltage shown in Fig. 2 along with a high level description of their qualities. Similar tables could be developed for control of cell temperature, current, and SOC. Together, the table and the figure show how information and actions flow through the control loop.

3.4. Potentially hazardous control actions

Now that the information/action flow through the control loop is defined, STPA step 1 can be performed. STPA step 1, identify potentially hazards control actions, is intended to allow the designer to better understand the ways that the control actions can be violated. This begins with listing four logical categories for how control actions can violate safety constraints [47]:

1. Control Needed and Not Provided
2. Control Provided
3. Control Provided Too Early or Too Late (sequence)
4. Control Provided For Too Long or For Not Long Enough (duration)

Table 6 lists each of the control actions from the representative control loop in Fig. 2 along with each logical violation. Collecting all of the potently unsafe control actions is important to ensuring a complete analysis. Note that each of these may or may not, by itself, cause an accident. It can often take a combination of many unsafe control actions to develop a hazardous system state that, under a set of worse case environmental conditions, could lead to an accident.

3.5. Causal scenarios

Once all of the unsafe control actions have been collected the causal factors can be determined by moving through each element, control action, and environmental factor in the system and assessing whether and how it could contribute to the unsafe control action. This produces a long list of contextualized causal factors which may or may not, by themselves, cause the unsafe control action. More impotently, this step attempts frame the search for causes to all that is not known about what can go wrong. By systematically exploring causal links, areas where there is insufficient knowledge can be identified and design choices can be made to avoid or control this uncertainty. Causal factors are presented in the form of vignettes or scenarios that explain both factors themselves as well as the context of the system. Context is vital as wherever contextual requirements are not met the design assumptions may no-longer hold. Below are four causal scenarios, each selected from one of the control actions in the representative control loop in Fig. 2.

[#] Element, Unsafe Control Action:
  - Potential Causes include:

1 Battery Module, Cell voltage not provided:
  - ‘Potential Causes include: For cell voltage to not be provided to the BMS there must be a disconnection somewhere within the measurement circuit. A disconnection

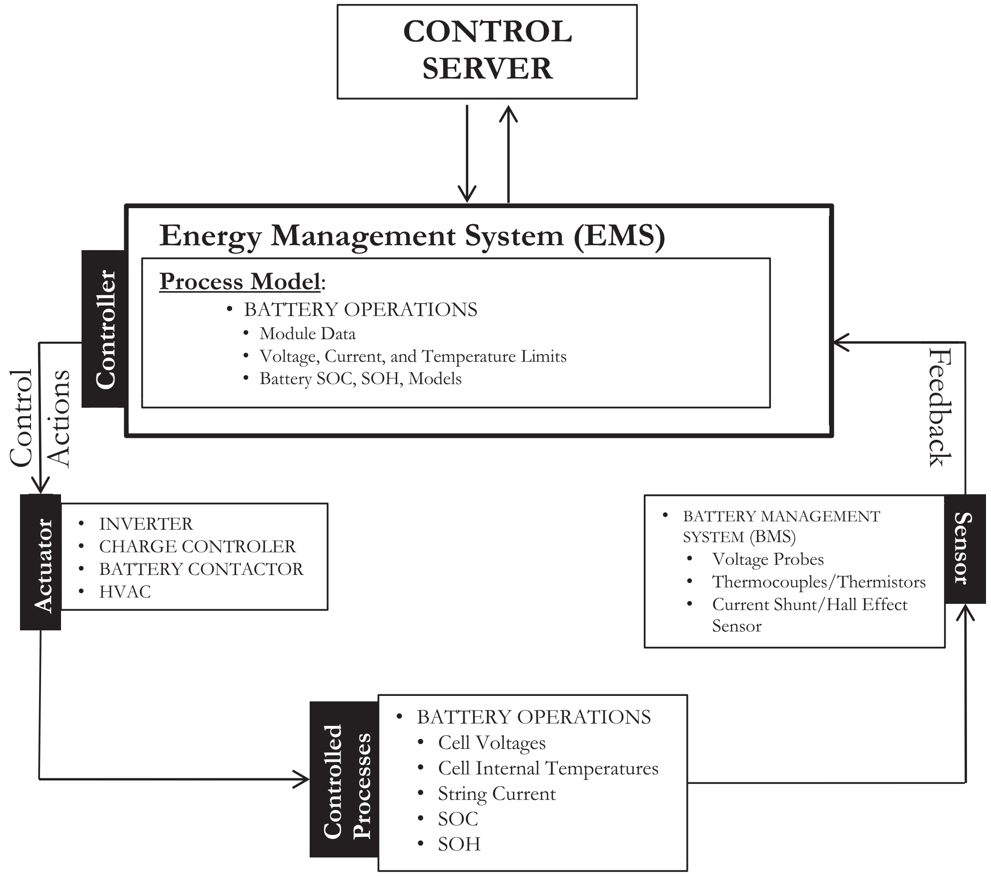

Fig. 2. Representative control loop.

Table 5
Safety responsibilities, constraints, and control actions.

Name	Responsibilities	Constraints	Control actions
EMS	Provide inverter safe power commands	Power commands must not drive battery module, Inverter, or other elements into an unsafe state	Provide inverter power commands within dynamically calculated system limits
Inverter	Actuate power commands to DC battery current safely	Battery current must not push battery into voltage, temperature, SOC or other condition exceeding present limits	Actuate power commands within dynamic limits
Battery module	Allow BMS to access safety related properties	Access to string current and each cell voltage and temperature must be uninterrupted and allow for accurate data to be collected	Provide BMS uninterrupted access to safety related properties for accurate data collection
BMS	Provide data to the EMS on dynamic battery limits	Data on highest cell voltage, lowest cell voltage, highest cell temperature, lowest cell temperature, string current, and the battery module warning/alarm status must be accurate and timely	Provide accurate and timely safety related data to the EMS

can happen in the factory if a terminal is not properly tightened or the BMS is configured incorrectly or in the field from a corrosive environment and lack of corrosion protection, access by rodents, or a voltage surge on the DC bus.'

2. BMS, Highest cell voltage transmission delay:
   - 'Potential Causes include: For there to be a delay in the BMS sending its highest measured voltage to the EMS there must be either a delay in collecting the data, processing the data and producing the highest cell voltage, or in transmitting the data to the EMS. Delays in collecting the data can occur when there is a digital isolation amplification filter that has a low bandwidth. Delays in processing can occur when the algorithm to choose the highest cell voltage is too large or run too often for the BMS processor or memory to keep up. Last, delays in transmission can occur when a communication channel is overwhelmed and there is overflow in the digital communication buffer.'
3. EMS, AC power command stuck:
   - 'Potential Causes include: For the AC power command to remain unchanged with respect to the battery conditions there must be a case for which the control software ceases operation without setting the power command to zero. Incomplete error handling, incomplete error lists,

Table 6
Example unsafe control actions.

Control action	Control needed and not provided	Control provided	Control provided too early or too late (sequence)	Control provided for too long or for not long enough (duration)
Battery module: Provide BMS uninterrupted access to safety related properties for accurate data collection	(1[a]) Cell voltage not provided	Inaccurate voltage	Voltage measurement delay	Voltage measurement stuck
BMS: Provide accurate and timely safety related data to the EMS	Highest cell voltage not provided	Inaccurate highest cell voltage	(2[a]) Voltage transmission delay	Voltage transmission stuck
EMS: Provide inverter power commands within dynamically calculated system limits	Power command not provided	Power command exceeds cell voltage or current limits	Power command delay	(3[a]) Power command stuck
Inverter: Actuate power commands within dynamic limits	DC current not provided	(4[a]) DC current exceeds cell voltage or current limits	DC current actuator delay	DC current actuator stuck

[a] Reference# to selected causal scenarios in Section 3.5.

developmental software, operating system updates, and incomplete code testing, can create the opportunity for this exemption to occur.'

4. Inverter, DC current exceeds cell voltage or current limits:
   - 'Potential Causes include: For the Inverter to violate the safety constraints on DC current, it must be too high or too low based on the complex set of conditions that the battery experiences. For the cell voltage constraint, this starts at the physical measurement on the cells themselves. Inaccuracy can be produced in physical measurement of cell voltages from: a lack or inaccuracy of calibration, rapid measurement drift, inaccurate bus-bar compensation, high impedance measurement isolation grounding, low measurement isolation input impedance, high measurement wire impedance, or some combination of these factors. Once cell voltage has been collected, the BMS must sort them and provide the highest and lowest cell voltages to the EMS. The incorrect voltage can be transmitted because of an incorrect algorithm that selects the wrong cell voltage to report, derived from incomplete validation and verification of the firmware or from incomplete, unclear, or unenforced, design and manufacturing practices for the BMS. The highest and voltage, along with other parameters, are then used by the EMS to calculate a maximum power command. This calculation can produce a violation in DC current if any of its inputs are highly inaccurate or there are mistakes in the algorithm itself. The inputs include measurements such as: highest cell voltage, temperature, SOC, measured string current, and manufacture cell limits. The algorithm used to perform the maximum DC current calculation could contain improper fault handling resulting from its development process or the application of industry standards. Last, the inverter must take the power command from the EMS and use it to change its set-point for DC current. A violation in DC current can be produced in this function from low measurement accuracy in the inverter DC current PI-control, unaccounted parasitic power draw on the DC bus, excessive pre-charge circuit current, or an AC waveform with or without zero crossings on DC current.'

4. Discussion

A systems perspective on safety has some advantages to the component-centric techniques as traditionally deployed. The kind of causal scenarios developed out of STAMP based techniques are qualitatively similar, but fundamentally different than those for PRA. While PRA based analysis helps find many probabilistic factors contributing to a system fire (e.g., a faulty measurement fuse), understanding accident scenarios where all components operate according to design (e.g., EMS software update changes the battery process model to a different battery type) takes a systematic perspective. STAMP, in contrast to PRA, views non-probabilistic components like technicians and software updates as part of a controlled process. Under this perspective, safety constraints are enforced through control and communication providing a variety of design choices to address identified issues. For example, if changing the EMS's battery process model can create a hazard then a designer can: A. program the software to check with the BMS on battery type before operation, B. make the technician enter in the battery's serial number during the software update which it then checks for type, or C. reconfigure component safety responsibilities such that the BMS is tasked with limiting operations thereby eliminating the hazardous system state. With each of these proposed changes, the flow of information in the system changes with the effect of better enforcing safety constraints on the batteries.

Causal scenario descriptions enable designers to make informed decisions about safety control. Consider the case from causal scenario 1 in Section 3.5 where a voltage surge on the DC bus is identified as a contributing factor to a loss of cell voltage measurement integrity. If given this information by itself, one might foresee a requirement to install surge protection which can be costly and in some cases unfeasible. However, given the context of how this unsafe control action can move the system toward an unsafe state, designers may instead chose to implement controls elsewhere such as installing lighting protection or making sure that the BMS can effectively identify when a voltage surge has damaged its measurement isolation. In this way, system safety constraints are enforced in an efficient manner and with due consideration to other design constraints like performance, cost, and schedule.

While PRA compares safety issues on the bases of relative risk, STPA enables designers to implement holistic control that keeps the system away from safety issues. Prioritization then becomes optimization of the performance and cost under the requirements for enforcement of safety constraints. Consider the case from causal scenario 2 in Section 3.5 here transmission delays in measured voltage can result from low filter bandwidth, long processing time, or overloaded communication buffers. If the battery is limited to a maximum voltage that it must not exceed for more than a set time (e.g., two seconds) then design choices can be made as long as this requirement is met. There exist a host of measurement filters, BMS devices, and programming architectures that can meet and ensure the enforcement of this constraint and engineers have the freedom to optimize design choices for performance and cost within this space.

More impotent to the effectiveness of a hazard analysis is the ability to understand and adapt to uncertainty. Note that each of the known Potential Cause scenarios can be "inverted" to produce a list of what is not known and should be specified in the requirements or otherwise controlled or accounted for in the design. For example, Scenario 4 can be inverted to ask the following example questions about the voltage enforcement control loop: How accurate is the voltage measurement/calibration procedure? How often should calibration be performed? How quickly does the measurement accuracy drift? What are the BMS design, manufacturing, and programming standards? What is the validation and verification procedure to be used on the EMS control software? Are there any measurements missing from the EMS for it to enforce voltage effectively? These questions should both direct design efforts to reduce uncertainty and help design around it where it cannot be reduced. For example, how a home owner may interact with a system is not fully known in the design stage. Still this analysis perspective allows that fact to be incorporated into the development process through staged/supervised beta testing that minimizes accident risk while feedback can be collected from the home owner. STPA enables the control of uncertainty at the heart of any successful safety engineering program.

Note that STPA is most effective when applied early in design process. If it is applied during conceptualization, as was shown viable by Fleming, all design options are available and design changes cost nothing [67]. This has the potential to reduce the cost of safety engineering programs, and may allow for more safe-by-design measures to be used than techniques that can only be performed later in the design process when options are limited and changes are expensive. Understanding the safety responsibilities and control actions can aid in the development of requirements and specifications for each component and for system integration. Early establishment of these requirements in a CESS design is speculated to reduce cost and time to market though further research is needed to determine if this is the case or not.

5. Conclusion

The analysis presented in this paper has demonstrated that a systems perspective on safety can be beneficial to the safety engineering process for lithium ion-battery systems. The five properties of lithium ion-batteries that can develop into hazards, voltage, arc-flash/blast potential, fire potential, vented gas combustibility potential, and vent gas toxicity, can develop hazards and combinations of hazards that are difficult to predict or control using conventional analysis techniques. This difficulty stems from the a reliance on Probabilistic Risk Assessment (PRA) which poorly models the complexity of accidents in modern systems. The proposed alternative, Systems-Theoretic Accident Model and Process (STAMP), views safety as an emergent property of sociotechnical systems and has been shown to better address complexity in many high consequence industries. Based on STAMP, Systems-Theoretic Process Analysis (STPA) provides a step-by-step procedure to analyze hazards which, by treating them as emergent system states, was especially effective when applied to a system with lithium-ion batteries.

To assess its benefits and drawbacks, STPA was applied to the design of a lithium-ion based Community Energy Storage System (CESS). STPA works by breaking down a complex system into the safety constraints that are imposed on component actions and interactions to maintain safety at the system level, and analyzing how those constraints could be violated. For the CESS, three unacceptable losses were identified along with six potentially hazardous system states which, under worst case environmental conditions, could lead to a loss. A safety control structure was also developed to illustrate functional system components and the flow of safety control actions throughout the system. From the identified hazards and control structure, the safety control actions were derived through an analysis of each component's safety responsibilities. Control actions can logically become unsafe if and only if they are: needed and not provided, provided, provided too early or too late, or provided for too long or not long enough. The system's logical unsafe control actions were then analyzed for the causal scenarios involving other system components, control actions, and environmental factors that could contribute to their development.

The causal scenarios developed from STPA provided holistic insight into how accidents might happen in the CESS. For example, the analysis showed how EMS software updates which change battery process model can cause the EMS to provide unsafe control actions and possibly allow thermal runaway to develop in the battery. It is important to recognize that nothing in this scenario has a probabilistic mechanism of failure and so generally would not be accounted for in a PRA based analysis. Understanding the complex causes of accidents promotes design changes that act systematically. In the example above this means that designers can choose the right combination of version control, database management, software testing, oversight, technician training, signage, and informational/hardware redundancy to assure that a new process model will not provide unsafe control. If scenarios are identified early enough in the design process, then even architectural changes can be made to eliminate accident scenarios altogether. These insights provide designers a complete picture of how to avoid accidents such that cost and performance optimization can be performed without compromising safety.

In addition to the benefits of applying these techniques to specific design challenges, a systems perspective on safety could have a positive impact on the energy storage industry at large, where there is a narrow focus on “battery safety.” The analysis in this paper has demonstrated that the batteries themselves are only one small piece of a much larger safety picture in a battery energy storage system. While it is a semantic distinction, using the term battery safety narrows the public's perspective on what design choices affect safety. Shifting usage to battery system safety or equivalent terminology more appropriately distributes the perceived responsibilities for safe design between battery development and integration engineering. If language is the medium through which humans provide control actions, then a breakdown in language could lead to hazardous system states. Given this potential, one could speculate that a concerted, industry wide effort to better communicate how lithium-ion battery systems can be designed safely would help breakdown safety concerns that are now a barrier to market growth.

Future work in on these techniques will include further development and application of STPA to analyze safety in energy storage systems, the application of Casual Analysis using Systems Theory (CAST) to analyze accidents, and working to make these abstract techniques more accessible to energy storage manufactures, integrators, and customers. This effort is working toward, in the long term, a large scale cost/effectiveness comparison between PRA and STPA for energy storage technologies.

Acknowledgments

This work was funded by the US DOE OE's Energy Storage Program. The authors would like to thank Dr. Imre Gyuk for his support of research advancing safety in grid energy storage. Special thanks to Dr. Katrina Groth, Dr. Summer Ferreira, and Dr. Josh Lamb for reviewing and editing the content this article.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

References

[1] T. Reddy, D. Linden (Eds.), Linden's Handbook of Batteries, forth ed., McGraw Hill, 2011.
[2] NFPA70E Standard for Electrical Safety in the Workplace.
[3] P. Ribiere, S. Grugeon, M. Morcrette, S. Boyanov, S. Laruellea, G. Marlair, Investigation on the fire-induces hazards of li-ion battery cells by fire calorimetry, Energy Environ. Sci. 5 (2012) 5271–5280.
[4] Q. Horn, Failure modes unique to large format cells and battery systems, in: NAATBatt Annual Meeting and Symposium, January 2014.
[5] L. Gordon, K. Carr, N. Graham, A Complete Electrical Arc Hazard Classification System and its Application, Los Alamos National Laboratory, LA-UR-14-29516.
[6] L. Florence, White Paper on Safety Issues for Lithium-ion Batteries, Underwriters Laboratories, 2012. URL, http://www.ul.com/global/documents/newscience/whitepapers/firesafety/FS_Safety%20Issues%20for%20Lithium-Ion%20Batteries_10-12.pdf.
[7] Z. Zhang, The main cause of li-ion safety and internal shorts, in: Battery Safety Conference, The Knowledge Foundation, Washington DC, 2014.
[8] D.H. Doughty, C.C. Crafts, FreedomCAR Electrical Energy Storage System Abuse Test Manual for Electric and Hybrid Electric Vehicle Applications, Tech. Rep. SAND2005-3123, Sandia National Laboratories, 2005.
[9] UL1642 Standard Lithium-Ion Batteries.
[10] UL2054 Alkaline Cell or Lithium/Alkaline Packs.
[11] United Nations, Recommendations on the Transport of Dangerous Goods, Manual of Tests and Criteria: 38.3 Lithium Metal and Lithium Ion Batteries.
[12] IEC62281 Safety of Primary and Secondary Lithium Cells and Batteries During Transport.
[13] IEC62133 Secondary Cells and Batteries Containing Alkaline or Other Non-Acid Electrolytes — Safety Requirements for Portable Sealed Secondary Cells, and for Batteries Made From Them, for Use in Portable Applications.
[14] ANSI C18.3M, Part 2-2011 American National Standard for Portable Lithium Primary Cells and Batteries Safety Standard.
[15] SAE j2929 Electric and Hybrid Vehicle Propulsion Battery System Safety Standard — Lithium-based Rechargeable Cells.
[16] IEEE1625 2008 Standard for Rechargeable Batteries for Multi-cell Mobile Computing Devices.
[17] IEEE1725 2011 Standard for Rechargeable Batteries for Cellular Telephones.
[18] L. Lu, X. Han, J. Li, J. Hua, M. Ouyang, A review on the key issues for lithium-ion battery management in electric vehicles, Power Sources 226 (2013) 272–288.
[19] Advancion: features and specs, (accessed 01.22.15.). URL http://www.aesenergystorage.com/advancion/features-specs/#safety-climate.
[20] NFPA11: Standard for Low-, Medium-, and High-expansion Foam, 2010.
[21] NFPA12: Standard on Carbon Dioxide Extinguishing Systems.
[22] NFPA 12a: Standard on Halon 1301 Fire Extinguishing Systems.
[23] NFPA 13: Standard for the Installation of Sprinkler Systems.
[24] NFPA 750: Standard on Water Mist Fire Protection Systems.
[25] NFPA 850: Recommended Practice for Fire Protection for Electric Generating Plants and High Voltage Direct Current Converter Stations.
[26] NFPA 2001: Standard on Clean Agent Fire Extinguishing Systems.
[27] J. Jeevarajan, Can cell-to-cell thermal runaway propagation in lithium-ion modules be prevented, in: Battery Safety Conference, The Knowledge Foundation, Washington DC, 2014.
[28] J.S. McLaughlin, Risks of lithium batteries in air transportation, in: Battery Safety Conference, The Knowledge Foundation, Washington DC, 2014.
[29] J. Lamb, C. Orendorff, L. Steele, S. Spangler, Failure propagation in multi-cell lithium ion batteries, J. Power Sources 283 (June 2015) 517–523.
[30] K. Marr, V. Somadepalli, Q. Horn, Explosion hazards due to failure lithium-ion batteries, in: Global Congress on Process Safety, 2013.
[31] NFPA 68: Standard on Explosion Protection by Deflagration Venting.
[32] NFPA 69: Standard on Explosion Prevention Systems.
[33] Aircraft Incident Report, Auxiliary Power Unit Battery Fire Japan Airlines Boeing 787-8, ja829j, National Transportation Safety Board, 2014. Tech. rep., URL, http://www.ntsb.gov/investigations/AccidentReports/Reports/AIR1401.pdf.
[34] Q. Wang, P. Ping, X. Zhao, G. Chu, J. Sun, C. Chen, Thermal runaway caused fire and explosion of lithium ion battery, Power Sources 208 (2012) 210–224.
[35] Battery Room Fire at Kahuku Wind-Energy Storage Farm, (accessed 01.22.15.). URL http://www.greentechmedia.com/articles/read/Battery-Room-Fire-at-Kahuku-Wind-Energy-Storage-Farm.
[36] Questions and Answers Concerning the NAS Battery Fire, (accessed 01.22.15.). URL http://www.ngk.co.jp/english/announce/111031_nas.html.
[37] APS Fire Probed, (accessed 01.22.15.). URL http://azdailysun.com/news/local/aps-fire-probed/article-1de2e924-ab0a-5e71-9a3a-6942c2d1c9bb.html.
[38] ISO 31000:2009, Risk Management.
[39] T. Aven, Quantitative Risk Assessment, Cambridge University Press, 2011.
[40] T. Aven, Foundations of Risk Analysis, John Wiley and Sons Ltd, 2003.
[41] M. Stamatelatos, Probabilistic Risk Assessment: what Is it and Why Is it Worth Performing it?, Tech. rep., National Aeronautics and Space Administration, 2000. URL, http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf.
[42] Probabilistic Risk Assessment PRA, (accessed 01.22.15.). URL http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html.
[43] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related System.
[44] UL9540 Outline of Investigation for Energy Storage Systems and Equipment.
[45] E. Zio, Reliability engineering: old problems and new challenges, Reliab. Eng. Syst. Saf. 94 (2009) 125–141.
[46] A. Stirling, Risk, precaution and science: towards a more constructive policy debate, Eur. Mol. Biol. Organ. Rep. 8 (4) (2007) 309–315.
[47] N. Leveson, Engineering a Safer World, first ed., The MIT Press, 2012.
[48] N. Taleb, The Black Swan: the Impact of the Highly Improbable, second ed., Random House Trade Paperbacks, 2010.
[49] R. C. A. Limited, Freighter Airplane Cargo Fire Risk, Benefit and Cost Model (Model Version 5), Tech. rep., Federal Aviation Administration, William J. Hughes Technical Center, 2013.
[50] D. Kahneman, Thinking, Fast and Slow, Farrar Straus and Giroux, 2011.
[51] A. Rae, R. Alexander, J. McDermid, Fixing the cracks in the crystal call: a maturity model for quantitative risk assessment, Reliab. Eng. Syst. Saf. 125 (2013) 67–81.
[52] T. Aven, E. Zio, Some considerations on the treatment of uncertainties in risk assessment for practical decision making, Reliab. Eng. Syst. Saf. 96 (2011) 64–74.
[53] C.H. Fleming, M. Spencer, J. Thomas, N. Leveson, C. Wilkinson, Safety assurance in nextgen and complex transportation systems, J. Saf. Sci. 55 (2013) 173–187. URL, http://sunnyday.mit.edu/papers/ITP-Final.pdf.
[54] N. Leveson, N. Dulac, D. Zipkin, J. Cutcher-Gershenfeld, J. Carroll, B. Barrett, Engineering resilience into safety-critical systems, Resil. Eng. Precepts (2006) 95–123.
[55] N. Leveson, Applying system engineering to pharmaceutical safety, J. Br. Interplanet. Soc. **62**. URL http://sunnyday.mit.edu/papers/JBIS-final.doc.
[56] T. Ishimatsu, Hazard analysis of complex spacecraft using systems theoretic process analysis, AIAA J. of Spacecr. Rockets. URL http://sunnyday.mit.edu/papers/JSR-paper-published.pdf.
[57] M. Placke, Application of STPA to the Integration of Multiple Control Systems: a Case Study and New Approach, Master's thesis, MIT, 2014. URL, http://sunnyday.mit.edu/papers/placke-thesis.pdf.
[58] M. Stringfellow, N. Leveson, B. Owens, Safety-driven design for software-intensive aerospace and automotive systems, Proc. Inst. Electr. Electron. Eng. 98 (4) (2010) 515–525.
[59] N. Leveson, M. Couturier, J. Thomas, M. Dierks, D. Wierz, B. Psaty, S. Finkelstein, Applying system engineering to pharmaceutical safety, J. Healthc. Eng. URL http://sunnyday.mit.edu/papers/healthcare-eng-final.doc.
[60] H. Alemzadeh, J. Raman, N. Leveson, R. Iyer, Safety Implications of Robotic Surgery: A Study of 13 Years of Data on Da Vinci Surgical Systems, Tech. rep., University of Illinois at Urbana-Champaign, 2013.
[61] A. Williams, System security: rethinking security for facilities with nuclear materials, Trans. Am. Nucl. Soc. 109 (2013) 1946–1947.
[62] W. Young, N. Leveson, An integrated approach to safety and security based on systems theory, Commun. ACM 57 (2014) 31–35.
[63] J. Thomas, F.L. de Lemos, N. Leveson, Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants, Tech. rep., MIT Technical Report, 2012. URL, http://sunnyday.mit.edu/papers/MIT-Research-Report-NRC-7-28.pdf.
[64] N. Leveson, A new accident model for engineering safer systems, Saf. Sci. 42 (2006) 237–270.
[65] J.T. Reason, J.T. Reason, Managing the Risks of Organizational Accidents, vol. 6, Ashgate, Aldershot, 1997.
[66] A.A. Akhil, DOE/EPRI 2013 Electricity Storage Handbook in Collaboration with NRECA, Tech. rep., Sandia National Laboratories, 2013.
[67] C. Fleming, Safety-driven Early Concept Analysis and Development, Ph.D. thesis, MIT, 2015. URL, http://sunnyday.mit.edu/Fleming-dissertation-final.pdf.