SANDIA REPORT
SAND2020-9360
Printed August 2020

Sandia National Laboratories

Grid-scale Energy Storage Hazard Analysis & Design Objectives for System Safety

Sandia: David Rosewater (PI)
Joshua Lamb
John Hewson
PNNL: Vilayanur Viswanathan
Matthew Paiss
Daiwon Choi
APS: Abhishek Jaiswal

Prepared for

Arizona Public Service,
Phoenix, Arizona 85004

Prepared by

Sandia National Laboratories,
Albuquerque, New Mexico 87185 and Livermore, California 94550

and

Pacific Northwest National Laboratory,
Richland, Washington 99354

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Battery based energy storage systems are becoming a critical part of a modernized, resilient power system. However, batteries have a unique combination of hazards that can make design and engineering of battery systems difficult. This report presents a systematic hazard analysis of a hypothetical, grid scale lithium-ion battery powerplant to produce sociotechnical "design objectives" for system safety. We applied system's theoretic process analysis (STPA) for the hazard analysis which is broken into four steps: purpose definition, modeling the safety control structure, identifying unsafe control actions, and identifying loss scenarios. The purpose of the analysis was defined as to prevent event outcomes that can result in loss of battery assets due to fires and explosions, loss of health or life due to battery fires and explosions, and loss of energy storage services due to non-operational battery assets. The STPA analysis resulted in identification of six loss scenarios, and their constituent unsafe control actions, which were used to define a series of design objectives that can be applied to reduce the likelihood and severity of thermal events in battery systems. These design objectives, in all or any subset, can be utilized by utilities and other industry stakeholders as "design requirements" in their storage request for proposals (RFPs) and for evaluation of proposals. Further, these design objectives can help to protect firefighters and bring a system back to full functionality after a thermal event. We also comment on the hazards of flow battery technologies.

ACKNOWLEDGEMENTS

This work was funded by the Energy Storage Systems Program of the U.S. Department of Energy Dr. Imre Gyuk, Program Director. Arizona Public Service provided proprietary technical details about an example lithium-ion battery system under non-disclosure agreement that informed this analysis. The authors would to thank Tim Bolden, Director Enterprise Risk of Arizona Public Service for supporting and contributing to this work.

The authors would like to thank Ben Schenkman at Sandia for providing an internal review of this report.

An earlier draft of this report was reviewed by Victoria Carey, Davion Hill, and Michael Kleinberg of DNV-GL and the authors would like to thank them for their comments.

CONTENTS

LIST OF FIGURES

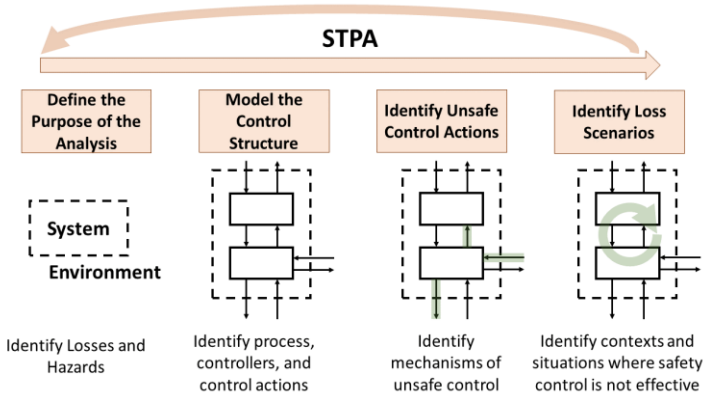
LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

Battery based energy storage systems can provide a number of services on the electric grid and have been increasingly adopted by U.S. utilities and independent power producers to be part of their generation asset portfolio. However, lithium-ion batteries present a unique combination of hazards that can make design and engineering of battery systems difficult. The hazard analysis presented in this report takes a holistic, systematic perspective on grid-scale energy storage system safety using system's theoretic process analysis (STPA). Rather than focusing on how the various battery system components fail, leading to accidents, our analysis looks at how the complex interactions among components can become unsafe, leading to potentially hazardous system states. This subtle distinction helps us anticipate not only loss scenarios caused by faulty equipment but also loss scenarios where every component works exactly as designed.

The hazard analysis of lithium-ion battery systems was conducted in four parts, shown in ES Figure 1: defining the purpose of the analysis, modeling the safety control structure, identifying unsafe control actions, and identifying loss scenarios. This illustration visually represents each part of the analysis and is described in greater detail in Section [1, 2] of this report. The purpose of the analysis was defined as to prevent loss of assets due to fires and explosions in lithium-ion battery systems, to prevent injury or loss of life due to battery fires and explosions, and to prevent loss of energy storage services due to non-operational battery assets. The safety control structure is modeled at the device level and at the sociotechnical level. Unsafe control actions are identified and enumerated in the spreadsheet in Appendix C. Six loss scenarios are identified as a result of this analysis, along with their constituent unsafe control actions and the resulting hazards. These scenarios are anticipated to occur in: procurement, system design, firefighting operations, system automation, and recovery after an incident.



ES Figure 1 Overview of system's theoretic process analysis (STPA) (adapted from [1])

Using this knowledge of how the safety control structure may fail to enforce safety constraints in lithium-ion battery systems, we are able to develop "design objectives" for system safety. The design objectives are presented as a framework which the industry can consider in the design and engineering of storage systems. The design objectives, in all or any subset, can be used by utilities as "design requirements", where applicable or appropriate, in storage request for proposals (RFPs) and for evaluating storage proposals on system safety. We realize that the energy storage industry is still on its path to maturity and it is possible that the current market offerings may not meet all the design objectives described in this report or that the design objectives may result in

prohibitive project cost. However, the design objectives help in identifying potential system deficiencies that will empower system owners/operators of these systems to see design risks more clearly and take risk management and mitigation actions (for example in the system operation and maintenance procedures). Furthermore, these design objectives provide an industry roadmap for system safety by – 1) encouraging vendors to consider the design objectives in their current and future product offerings, 2) educating standard organizations, cities and other stakeholders to incorporate design objectives in future standards and codes and 3) providing justification to utilities for additional project cost so as to incorporate the design objectives as RFP design requirements. The design objectives are summarized below and are categorized into: firefighter interaction, propagation prevention, explosion prevention, operational recovery, and data integrity. We also provide significant supplemental information about the design options integrators may choose, where appropriate, to meet these design objectives.

Design objective 1.1: The system **includes a durable, external display,** accessible from a safe location, **for firefighters to access the following information**: 1) what percentage of the cells in the system have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, 5) what actions have been taken by the automated systems (e.g. fire suppression), and 6) the presence or absence of any gases in hazardous concentrations (including smoke). Note that this design standard is dependent on local firefighters having, at least, the Technician level firefighter training standard, discussed in Section 2.3.6.	Design objective 1.2: The system includes continuous monitoring by a designated individual. This designee may be a trained and qualified utility employee or integrator employee. **This designee must be able to provide firefighters with the following information**: 1) what percentage of the cells in the system have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, 5) what actions have been taken by the automated systems (e.g. fire suppression), and 6) the presence or absence of any gases in hazardous concentrations (including smoke). To meet this design requirement a designee must be available at all times to respond to the site within a specified time period. The emergency telephone number must then be provided to the fire department and posted visibly and durably on the outside of the enclosure.
Design objective 1.3: The system includes one or more methods for firefighters to **extinguish fires and/or ventilate the environment inside the system without being exposed to fire or a potentially explosive environment**. At a minimum this includes a grid-disconnect (E-Stop) switch.	
Design objective 2.1: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to **violate the safe temperature limits** of any nearby cells, relying only on passive design.	Design objective 2.2: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to **initiate venting** in any nearby cells, relying only on passive design. See UL 1973 [28].
Design objective 2.3: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to **violate the safe temperature limits** of any cells in nearby modules, relying only on passive design.	Design objective 2.4: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to **initiate venting** in any cells in nearby modules, relying only on passive design. See UL 9540A [28] and NFPA 855 [30].
Design objective 2.1-1.4 Active: The system **includes active propagation suppression design to meet one or more of design standards 2.1-2.4**. To stop the propagation of thermal runaway using active suppression, the system design shall: 1) be able to identify when thermal runway is occurring reliably, within a short enough time to, 2) activate emergency cooling to the affected cells/modules and those cells/modules subject to direct heat transfer from the affected cells/modules, and 3) apply sufficient cooling to satisfy one or more of design standards 2.1-2.4.	Design objective 2.5: **Flammable materials** are not stored within a defined proximity (e.g. 3 feet) of the batteries. Design objective 2.6: A **fire suppression system**, for preventing fires that are not-originating from batteries (e.g. power electronic/electrical fires) from spreading to the batteries, is included in the design and installed according to the appropriate NFPA standard for its type.
Design objective 3.1: The system's enclosed environment has enough volume and a minimum passive air exchange sufficient to **prevent combustible gasses from battery venting from reaching 25% of their LEL**. The maximum rate of thermal runaway propagation assumed in analysis and testing is specified. See IEEE 1635-2018 [46] and NFPA 69 [24].	Design objective 3.2: The system has an active ventilation subsystem that identifies when thermal runway is occurring and activates forced air ventilation sufficient to **prevent combustible gasses from battery venting from reaching 25% of their LEL**. The maximum rate of thermal runaway propagation assumed in analysis and testing is specified. See IEEE 1635-2018 [46] and NFPA 69 [24].
Design objective 4.1: When the system controller detects thermal runaway in a cell, the system is designed to **electrically segment off the affected cell, module, or string, allowing the unaffected areas of the system to continue to operate.** The specific areas (racks, cabinets, containers, etc.) effected during an emergency discharge are specified. An incident recovery procedure is provided to restore the system to full or partial operation after an incident.	Design objective 3.3: The **system is designed to limit damage and vent the explosion safely** when an explosion does occur. Nearby structures are considered when siting the enclosure and locating the deflagration vents. NFPA 68 provides clarity on deflagration venting design requirements [25]. Design objective 4.2: When the system controller detects thermal runaway in a cell, the system is designed to **safely discharge any electrically independent modules** in the same enclosure to a safe handling/storage/shipping SoC (e.g. 30%).
Design objective 4.3: **The system is designed to continue to collect and record data, throughout a power outage or an extended internal fire (as able).** The expected minimum duration of backup in case of an outage is specified.	
Design objective 4.4: A complete **maintenance plan and schedule** are provided. Specific provisions are provided to remove, replace, or refurbish cells or modules where faults or latent faults have been identified. Procedures are provided to identify, trace, and remove ground faults during regular maintenance before they become hazardous or disrupt operations.	Design objective 5.1: A **field calibration verification checklist of safety critical measurements is provided** to check that the accuracy and acquisition delay of data meets requirements. Voltage measurements shall be within 2% of full-scale, current measurements shall be accurate to within 5% of full-scale, and temperature measurements shall be accurate to within 2 degrees Celsius. For safety critical automation, the time between measurement and system controller actuation shall be no more than 10 seconds. Ground fault detection circuits are tested during commissioning

Note: These design objectives overlap with each other or provide alternative methods to enforce the same safety constraint. The following list illustrates the overlapping structure of these design objectives:

- Safety critical information availability to firefighters
    - Design objective 1.1 and/or,
    - Design objective 1.2
- Safety of firefighter intervention
    - Design objective 1.3
- Thermal runaway prorogation resistance

    - Passive design or,
        - Runaway does not violate safe temperature limits in other cells (more stringent)
            - Design objective 2.1 (cell-to-cell) and/or,
            - Design objective 2.3 (module-to- module)
        - Runaway does not initiate self-heating in other cells (less stringent)
            - Design objective 2.2 (cell-to-cell) and/or,
            - Design objective 2.4 (module-to- module)
    - Active design
        - Runaway does not violate safe temperature limits in other cells (more stringent)
            - Design objective 2.1-Active (cell-to-cell) and/or,
            - Design objective 2.3-Active (module-to- module)
        - Runaway does not initiate self-heating in other cells (less stringent)
            - Design objective 2.2-Active (cell-to-cell) and/or,
            - Design objective 2.4-Active (module-to- module)
- External fire prevention/suppression
    - Design objective 2.5 and,
    - Design objective 2.6
- Explosion prevention
    - Design objective 3.1 (passive ventilation) or,
    - Design objective 3.2 (active ventilation)
- Explosion protection
    - Design objective3.3
- Automated response to a fire and/or power outage
    - Design objective 4.1 and,
        - Design objective 4.2 (subject to 4.1)
    - Design objective 4.3
- Regular maintenance and ground fault management
    - Design objective 4.4
- Data integrity and accuracy
    - Design objective 5.1

A lithium-ion battery system integrator can choose either design objective 1.1 or 1.2 to convey safety critical information to firefighters, implementing both in the same system would be redundant. Design objectives 2.1 and 2.3 are stricter versions of 2.2 and 2.4 respectively. Design objective 2.1-2.4 Active are alternative methods of implementing the passive requirements in 2.1-2.4. Explosion prevention can be achieved through either 3.1 or 3.2. Lastly, reduction of stranded energy is achieved through 4.2, which is dependent on the automated segmentation achieved through 4.1. Design objectives 1.3, 2.5, 2.6, 3.3, 4.3, 4.4 and 5.1 are independent.

Additionally, we define training objectives for firefighters responding to thermal events in battery systems. As design objectives 1.1. and 1.2 discusses the information to be provided to firefighters, training is needed to enable firefighters to interpret that information. The training outlined in this report is meant to provide the knowledge that firefighters need to interpret these data and manage risk accordingly.

Lastly, we provide overviews of the hazards and safety controls for flow battery systems. The primary hazard in flow batteries is the potential for an electrolyte spill, which can be controlled through a combination of passive engineering, active control, and emergency preparedness. While this analysis does not investigate flow battery systems in as much depth as lithium-ion systems, flow batteries are viable alternatives in both performance and safety.

This analysis provides guidance for the rapidly, evolving energy storage industry in its efforts to design, procure, and operate safe and reliable battery energy storage systems. The design objectives enable clear communication between utilities and vendors on safety related design considerations and the design objectives indirectly help to strengthen and mature the energy storage market in the U.S., thereby supporting the national interest.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AHJ	Authority Having Jurisdiction
APS	Arizona Public Service
BESS	Battery Energy Storage System
BMS	Battery Management System
EIS	Electrochemical Impedance Spectroscopy
FMEA	Failure Modes and Effects Analysis
HRR	Heat Release Rate
HVAC	Heating, Ventilation, and Air Conditioning
ICC	International Code Council
IEEE	Institute of Electrical and Electronics Engineers
IFC	International Fire Code
LFL	Low Flammability Limit
MSDS	Material Safety Data Sheet
NFPA	National Fire Protection Association
NRTL	Nationally Recognized Testing Laboratories
OEM	Original Equipment Manufacturer
PCS	Power Conversion Systems
S.D.	Smoke Detector
SDO	Standards Development Organization
SoC	State-of-Charge
STPA	Systems-Theoretic Process Analysis
THR	Total Heat Release
UCA	Unsafe Control Actions
UL	Underwriters Laboratory

1. INTRODUCTION

Battery based energy storage systems are rapidly becoming an integral part of efficient and resilient power systems around the world. This rate of proliferation is driven in part by the falling cost of batteries and in part by the increasing value they can provide as conventional generation units are retired in favor of renewable power. However, batteries can have certain failure mechanisms that make the safe operation of battery systems difficult to guarantee. But comparing the hazards of batteries to petroleum products, we realize that it is not necessarily the physical properties of batteries that lead to this difficulty, but perhaps the complex systems we engineer around them. With systemic thinking, we recognize that the cause frequently lies in the very structure and organization of the system [3].

The primary focus of this report is on lithium-ion battery systems. Section 2. applies a hazard analysis method based on system's theoretic process analysis (STPA) to develop "design objectives" for system safety. These design objectives, in all or any subset, can be used by utilities "design requirements" for issuing requests for proposals (RFPs) and for reviewing responses as a part of their procurement process. The design objectives can also serve as model standards for standard development organizations (SDOs) to consider in the course of their consensus-based work. Section 3 briefly discusses flow battery technologies as a viable alternative to lithium ion battery systems. This report's conclusions are discussed in Section 4.

2. HAZARD ANALYSIS IN LITHIUM-ION BATTERY POWER PLANTS

Our goal is to perform a systematic analysis of the complex web of causes and effects that could lead to losses and injuries from fire and/or explosion in lithium-ion battery-based energy storage. This section outlines a qualitative, systematic safety analysis of a lithium-ion battery energy storage systems (BESS) to determine high-level design requirements for battery management, fire suppression, ventilation, and emergency response.

2.1. Hazardous energy classification

Before we start to analyze hazards at the system level, we must first understand the types of energy contained in lithium-ion batteries that are potentially hazardous. Specifically, we look at the potential for fire and the deflagration of off-gases generated during thermal runaway. Thermal runaway is a 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 [4]. Causes of thermal-runaway are varied but include mechanical, electrical, and thermal abuse [5, 6]. The hazardous energy level of a given cell design, under certain testing conditions, can be measured on a scale between 0 and 7, shown in increasing order of severity Table 1 [5, 7]. At high hazard levels (5, 6, or 7) cells can produce enough heat to catch fire, rupture or explode.

Table 1 Hazardous energy levels and descriptions (adapted from Ref. [7])

Hazardous energy 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.
3	Leakage mass less than 50%	No venting, fire, or flame; no rupture; no explosion. Weight loss less than 50% of electrolyte weight.
4	Venting mass greater than 50%	No fire or flame; no rupture; no explosion. Weight loss greater than 50% of electrolyte weight.
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).

This scale, however does not necessarily reflect the potential for damage that a cell in thermal runaway could cause within a system. Hazard levels 3 and 4 can still produce a tremendous amount of heat, which, if it is not absorbed or dissipated quickly enough, can cause adjacent cells to fail in a propagating cascade. Further, it is not clear what the worst-case hazard level is. A module of well insulated cells may not propagate when one cell ruptures, releasing much of its potential heat to vent gas, while a less energetic reaction can slowly heat nearby cells resulting in a larger fire when the whole module enters thermal runaway. Perhaps more useful metrics, at least to system designers, are the heat release rate (HRR), the total heat release (THR), and the convective heat transfer rate [8]. In general, lower HRR and THR at the cell level are better, however this is not always the case. Consider first, the implications to module design between one cell type with low HRR and high THR, and another with high HRR and low THR. The first case may have more time to dissipate heat, but the second case will have less total heat to work with. Consider second, the comparison between a module of densely packed cells with relatively low HRR/THR verses a loosely packed module of cells with higher HRR/THR. Which design is less likely to undergo thermal runaway propagation depends greatly on many factors not captured by HRR or THR. These metrics present a complex picture of how heat is generated, transferred, and dissipated.

Looking at the relative HRR between chemistries, one may be inclined to assume that lithium-iron phosphate batteries are not subject to thermal runaway because their HRR characteristics are much lower than other chemistries. However, this presents only heat generation, not heat dissipation. Because lithium-iron phosphate batteries have lower specific energy, many systems that use them pack them in modules that have little or no thermal separation between cells. If there is insufficient thermal mass to absorb heat produced in a failed cell and/or the module is insulated such that the heat is not dissipated safely, then lithium-iron phosphate battery modules may indeed be vulnerable to thermal runaway propagation. Further, HRR does not account for the flammability of the electrolyte. If one or more cells are ruptured and the electrolyte starts to burn, this exothermic reaction can generate a tremendous amount of heat very quickly.

Conventional controls that system engineers use to prevent/mitigate lithium-ion battery fires can be categorized as abuse testing, battery management design, and emergency systems. Abuse testing exposes representative cells to a range of environmental conditions they would expect to see during abnormal operation, sometimes referred to as anticipated misuse, and are intended to establish safety limits [7]. Many abuse testing standards are available [9-17], each with different tests meant for different battery applications. Integrators then impose these safety limits through the design and installation of a battery management system (BMS). BMSs are designed to detect and respond to a violation of operational limits [18]. When fires occur, systems can be designed to suppress the fire with a clean agent or water. However, if the energy in the batteries remain, suppressing the fire may or may not stop the propagation of thermal runaway [19]. Instead, a variety of design methods are available for the prevention of thermal runaway propagation [20-22]. The majority of these methods can be summarized in the following categories: reducing HRR and THR through cell selection, cell level safety features, increasing module level thermal mass/separation, and increased heat-dissipation or cooling. Information on the state-of-the-art on this topic is provided in Section 2.3.2.

Vent gasses, including carbon dioxide, carbon monoxide, hydrogen, and methane, can be released from a cell in thermal runaway at reactivity levels 3 through 7. If they reach a critical concentration as an aggregate gas, the low flammability limit (LFL), in an enclosed space, a spark can cause an explosion [23]. This phenomenon can be investigated with a cell test chamber, gas analysis, and combustion test chamber apparatus. In a series of tests performed on 7.7 Ah, lithium-ion cells at 100% SoC produced approximately 2.5 L of gas mixture with an aggregate LFL of 6.3% and explosion severity index Kg 65 m-bar/s (comparable to methane at 46 m-bar/s, or propane at 76 m-bar/s) [23]. This kind of potential hazard is typically controlled by deflagration prevention ventilation which keeps gas concentrations from reaching the LFL [24], and/or explosion protection by deflagration venting [25].

2.2. Hazard analysis

The purpose of this analysis is to provide an answer for how to prevent fires and explosions in large-scale, stationary, lithium-ion battery energy storage systems (BESS). Additionally, we want to answer for how firefighters can respond safely to a fire in a lithium-ion BESS. We will consider a roughly 2MW-8MWh system deployed in a standalone building or container. With this example in mind, we can begin to establish the physical boundaries of the system and imagine how firefighters may interact with it. Beyond the boundaries of the system and incident response, there is a sociotechnical system that designs, installs, operates, and decommissions a lithium-ion battery system. A secondary purpose of this analysis is to determine how to effectively integrate fire and explosion prevention, and firefighter response, into this system such that battery energy storage devices can continue to supply critical grid services.

The analysis in this report takes a holistic, systematic perspective on grid energy storage system safety. Rather than focusing on how the various battery system components fail, leading to accidents, our analysis looks at how the complex interactions between components can become unsafe, leading to potentially hazardous system states. This subtle distinction helps us anticipate both loss scenarios caused by faulty equipment, and loss scenarios where every component works exactly as designed. The method we use is Systems-Theoretic Process Analysis (STPA) [1, 2, 26]. STPA is useful in situations where there are many "unknown-unknowns," or hazardous situations that are difficult to predict before they happen. While many technologies have the advantage of a long track record, lithium-ion batteries are a relatively new technology that is being used in new

environments and applications. The broad structure of an SPTA is shown in Figure 2. This illustration visually represents each part of the analysis and is described in greater detail in [1, 2]. We have followed this structure in our analysis, and in this report.

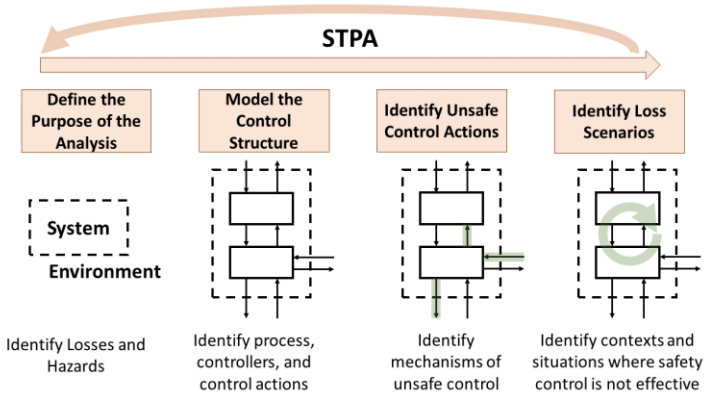


Figure 2 Overview of STPA (adapted from [1])

2.2.1. Definition of Purpose

As stated above, the primary purpose of this analysis is to prevent fires and explosions in lithium-ion battery systems. From this objective we will define several loss events that systems should be designed to prevent.

Loss 1 [L1]: Thermal-runaway propagation. Loss of Asset: Lithium-ion batteries can fail in thermal runaway. In a BESS, failure of one cell can cause nearby cells to fail. The loss of one cell, one module, or even one whole string could be considered acceptable. In this analysis, we will define two levels of propagation that are considered unacceptable outcomes: cell-to-cell, and module-to-module. Cell-to-cell is where a single cell in thermal runaway generates the conditions for another cell to enter thermal runaway. Module-to-module propagation is where one or more cells in thermal runaway in one modular unit of cells generates the conditions for a cell to enter thermal runaway in another modular unit.

Loss 2 [L2]: Vent-gas explosion. Loss of Asset: When in thermal runaway, lithium-ion batteries can off-gas combustible elements and compounds. In an enclosed or localized area, these gases can explode, causing severe equipment damage.

Loss 3 [L3]: Injury or death. Loss of health or life: If humans are exposed to the fire or explosion conditions, it could lead to their injury or death. Different categories of people could be exposed differently to the same incident. For example, a firefighter may have a breathing apparatus to protect them from smoke, but bystanders may not have such personal protective equipment.

Loss 4 [L4]: Non-operation: Loss of energy storage services**.** The services being provided by a BESS could be critical to maintaining a safe and reliable power system. In some circumstances loss of power can cost lives and so continuity of service is important. This also includes a system being unrecoverable after an incident.

These losses could result from a hazardous system state in combination with some worst-case environmental condition. An example of this is where a build-up of combustive gas (hazard) may or may not lead to an explosion (loss). The system should be designed to avoid hazards. A list of the

hazardous system states we will assess is presented in Table 2. These hazards are ordered numerically for easy reference, and not by increasing severity.

Table 2 Hazardous System State Definitions

Hazard #	Definition
Hazard 1 [H1]:	an otherwise normal cell exceeds safe limits on voltage, current, or temperature [L1]
Hazard 2 [H2]:	off-gas concentration exceeds safe limit [L2]
Hazard 3 [H3]:	human exposure to a fire or an explosion [L3]
Hazard 4 [H4]:	human exposure to hazardous voltage or arc-flash [L3]
Hazard 5 [H5]:	human exposure to toxic smoke or hazardous fire suppression [L3]
Hazard 6 [H6]:	extended service outage, or numerus maintenance calls [L4]

Note that this is not an exhaustive list of the potentially hazardous states, only those that apply to the losses defined above.

2.2.2. Model of the safety control structure

The system enforces safety constraints at two levels: a sociotechnical level and a device level. An illustration of the sociotechnical control system is shown in Figure 3. At this level, control actions are decisions made by people based on their understanding of the hazards of lithium-ion batteries and how to prevent fires. A detailed description of each actor/controller, their safety responsibilities, and their mental models is provided in Appendix B.

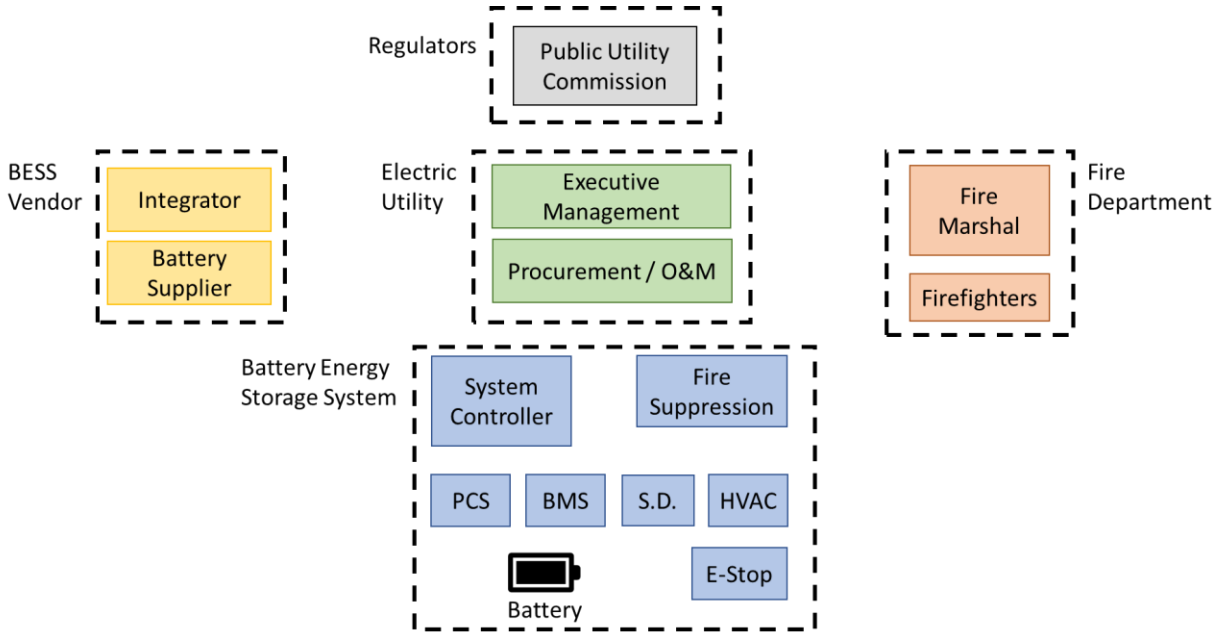


Figure 3 High-level sociotechnical safety control structure of a battery energy storage system

An illustration of the device level control system is shown in Figure 4. At this level the system controller makes automated decisions based on the programed models and thresholds. A single representative battery is used to simplify our analysis, but the analysis includes the connections from

this battery to the many batteries that are installed near this battery. During thermal runaway, the heat produced by one cell will, to some degree, be absorbed by nearby cells. In this context, cell refers to a single manufactured electrochemical cell, whereas the term battery refers to any collection of cells. In this analysis, we will use battery to refer to a collection of cells that are manufactured together (e.g. "A car battery has six lead-acid cells in series to achieve 12V at the terminals"). A control loop, in this context, is made up of four component types: controlled processes, sensors, actuators, and controllers/decision makers. The safety of the representative battery is the controlled process, the sensors collect data from the battery through measurements and supply data to the system controller through a communication protocol such as MODBUS (or in some devices, such as many smoke detectors (S.D.) and thermostats, a simple contactor). The system controller then makes decisions about charge/discharge, fire suppression, heating, cooling and ventilation. Note that these decisions can be made separately by an energy management system, fire-control-console, thermostat, etc., but these are all components of the system controller in our analysis. The system controller's decisions are implemented through actuators: charge/discharge through the power conversion system (PCS), heating, cooling and ventilation through the heating, ventilation, and air conditioning (HVAC) system and fire suppression through the fire suppression system.

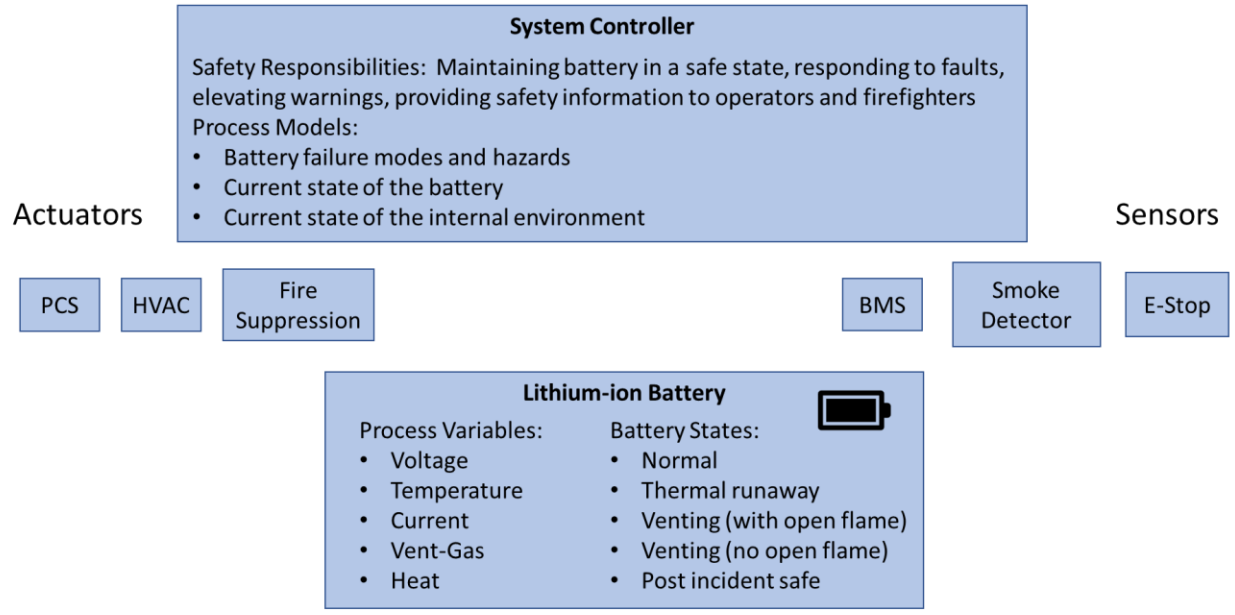


Figure 4 Automated battery energy storage system safety control structure

Each element within these safety control structures has some number of inputs, outputs, and models for how other components behave (in automated controllers these are engineered models, in humans these are mental models). We enumerate all outputs from each element as rows in the table presented in Appendix C. Each output is a control action that works to enforce safety constraints and avoid hazardous system states. The exhaustive list can be difficult to navigate and is included only for completeness and for reference in the identification of unsafe control actions.

2.2.3. Identification of unsafe control actions

Each control action identified in the safety control structure has the potential to generate a hazardous system state through one of four mechanisms: 1) it could cause a hazard by not being provided when needed, 2) it could cause a hazard by being provided when not needed, 3) it could cause a hazard by being provided too early, too late, or out of order, and 4) it could cause a hazard by being provided for too much time or too little time. The process of enumerating each unsafe control action is lengthy but useful in identifying the context and triggers that could lead to the hazards described above. In the analysis we classify unsafe control actions into five categories, listed in Table 3. This categorization helps us to later collect unsafe control actions into descriptive loss scenarios. The full list of unsafe control actions is included in Appendix C.

- Control action: Any physical or digital signal between elements in the safety control structure. Examples include:
    - Heat transferred from a cell in thermal runaway (with an open flame) to another, otherwise normal, cell (row #83 in Appendix C)
    - The MODBUS communication of cell temperatures provided by the BMS to the system controller (#58 in Appendix C)
    - The utility issuing a Request for Proposals (RPF) to collect bids for a new battery system (row #21 in Appendix C)
- Unsafe control action (UCA): A control action that violates a safety constraint and generates a hazard
    - UCA-D83: With open flames, the heat produces by a single cell in thermal runaway is immense. An unsafe control action would be if heat exceeded the maximum design limit to prevent propagation of thermal runaway [H1].
    - UCA-E58: Useful data must be appropriately timestamped. A mistimed temperature measurement could appear to reverse causes and effects in a post-mortem analysis. This could make causal analysis more difficult and could lead to extended system downtime [H6].
    - UCA-D21: Writing a complete RFP requires some knowledge of battery energy storage technologies. Being able to interpret the proposals received requires even more. Selecting a vendor who has a design that insufficiently enforces safety constraints could lead to a hazard [H1, H2].

Table 3 Unsafe Control Action (UCA) Categories

Category	Category Descriptions
BESS Procurement	This category is assigned to all UCAs involved in the following: As a result of the process of issuing a request for proposals and selecting an integrator, a vendor and system is selected that does not effectively enforce safety constraints.
BESS Design, installation, and commissioning	This category is assigned to all UCAs involved in the following: In the process of designing, installing and commissioning the operational system does not effectively enforce safety constraints

Category	Category Descriptions
Firefighter Training and Response	This category is assigned to all UCAs involved in the following: When responding to a fire in a battery system, firefighters are unable to identify, avoid, or mitigate hazards effectively.
System Response to Spontaneous Cell Fire	This category is assigned to all UCAs involved in the following: During charge/discharge operations one cell enters the self-heating state. It progresses into thermal runaway and vents gases to its environment. It generates heat which is absorbed by adjacent cells. The propagation of thermal runaway continues until other cells catch fire and/or until vent gases accumulate.
Post incident response and recovery	This category is assigned to all UCAs involved in the following: After an incident has occurred damaged modules are removed and replaced, allowing the system to be restored to full functionality. The response and recovery process is conducted such that a hazard develops or the restored system does not effectively enforce safety constraints.

2.2.4. Identification of loss scenarios

In this section we identify six scenarios that describe how the unsafe control actions could combine with environmental factors to generate hazards. These scenarios are not meant to anticipate every possible path to a loss, only to help identify systematic failure mechanisms such that we can plan or design systems to avoid them.

Note: each scenario references numeric codes for unsafe control actions (UCAs). The description of each UCA can be found in Appendix C. The letter refers to the column, which are organized by type (C: control not provided when needed, D: control provided when not needed, E: control provided too early or late, F: control stopped too soon, applied too long). The number refers to the row and is organized by control action (e.g. 56: BMS providing voltage measurements to the system controller).

Scenario 1 Procurement: In following procurement targets set by the public utility commission PUC (UCA-E4) executive management at the utility applies inappropriate risk tolerance (UCA-D18) to their procurement department. The engineers in the procurement process then establish requirements in the request for proposals that either do not adequately enforce safety constraints or are cost prohibitive (UCA-D21). As the locally adopted codes may not adequately cover fire and/or explosion in lithium-ion systems, utility personnel, the fire marshal, and other authorities having jurisdiction may not be adequately equipped to judge if a vendor's system adequately enforces safety constraints (UCA-D22, UCA-D28). This pervasive uncertainty leads to both inefficiency in the procurement process and an inability to know when an unsafe system has been procured [H1, H2].

Scenario 2 Design: If there is uncertainty in how much heat or vent gas is released in the worst-case cell failure (UCA-E13) then it could be difficult to design the system to avoid propagation of thermal runaway or combustion (UCA-E7) [H1, H2]. If the limits on voltage, current, and temperature are uncertain (UCA-E13) or are not communicated effectively to the integrator (UCA-

C14, UCA-D14) then the system may not be designed to enforce the correct limits through the BMS's configuration (UCA-E7) [H1, H2]. This, in turn, would also make it difficult to communicate the effectiveness of safety constraint enforcement in the proposal process (UCA-E8). Lastly, these uncertainties would also make it difficult to test the effectiveness of safety constraint enforcement during commissioning (UCA-E9), which could lead to a hazard [H1, H2].

Scenario 3 Fire Response: When firefighters arrive on the scene of a battery system fire they assess what people or property are in danger and what hazards are present. If these hazards and potential hazards are not clear, they unknowingly may be exposed to a hazard. For example, if thermal runaway has propagated to the to the point where there is a hazardous build-up of combustive gas [H2], then this may not be clear when looking at the system from the outside. Hence, firefighters may decide to open the system to inspect the inside, thereby being exposed to a hazard [H3] (UCA-D32). Conversely, they may first ask the system owner (electric utility) (UCA-C33, UCA-E33) for information, but the utility POC may not have any more information about the current state of the system than the firefighters (UCA-C25, UCA-D25), especially if some or all of the data from inside the system is unavailable or inaccurate (UCA-D40).

Scenario 4 System Automation 1: There are overlapping and potentially conflicting goals/responsibilities between active fire suppression, combustion prevention, and thermal runaway propagation prevention. For example, if a cell is in thermal runaway it may not generate sufficient smoke to be detected by the smoke detector (UCA-C63, UCA-D82), and in a close packed environment, the failure may propagate from cell-to-cell (UCA-D83, UCA-D90) [H1]. If enough cells are in runaway to trigger the smoke detector, then extinguishing the flames with active fire suppression may cause more combustive gas to be generated (UCA-D82 to UCA-D89). This is because the flammable gases would not be actively consumed by the flame. Hence, while fire suppression is meant to slow propagation of thermal runaway, it may inadvertently lead to the build-up of combustive gases [H2] (UCA-C44). In response, the HVAC could rapidly ventilate the enclosure. If the air temperature outside the system were high, then this action may accelerate and exasperate propagation of thermal runaway by pre-heating cells and feeding any open flame with oxygen [H1] (UCA-D44). If propagation accelerates enough then the generation of vent gas could outpace the capabilities of the HVAC (UCA-C44), leading to a build-up of combustive gases [H2]. This loss scenario could be instigated by an internal short-circuit, an external short-circuit, electrical/thermal/mechanical abuse conditions, or an external fire (UCA-D72).

Scenario 5 System Automation 2: Complete system shutdown and disconnection may remove some hazards while it leads to other hazards. The idea behind system shutdown is to disconnect energy sources from each other to place the system in a safe state (UCA-C40). Battery strings can be disconnected and segmented to reduce voltage to a safer level. Not doing so before maintenance could expose a worker to hazardous voltage [H4]. However, if thermal runaway is actively progressing, disconnecting the batteries from the grid may simply strand the energy where it could otherwise be fuel for a runaway reaction. Additionally, removing the grid as a power source places the sensor system on backup power. When the backup runs out, firefighters and the utility operations would no longer have access to data from inside the system (UCA-D40) [H3, H4, H5]. A ground fault (UCA-C60) can lead to operation disruption [H6] or exposure to voltage if a worker is unaware of it [H4].

Scenario 6 Recovery: It is critical to system recovery that the data collected from all cells in the system can be trusted to be accurate in both value and timestamp (UCA-E56-58, and UCA-E69 through UCA-E87). Accurate date would enable a postmortem analysis to determine which cells

violated their safety constraints (and whose modules need to be replaced) and which cells did not violate their safety constraints and are safe to return to service (UCA-F59). For those cells that have violated safety constraints, a latent internal fault (e.g. short circuit) could lead to self-heating or even thermal runaway (UCA-D95, UCA-E95) after an indeterminate amount of time. Discharging these cells to a safe SoC could mitigate or even eliminate this hazard, but it may not be possible to do so (UCA-C93). If cells are not monitored closely (UCA-C94, UCA-E93, UCA-E94) then they could be in a hazardous state when next needing to be moved or disposed (UCA-D93) [H3, H4, H5].

2.3. Risk management and mitigation

Clear design objectives are useful for reducing uncertainty in system integration and procurement (Scenario 1 and Scenario 2). Importantly, the proposed design objectives in this section are principled but simplified drafts for consideration by standards development organizations or utilities. Design Objectives 1.1, 1.2 and 1.3 help clarify how firefighters will interact with a BESS (Scenario 3). Design Objectives 2.1 through 2.6 help clarify how a BESS can be designed to prevent the propagation of thermal runaway (Scenario 4). Design Objectives 3.1 and 3.2 help clarify how a BESS can be designed to prevent the build-up of combustive vent gases (Scenario 4). Design Objectives 4.1 through 4.3 help clarify how a BESS can be designed to safely recover from incidents and be restored to full functionality (Scenario 5 and Scenario 6). Objective 4.4 defines the needs of a maintenance plan and schedule (Scenario 5). Design Objective 5.1 specifies how system commissioning plays an important role in all the other design objectives (Scenario 2). These design objectives overlap with each other or provide alternative methods to enforce the same safety constraint. An integrator can choose either chose design objective 1.1 or 1.2 to convey safety critical information to firefighters, implementing both in the same system would be redundant. Design objectives 2.1 and 2.3 are stricter versions of 2.2 and 2.4 respectively. Design objective 2.1-2.4 Active is an alternative method of implementing the passive requirements in 2.1-2.4. Design objectives 2.5 and 2.6 are intended to prevent an external fire from spreading to the battery system. Lastly, explosion prevention can be achieved through either 3.1 or 3.2.

Note that these objectives are meant to reduce the likelihood and impact of fires and explosions. They do not make any guarantees that fires or explosions cannot occur when implemented. Every design objective can be thwarted by human error, sabotage, or unanticipated circumstances.

2.3.1. Design objectives for firefighter safety

When firefighters arrive on the scene of a battery system fire, they initiate an ongoing hazard assessment with priorities being life, property, then environment. The system must be designed such that firefighters can understand the current state of the system without being exposed to a hazard. Information they need to assess the system hazards include 1) what percentage of the cells in the system have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, 5) what actions have been taken by the automated systems (e.g. fire suppression), and 6) the presence or absence of any gases in hazardous concentrations (including smoke). When firefighter action is required, such as in the case of an uncontrolled runaway reaction that may spread to nearby structures, options must be available for actions that do not expose firefighters to the hazards inside the system. An example of this is for an external valve allowing a fire truck to pump water directly into a system from the outside. Another example is an externally located manual exhaust switch to ventilate the interior. These

options shall be clearly defined in the BESS emergency action plan provided to the fire department prior to commissioning the system.

Design objective 1.1: The system includes a durable, external display**,** accessible from a safe location, for firefighters to access the following information: 1) what percentage of the cells in the system have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, 5) what actions have been taken by the automated systems (e.g. fire suppression), and 6) the presence or absence of any gases in hazardous concentrations (including smoke). Note that this design objective is dependent on local firefighters having the training to interpret the information provided, as discussed in Section 2.3.6.

Design objective 1.2: The system includes continuous monitoring by a designated individual[1]. This designee may be a trained and qualified utility employee or integrator employee. This designee must be able to provide firefighters with the following information: 1) what percentage of the cells in the system have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, 5) what actions have been taken by the automated systems (e.g. fire suppression), and 6) the presence or absence of any gases in hazardous concentrations (including smoke). To meet this design requirement a designee must be available at all times to respond to the site within a specified time period. The emergency telephone number must then be provided to the fire department and posted visibly and durably on the outside of the enclosure. Note that this design objective is dependent on local firefighters having the training to interpret the information provided, as discussed in Section 2.3.6.

Design objective 1.3: The system includes one or more methods for firefighters to extinguish fires and/or ventilate the environment inside the system without being exposed to fire or a potentially explosive environment. At a minimum this includes a grid-disconnect (E-Stop) switch.

Examples information display:

This section offers guidance on how to display information about the current state of the system in a durable exterior energy storage fire alarm control panel. Figure 5 shows an example alarm control panel designed to convey information that satisfies design objective 1.1. Note that the display should be accessible from a safe location.

[1] This is intended to be a rotating position that is designated to one or more responsible individuals at a time with a clear primary/backup/secondary backup designation.

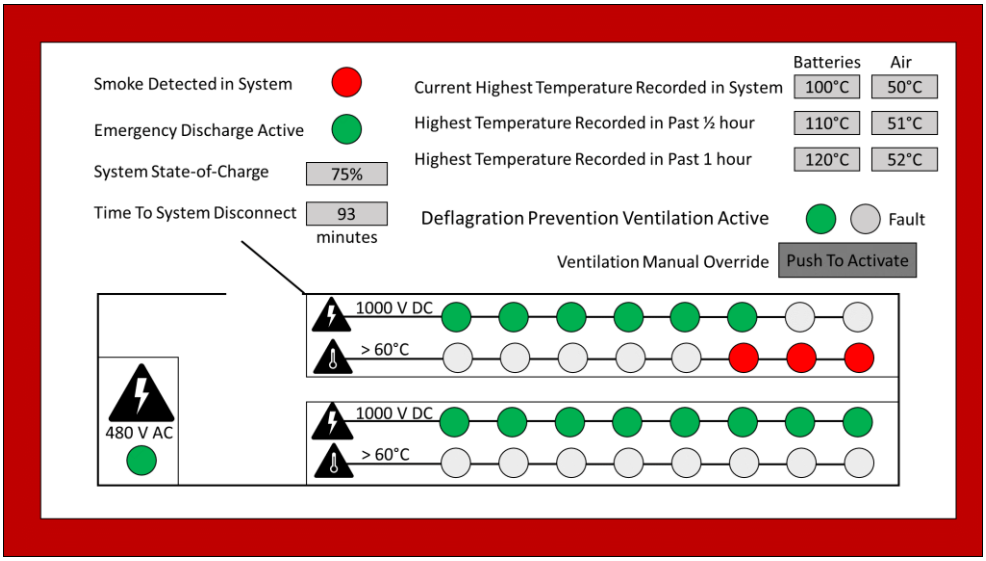


Figure 5 Example layout for an energy storage fire alarm control panel

2.3.2. Design Objectives for Thermal-Runaway Propagation Prevention

To prevent the (cell-to-cell) propagation of thermal runaway, the heat produced by any one cell undergoing thermal runaway must not be sufficient to violate the temperature safety constraints of any other cell. To prevent the (module-to-module) propagation of thermal runaway using a passive system design, the heat produced by any one module undergoing thermal runaway must not be sufficient to violate the temperature safety constraints of any cells in the adjacent modules. To be successful, these requirement needs to hold even when the other cells are pre-heated through operation to the maximum temperature at which they are expected to operate. This can be accomplished through a range of methods including 1) increasing cell thermal separation (e.g. with air, insolation, or heat absorbing/conducting material), 2) reducing the total heat released during thermal runaway (e.g. by selecting a different cell chemistry or operating at a reduced SoC). The design should consider what the worst-case temperature and charging/discharging conditions are, if it is feasible that the adjacent cell could be in this condition, and how that may affect the maximum temperature reached. To qualify as a passive design, preventing propagation must not rely on any active suppression systems. Note that as external fires can cause thermal runaway in any number of cells simultaneously, fulfilling passive propagation requirements do not exempt the system from ventilation or emergency response design requirements. Cell-to-cell and module-to-module propagation test procedures to demonstrate these design objectives are available in [27-29] and [30].

Fire suppression and thermal runaway propagation prevention, while often conflated, are designed to suppress extremely different phenomena. The role of a fire suppression system is, primarily, to extinguish flames. As lithium-ion batteries in thermal runaway retain their ability to generate heat with or without an open flame, fire suppression has limited effectiveness when applied in this context. To be effective at preventing thermal runaway propagation, a fire suppression system needs to remove enough heat, over a long enough period, to prevent nearby cells or modules from exceeding their safe temperature limit and/or entering a self-heating state. The work in [19] provides an example of how a sprinkler system, in combination with adequate separation distances, can be used to effectively prevent thermal runaway propagation. A fire suppression system can be a critical part of preventing an external fire from spreading to the batteries. A fire can start in the electronics

or structural materials near the batteries and in such cases propagation prevention could be insufficient to protect the system.

Design objective 2.1: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to **violate the safe temperature limits** of any nearby cells, relying only on passive design.

Design objective 2.2: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to **initiate venting** in any nearby cells, relying only on passive design. See UL 1973 [29] or IEC62619 [30].

Design objective 2.3: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to **violate the safe temperature limits** of any cells in nearby modules, relying only on passive design.

Design objective 2.4: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to **initiate venting** in any cells in nearby modules, relying only on passive design. See UL 9540A [28] and NFPA 855 [31].

Design objective 2.1-2.4 Active: The system includes **active propagation suppression design** to meet one or more of design objectives 2.1-2.4. To stop the propagation of thermal runaway using active suppression, the system design shall: 1) be able to identify when thermal runway is occurring reliably, within a short enough time to, 2) activate emergency cooling to the affected cells/modules and those cells/modules subject to direct heat transfer from the affected cells/modules, and 3) apply sufficient cooling to satisfy one or more of design objectives 2.1-2.4.

Design objective 2.5: Flammable materials are not stored within a defined proximity (e.g. 3 feet) of the batteries.

Design objective 2.6: A fire suppression system, for preventing fires that are not-originating from batteries (e.g. power electronic/electrical fires) from spreading to the batteries, is included in the design and installed according to the appropriate NFPA standard for its type.

State of the Art in Thermal Runaway Propagation Prevention

The design of modules of both high energy density and high reliability presents a specific challenge in regard to preventing a single cell thermal runaway from propagating to neighboring cells. Further, most consumer level safety devices are designed with low voltage consumer electronics in mind and are often inadequate in high energy battery modules. The principal concern is preventing a single cell failure from propagating to the surrounding cells. Randomized single cell failures, while rare, are difficult to prevent under all conditions. When a system level failure is an unacceptable consequence, the primary solution is ultimately designing the system to be robust to failure propagation. Propagation resistance is typically tested by initiating a single cell within a battery and observing if the thermal runaway of the single cell propagates to neighboring cells and further through the module. Various testing organizations have developed procedures for performing this test [15, 27, 28, 32].

Current strategies use a combination of cell selection, spacing of cells and interstitial material to build passive thermal runaway propagation resistance into the module. NASA's manned spaceflight programs have been at the forefront of the design of high energy density, high reliability modules [32]. Darcy et al. [33] have presented a design using LG MJ1 cells in an aluminum heat sink

array, which provides both separation of the cells and additional heat sink material. This provides a thermal runaway propagation resistant design with a specific energy of 191 Wh/kg.

While vehicle original equipment manufacturers (OEMs) typically do not have the same reliability requirements seen in Space and Defense missions, they have fielded the largest numbers of high capacity and high energy density systems to date and in some cases have developed strategies toward failure propagation mitigation. Propagation resistant designs typically focus on cylindrical cells such as those previously patented by Tesla, as well as those developed at NASA [33, 34]. Even close packing of cylindrical cells provides significant gaps between cells, with minimal contact area between cells. Cylindrical cells also have the advantage of built-in safety devices (e.g. ventilation circuit breaker pop-tabs) that have been shown to be effective at preventing some forms of failure [35]. However, the geometric inefficiency of cylindrical cells also limits at least the volumetric energy density, as significant space is lost in the module design. Pouch cells offer a much higher energy density (Wh/L), and even a higher specific energy (Wh/kg) as they typically are enclosed in a small amount of polymer wrapping. However, because they lack the cases that naturally absorb and help dissipate heat, pouch cells can be significantly more challenging to design in a system that takes thermal runaway propagation resistance into account.

System level safety improvements are an attractive target for improving energy density of batteries while still maintaining high reliability. The notion is that improving safety at the system level would allow the use of high energy density cell chemistries while still maintaining high reliability. A strategy currently being pursued is advanced methods for failure detection, especially in regard to improving the energy density of lithium ion systems. The goal is to provide a means for detecting single cell failure during early stages before catastrophic thermal runaway. With demonstrated reliability, these strategies could be an alternative to thermal runaway propagation resistance. Rather than ensuring thermal runaway is unable to propagate, the system would detect the onset of failure early and allow for intervention (e.g. emergency water cooling). This would be most helpful in manned systems, where intervention by an operator would be possible.

Advanced materials to mitigate cell-to-cell failure propagation are also being explored. Phase change materials have been proposed [34, 36] by various parties as a potential thermal runaway propagation barrier. The current technical challenge with phase change materials is if thermal management is also needed for normal operation. Phase change materials are typically tuned to be active at a specific temperature. Temperatures where thermal runaway is a concern are often much higher than the normal operating temperatures of a battery, so phase change materials can often be tuned for normal thermal management, or thermal runaway mitigation, but not both. Darcy et al. [33] demonstrated the use of a vaporizing heat sleeve to prevent thermal runaway propagation. Under a specific set of abuse conditions, this design was able to prevent the propagation of thermal runaway with 227 Wh/kg at the module level.

State of the Art in Early Battery Fault Detection

There is current research and development in the area of early battery fault detection, suggesting researchers possibly are nearing a breakthrough. CAMX Power has developed and marketed a device claimed to detect internal short circuits [37]. While little details on the operating principals of the technique are publicly available, demonstrations that have been made public have been promising and the device is a size that is suitable for on-board integration.

Electrochemical Impedance Spectroscopy (EIS) is a potentially powerful method for interrogating batteries, as it can provide a snapshot of the electrochemical state of a battery, however the equipment is typically limited to the laboratory due to the time and expertise required for making

measurements. New techniques and hardware strategies are being explored to make it more useful as a diagnostic and monitoring tool. Love et al [38, 39] as well Srinivasan et al [40-42] have explored using single frequency EIS measurements, under certain conditions, to detect changes in battery temperatures (through predictable changes in the impedance spectrum) as well as to evaluate the health of a cell. Single frequency measurements are comparatively fast and easier to evaluate making them ideal for on-board monitoring. Idaho National Laboratories working with Montana Tech [43-45] developed a tool capable of making full spectrum measurements in seconds instead of hours. This has been used at Sandia National Laboratories to evaluate lithium ion cells under abuse conditions. This hardware is currently at the laboratory benchtop scale and significant miniaturization would be needed to make it appropriate for on-board monitoring.

Sensors for abnormal concentrations of lithium-ion vent gasses have been developed through the US Navy, DOE, and private sector to be recently commercialized [46]. A network of sensors distributed throughout a system and at any air intakes and outlets, can detect trace amounts of vent gasses, preempting a classical smoke detector by 5 to 30 minutes in some cases. This type of sensor could be a critical component in an active thermal runaway propagation suppression design.

2.3.3. Design Objectives for Explosion Prevention and Protection

To prevent the build-up of combustible gases within an enclosed environment using a passive design, the system needs to have enough ventilation to prevent the vent-gases from reaching their LFL. In a space with little or no ventilation, this requirement is determined by the volume of the enclosed area and the maximum amount of vent-gas produced by the cells during thermal runaway (no open flame). In a space with open vents, this requirement is a function of the volume of the space, the rate of gas generation in individual cells, the maximum rate of thermal runaway propagation between cells, and the number and size of the vents. For active ventilation designs, the system must be able to identify when thermal runway is occurring reliably, within a short enough time to activate forced air ventilation. The minimum air-flow-rate requirement is calculated as a function of the volume of the space, the rate of gas generation in individual cells, and the maximum rate of thermal runaway propagation between cells.

Systems that satisfy design objectives 2.1-2.4 on passive thermal runaway propagation prevention or 2.1-2.4 Active on active thermal runaway propagation suppression should use a minimum thermal runaway propagation rate provided to and approved by the customer or Authority Having Jurisdiction (AHJ) (e.g. one cell per minute). The IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications [47], while applicable only to lead-acid and nickel-cadmium batteries, provides guidance on passive ventilation analysis. The National Fire Protection Association (NFPA) 69 provides some clarity on deflagration prevention by combustible concentration reduction [24]. This requires that the combustible gas concentration shall be maintained at or below 25% of the lower flammability limit. Note that NFPA 69 also contains provisions for deflagration prevention by oxidant concentration reduction. As oxygen can be a product of the thermal runaway-venting in some lithium-ion batteries, specifically from decomposition of the positive active material [48], this kind of deflagration prevention might not be effective. Smoke and vent-gas must be ventilated such that concentrations are defused for nearby homes or businesses.

Design objective 3.1: The system's enclosed environment has enough volume and a minimum passive air exchange sufficient to **prevent combustible gases from battery venting from**

reaching 25% of their LFL. The maximum rate of thermal runaway propagation assumed in analysis and testing is specified. See IEEE 1635-2018 [47] and NFPA 69 [24].

Design objective 3.2: The system has an active ventilation subsystem that identifies when thermal runway is occurring and activates forced air ventilation sufficient to **prevent combustible gases from battery venting from reaching 25% of their LFL**. The maximum rate of thermal runaway propagation assumed in analysis and testing is specified. See IEEE 1635-2018 [47] and NFPA 69 [24].

Design objective 3.3: The system is designed to limit damage and vent the explosion safely when an explosion does occur. Nearby structures are considered when siting the enclosure and locating the deflagration vents. NFPA 68 provides clarity on deflagration venting design requirements [25].

2.3.4. Design Objectives for Operational Recovery

To ensure that the system is recoverable after minor incidents, it should be designed to discharge every available cell to a safe handling SoC upon identification of one or more cells in the self-heating state (or detection of smoke or vent-gas). Reducing stranded energy both removes potential fuel for a propagating reaction and makes returning a system to service after an incident much easier because removal and replacement of damaged cells is easier, safer, and less costly at low SoC. Data acquisition systems should be designed to continue to collect and record data during and after an incident. As incidents can last for 24 hours or more, the system can be designed not to disconnect the data acquisition system from grid power during an incident. The integrator should supply an incident recovery procedure for performing a post-mortem analysis, identifying which cells need to be removed/replaced, and recommendations for restoring the system to full operation.

Design objective 4.1: When the system controller detects thermal runaway in a cell, the system is designed to electrically segment off the affected cell, module, or string, allowing the unaffected areas of the system to continue to operate. The specific areas (racks, cabinets, containers, etc.) effected during an emergency discharge are specified. An incident recovery procedure is provided to restore the system to full or partial operation after an incident.

Design objective 4.2: When the system controller detects thermal runaway in a cell, the system is designed to safely discharge any electrically independent modules in the same enclosure to a safe handling/storage/shipping SoC (e.g. 30%).

Design objective 4.3: The system is designed to continue to collect and record data, throughout a power outage or an extended internal fire (as able). The expected minimum duration of backup in case of an outage is specified.

Design objective 4.4: A complete maintenance plan and schedule are provided. Specific provisions are provided to replace or refurbish cells or modules where faults or latent faults have been identified. Procedures are provided to identify, trace, and remove ground faults during regular maintenance before they become hazardous or disrupt operations.

2.3.5. Design Objectives for Measurement Assurance

Design objectives 1.1, 1.2, 1.3, 2.3, 3.2, and 4.1-4.4 all depend on accurate values and time stamps for data collection and records. Because of this, tests on the accuracy and timeliness of data during

commissioning are critical for preventing and responding to fires in BESS. Commissioning must include a checklist of measurements that undergoes field calibration.

Design objective 5.1: A field calibration verification checklist of safety critical measurements is provided to check that the accuracy and acquisition delay of data meets requirements. Voltage measurements shall be within 2% of full-scale, current measurements shall be accurate to within 5% of full-scale, and temperature measurements shall be accurate to within 2 degrees Celsius. For safety critical automation, the time between measurement and system controller actuation shall be no more than 10 seconds. Ground fault detection circuits are tested during commissioning[2].

2.3.6. Firefighter Training Objectives

Clear training objectives are useful for reducing uncertainty for firefighters responding to incidents in lithium-ion BESSs (Scenario 3). These are meant to guide the development of online and classroom and trainings to be offered to firefighters in areas where lithium-ion battery power plans are or may be installed. As design objectives 1.1. and 1.2. discuss the information to be provided to firefighters training is needed to enable firefighters to interpret that information. The training outlined below is meant to provide the informational models that firefighters need to interpret these data and manage risk accordingly. As the design and the training are codependent, it is recommended that that they be developed together. An exemplary safety training program is discussed in [49].

Training objective: This training will be classroom based and will focus on hazard identification, risk assessment, and actions that can be taken in different example scenarios. Firefighters will be trained to recognize the presence of lithium-ion batteries. They will be trained to recognize high voltage hazards, and compounding factors (such as an enclosed spaces). They will be trained to recognize that the smoke vented from batteries during a fire could be combustible and should be allowed to ventilate before it is safe to approach. Trainees will be instructed on how to interpret system state information provided by the operations designee to perform on-site risk assessment. This information will include system hazards such as 1) what percentage of the cells in the system may have vented, 2) is the ventilation system working as expected, 3) what voltages are present in the system, 4) what the temperature trending history is internally, and 5) what actions have been taken by the automated systems (e.g. fire suppression). Guidance will be provided on how a visual inspection may provide sufficient information to assess the hazard. Finally, best practices will be provided on determining safe entry, methods for limiting the spread of a battery fire, identifying when the best approach is to not put out the fire (letting hazardous stored energy be dissipated safely), and determining when it is safe to leave an incident site.

[2] There should be at most one impedance-based ground fault detection device connected to each dc circuit, because of their potential to interfere with each other. Note that ground faults can often occur intermittently or slowly as insolation wares down over time. While a hard ground-fault should trigger disconnection and segmentation of a battery string, ground fault management is generally a part of regular maintenance because warnings can be issued well before a short circuit hazard is present.

3. HAZARD ANALYSIS IN FLOW BATTERY POWER PLANTS

Flow battery technologies are a becoming a viable alternative to lithium-based energy storage systems. The two most widely used flow battery chemistries are vanadium-redox, and zinc-bromide [50]. These technologies do not pose the same risk of fire or explosion as lithium-ion-based systems. However, they possess their own unique hazards that can make them difficult to engineer. While this report focuses on lithium-ion batteries, this section will provide a brief assessment of the hazards in flow battery systems. Our goal is to prepare an overview of the hazards that could lead to losses and injuries from electrolyte leaks in flow battery energy storage.

3.1. Hazardous energy classification

Flow batteries have two electrolytes- catholyte for the positive electrode (cathode) and anolyte (anode) for the negative electrode. The terms cathode and anode correspond to reduction and oxidation occurring at positive and negative terminals during discharge. Flow battery electrolytes can be hazardous in several ways including acidity and toxicity. Acidity is measured on the ph scale. Flow battery electrolyte is not especially acidic when compared to lead-acid battery electrolyte (close to ph = 0). If human skin is exposed to electrolyte, it may cause rashes or chemical burns if not treated quickly. Similarly, eye contact may result in irritation, lacrimation, pain, redness, corneal burns, and possible permanent, partial, or complete blindness if not treated quickly. The toxicity of the electrolyte has additional effects if ingested, inhaled, or released to the environment. Large pools from electrolyte spills can generate localized gas clouds that can be hazardous to human health. In an analysis of a hypothetical 500-gallon spill from a specific vanadium redox flow battery, with reasonable assumptions about hydrochloric acid (HCl) concentration in solution, spill volume, ground absorption, and local weather conditions, HCl concentrations in the air could reach potentially lethal exposure levels, after 60 minutes, at a range of 28m from the edge of the spill (using acute exposure guideline levels (AEGL)). Note that vanadium redox electrolyte can also contain sulfuric acid. As high temperatures can reduce vapor pressures significantly, a coincident fire can exasperate the toxicity hazard, however flow battery electrolytes are generally not flammable. While these specific figures do not apply across all technologies, the hazard from chemical off-gassing of large spills should be considered in the design, siting, installation, and emergency response procedures.

When the positive and negative charged electrolytes mix at a high state-of-charge, significant heat is generated, with violent release of toxic and/or flammable gases. For a vanadium flow battery, hydrogen and oxygen may be released, for a mixed acid vanadium flow battery, chlorine may also be released. Hence it is critical that the electrolytes that are stored in separate tanks, do not mix. This requires secondary containment for each tank. The secondary containment volume must be sufficiently large to accommodate the electrolyte volume contained in the tank. The electrolyte captured in the secondary containment may not be reused before treatment. Proper procedure for treating this spilled electrolyte before reuse has yet to be standardized and may lead to a delay in restoring system functionality.

The ecological impact of a large spill should also be considered. The material safety data sheet (MSDS) from a large zinc bromide flow battery manufacturer describes that major components of their electrolyte "are considered to be very harmful to aquatic life" [51]. So, proximity to nearby water sources or aquifers should be taken into consideration in siting.

3.2. Hazardous energy controls

This section discusses several common controls for the hazards introduced above.

3.2.1. Electrolyte tank design

The electrolyte tank material needs to be compatible with the electrolyte. During selection of material several factors come into play – cost, ease of manufacturability, economies of scale, compatibility, and critical design considerations. Compatibility and critical design considerations must be the top priority, after which the other factors may be considered. An example of a critical design consideration is stress analysis for the tank. Rounded corners have less stress compared to sharp corners, as an example.

Ensure stack materials (including gaskets) are compatible with the electrolyte. Ensure gasket thickness and torque applied is appropriate. Ensure pipe material is compatible with the electrolyte. Ensure fittings are compatible with the electrolyte. Ensure ease of assembly and disassembly to allow ease of maintenance. Perform stress analysis especially at corners – rounded corners are better at containing pressure because they distribute material stresses more evenly.

3.2.2. Containment and Leak Detection

The current draft of IEEE P1578 Draft Recommended Practice for Stationary Battery Electrolyte Spill Containment and Management has an Annex B which provides model code language for battery electrolyte spill management, containment, and absorption and/or neutralization [52]. Their recommendation for spill control reads as follows:

> "The battery room or area shall be provided with an approved method to manage an electrolyte spill and prevent it from spreading to areas where it could pose a hazard to the facility, equipment, or personnel. The volume to be managed shall be 1% of the total in all of the battery containers, or the amount of free-flowing liquid electrolyte in a single container, whichever is greater." [52]

While secondary containment helps with the containment of anolyte or catholyte present in each tank, there needs to be a tertiary containment to capture any leaks from segments of piping carrying electrolyte during operation. With proper leak detection systems, the leak can be detected within a few seconds, and the system (or that segment) can be stopped to allow maintenance and repair. Thus, the tertiary containment needs to be designed such that it can accommodate leakage at maximum flow for a sufficient duration until the pumps are stopped. Secondary and tertiary containment should be shielded from fire sprinkler system discharge to avoid filling it, thus rendering it ineffective, during a fire. Electrolyte can leak through gaskets to the surface of stacks and present electrocution hazards. This can happen when the operator touches spilled electrolyte simultaneously at two locations that are significantly different in voltage. By following proper procedures, this hazard can be mitigated or eliminated. Other than visual inspection, leak detection with stacks may be implemented by observing an inconsistent electrical performance of these stacks.

Once a tank leak is detected, that portion of the system is shut down for repair. This involves inspection of the damaged tank, followed by either replacement or repair. The tank is drained up to the level where the leak is present, and repairs are attempted in situ. In a case where a tank needs to be replaced, the entire tank is drained of electrolyte, followed by tank replacement. Preferably, there is a replacement tank on site, so the electrolyte can be transferred directly to the

replacement tank. If a replacement tank is immediately unavailable, proper procedures must be developed for electrolyte storage until a replacement tank arrives. The procedure could be as simple as waiting for the replacement tank to arrive, and then pumping the remaining electrolyte from the damaged tank to the replacement tank. For the electrolyte retained in secondary containment, proper procedures must be followed to ensure this electrolyte is treated properly before being used.

Once a pipe leak is detected, flow in that section (and the corresponding section for the opposite polarity) is stopped for maintenance repair. Stack leakage detection is followed by disconnecting the stack from the rest of the system. For strings with multiple stacks in series, this may require power flow to be stopped through the entire string. For stacks that are parallel connected, this stack may be isolated (electrically and fluid flow) for maintenance repair. Assuming each cell within a stack is easily replaceable (such as a unitized membrane electrode assembly design common in proton exchange membrane (PEM) fuel cells), this repair may be quite easy. In systems without modular cell design, the stack must be disassembled to reach the offending cell, with suitable gasket replacement and retorquing.

3.2.3. Emergency Response Actions

Hazmat trained personnel, often in the fire department, can respond to spills of hazardous materials such as battery electrolyte. Personal protective equipment is critical to preventing exposure in this scenario both for skin contact and for inhalation of toxic off-gas. Chemical safety gloves and a positive pressure breathing apparatus are critical components of any chemical spill response kit. IEEE P1578 lists the following model regulations for absorption and/or neutralization:

> "An approved method and materials shall be provided in sufficient quantity to absorb and neutralize, to a pH between 5.0 and 9.0, all of the electrolyte in the largest battery container in each battery system. Both active and passive neutralization methods shall be permitted. Absorption and neutralization materials shall be accessible within 10 m (33 ft) of the battery system." [52]

Procedures should include warning/evacuating people who are located near or downwind of the spill.

4. CONCLUSIONS

This work provides guidance for the energy storage industry in its efforts to design, procure, and operate safe and reliable lithium-ion based battery energy storage systems. Using system's theoretic process analysis (STPA), we are able to develop "design objectives" for system safety. The design objectives, in all or any subset, can be used by utilities as "design requirements" in storage request for proposals (RFPs) and utilities can use the design requirements for evaluating storage proposals on system safety. The design objectives enable clear communication between utilities and vendors on safety-related design considerations. While the design objectives presented here apply only to preventing fire and explosions in lithium-ion battery systems, the principles of the analysis apply broadly. By organizing a complex system to effectively enforce safety constraints we are able to prevent hazardous system states, and therefor prevent accidents. This report also includes broad overviews of the hazards in flow-battery technologies, which are viable alternatives to lithium-ion based systems.

We realize that the design objectives for safety of lithium-ion battery systems as defined here may possibly be a future state. It may be the case at first that no vendor proposals meet the design objectives for safety or those that do are prohibitively expensive. Our intent is that even in these scenarios, the design objectives help the system owners/operators to identify design deficiencies and associated risks more clearly and to take any necessary risk management and mitigation steps. We also anticipate that the design objectives will draw attention in the energy storage industry to the design deficiencies in the current market offerings through the following three mechanisms. First, if the market exists for systems that meet these requirements, competitive integrators will optimize their designs, bringing down costs and increasing the number of options available. Second, as these design objectives have significant overlap with the requirements in New York City and other localities, industry design requirements will move to catch up with the industry thought leaders. Third, as utilities across the country outlay procurement plans with regulators and shareholders, they can use the design objectives such as these to justify cost estimates for meeting procurement targets/goals. Together, these mechanisms have the potential to, over time, push the market to provide a range of supplier options to utilities, such that they can meet their procurement targets.

The high-level results of this analysis provide understanding on the hazards of battery energy storage systems and design objectives for system safety. This communication will help educate the U.S. energy storage industry and facilitate improved system design, procurement and operations of energy storage systems. As the electric grid evolves with a critical role for energy storage systems, the design objectives for system safety also serve to strengthen and mature the market for energy storage in the U.S. and thereby support the national interests of energy independence, crucial infrastructure resilience, and reduced greenhouse gas emissions.

REFERENCES

[1] N. Leveson and J. Thomas, "STPA Handbook," 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[2] N. Leveson, *Engineering a Safer World: System's Theory Applied to Safety*. Cambridge, MA: MIT Press, 2012.

[3] P. M. Senge, *The fifth discipline: The art & practice of the learning organization*. New York, NY: Doubleday, 1990.

[4] D. Rosewater and A. Williums, "Analyzing system safety in lithium-ion grid energy storage," *J. Power Sources,* vol. 300, pp. 460-471, 2015. [Online]. Available: https://doi.org/10.1016/j.jpowsour.2015.09.068.

[5] T. Reddy and D. Linden, *Linden's Handbook of Batteries*, forth ed. McGraw Hill, 2011.

[6] Z. Zhang, "The main cause of li-ion safety and internal shorts," presented at the Battery Safety Conference, Washington DC, 2014.

[7] D. H. Doughty and C. C. Crafts, "FreedomCAR Electrical Energy Storage System Abuse Test Manual for Electric and Hybrid Electric Vehicle Applications," SAND2005-3123, 2005.

[8] C. F. Lopeza, J. A. Jeevarajanb, and P. P. Mukherjeea, "Characterization of Lithium-Ion Battery Thermal Abuse Behavior Using Experimental and Computational Analysis," *J. Electrochem. Soc.,* vol. 162, no. 10, pp. A2163-A2173 2015, doi: 10.1149/2.0751510jes

[9] *IEC62133 Secondary Cells and Batteries Containing Alkaline or Other Non- Acid Electrolytes e Safety Requirements for Portable Sealed Secondary Cells, and for Batteries Made From Them, for Use in Portable Applications*, 2017.

[10] *IEC62281 Safety of Primary and Secondary Lithium Cells and Batteries During Transport*, 2019.

[11] *UL 2054 Standard for Household and Commercial Batteries*, 2004.

[12] *UL 1642 Standard for Lithium Batteries*, 2012.

[13] *United Nations Recommendations on the Transport of Dangerous Goods, Manual of Tests and Criteria: 38.3 Lithium Metal and Lithium Ion Batteries*, 2016.

[14] *ANSI C18.3M, Part 2-2011 American National Standard for Portable Lithium Primary Cells and Batteries Safety Standard.*, 2011.

[15] *SAE J2464: Electric and Hybrid Vehicle Propulsion Battery System Safety Standard for Lithium-based Rechargeable Cells*, 2011.

[16] *IEEE 1625-2008 - IEEE Standard for Rechargeable Batteries for Multi-Cell Mobile Computing Devices*, 2008.

[17] *IEEE 1725-2011 - IEEE Standard for Rechargeable Batteries for Cellular Telephones*, 2011.

[18] L. Lu, X. Han, J. Li, J. Hua, and M. Ouyang, "A review on the key issues for lithium-ion battery management in electric vehicles," *J. Power Sources* vol. 226, pp. 272-288, 2013.

[19] J. R. Thomas Long and A. M. Misera, "Sprinkler Protection Guidance for Lithium-Ion Based Energy Storage Systems," Fire Protection Research Foundation, 2019. [Online]. Available: https://www.nfpa.org/News-and-Research/Data-research-and-tools/Suppression/Sprinkler-Protection-Guidance-for-Lithium-Ion-Based-Energy-Storage-Systems

[20] J. Jeevarajan, "Can cell-to-cell thermal runaway propagation in lithium-ion modules be prevented," presented at the Battery Safety Conference, Washington DC, 2014.

[21] J. McLaughlin, "Risks of lithium batteries in air transportation," presented at the Battery Safety Conference, Washington DC, 2014.

[22] J. Lamb, C. Orendorff, L. Steele, and S. Spangler, "Failure propagation in multi-cell lithium ion batteries," *J. Power Sources,* vol. 283, pp. 517-523, 2015.

[23] K. Marr, V. Somadepalli, and Q. Horn, "Explosion hazards due to failure lithium-ion batteries," presented at the Global Congress on Process Safety, 2013.
[24] *NFPA 69: Standard on Explosion Prevention Systems*, 2019.
[25] *NFPA 68: Standard on Explosion Protection by Deflagration Venting*, 2018.
[26] D. Rosewater and A. Williams, "Analyzing system safety in lithium-ion grid energy storage," *J. Power Sources,* vol. 300, pp. 460-461, 2015.
[27] C. Orendorff, J. Lamb, and L. Steele, "Recommended Practices for Abuse Testing Rechargeable Energy Storage Systems (RESSs)," Sandia National Laboratories, 2017.
[28] *UL 9540A, Test Method for Evaluating Thermal Runaway Fire Propagation in Battery Energy Storage Systems*, 2019.
[29] *UL 1973 Standard for Batteries for Use in Stationary, Vehicle Auxiliary Power and Light Electric Rail (LER) Applications.*
[30] *IEC 62619:2017 Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for secondary lithium cells and batteries, for use in industrial applications.*
[31] *NFPA 855 Standard for the Installation of Stationary Energy Storage Systems.*
[32] *NASA JSC 20793 Rev D, Crewed Space Vehicle Battery Safety Requirements*, 2017.
[33] E. Darcy, J. Darst, W. Walker, D. Finegan, and P. Shearing, "Design Guidelines for Safe, High Performing Li-ion Batteries with 18650 cells," presented at the JRC Exploratory Research Workshop, Petten, Netherlands, 2018.
[34] J. B. Straubel, D. Lyons, E. Berdichevsky, S. Kohn, and R. Teixeira, "System and method for inhibiting the propagation of an exothermic event," USA, 2007.
[35] D. A. Corrigan and A. Masias, "Batteries for Electric and Hybrid Vehicles," in *Linden's Handbook of Batteries*. New York: McGraw Hill, 2011, pp. 29.15-29.21.
[36] S. Wilke, B. Schweitzer, S. Khateeb, and S. Al-Hallaj, "Preventing thermal runaway propagation in lithium ion battery packs using a phase change composite material: An experimental study," *J. Power Sources,* vol. 340, pp. 51-59, 2017.
[37] B. Barnett, C. H. McCoy, D. Ofer, and S. Sriramulu, "Successful Early Detection of Incipient Internal Short Circuits in Li-ion Batteries and Prevention of Thermal Runaway," presented at the ECS Meeting 2016.
[38] C. T. Love, M. B. V. Virji, R. E. Rocheleau, and K. E. Swider-Lyons, "State-of-health monitoring of 18650 4S packs with a single-point impedance diagnostic," *J. Power Sources,* vol. 266, pp. 512-519, 2014.
[39] C. Love and K. Swider-Lyons, "Impedance Diagnostic for Overcharged Lithium-Ion Batteries," *Electrochemical and Solid-State Letters,* vol. 15, no. 4, pp. A53-A56, 2012.
[40] R. Srinivasan, B. G. Carkhuff, M. H. Butler, and A. C. Baisden, "Instantaneous measurement of the internal temperature in lithium-ion rechargeable cells," *Electrochimica Acta,* vol. 56, no. 17, pp. 6198-6204, 2011.
[41] R. Srinivasan, A. C. Baisden, B. G. Carkhuff, and M. H. Butler, "The five modes of heat generation in a Li-ion cell under discharge," *J. Power Sources,* vol. 262, no. 0, pp. 93-103, 2014.
[42] R. Srinivasan and B. G. Carkhuff, "Empirical analysis of contributing factors to heating in lithium-ion cells: Anode entropy versus internal resistance," *J. Power Sources,* vol. 241, no. 0, pp. 560-566, 2013.
[43] J. P. Christophersen, D. F. Glenn, C. G. Motloch, R. B. Wright, C. D. Ho, and V. S. Battaglia, "Electrochemical impedance spectroscopy testing on the advanced technology development program lithium-ion cells," *IEEE Trans. Veh. Technol.,* vol. 56, no. 3, pp. 1851-1855, 2002.

[44] J. P. Christophersen, W. H. Morrison, J. L. Morrison, C. G. Motloch, and D. M. Rose, "Crosstalk compensation for a rapid, higher-resolution impedance spectrum measurement," presented at the IEEE Aerospace Conference, 2012.
[45] J. L. Morrison, J. P. Christophersen, and W. H. Morrison, "Universal auto-calibration for a rapid battery impedance spectrum measurement device," presented at the IEEE Aerospace Conference, 2014.
[46] B. Gully, H. Helgesen, J. E. Skogtvedt, and D. Kostopoulos, "Technical ReferenceforLi-ion Battery Explosion Risk and Fire Suppression," DNV-GL, 2019.
[47] *1635-2018 - IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications*.
[48] K. Marr, V. Somadepalli, and Q. Horn, "Explosion Hazards Due to Failure Lithium-Ion Batteries," ed, 2013.
[49] NFPA. "Energy Storage & Solar Systems: Safety Training Program." National Fire Protection Association. https://www.nfpa.org/News-and-Research/Resources/Emergency-Responders/High-risk-hazards/Energy-Storage-Systems (accessed 02/20/2020.
[50] U. S. DOE. "Global Energy Storage Database." https://www.energystorageexchange.org/ (accessed 12/10/2019.
[51] "Redflow Installation and Operation Manual ZBM2 (3kW/10kWh) " Redflow Limited, Brisbane QLD, Australia 2019. [Online]. Available: https://redflow.com/wp-content/uploads/2019/07/ZBM2-Installation-and-Operation-Manual-CE-V4.0.pdf
[52] *IEEE P1578 Draft Recommended Practice for Stationary Battery Electrolyte Spill Containment and Management*, 2019.

APPENDIX A. ANSWERS TO SPECIFIC QUESTIONS

Answers provided in this appendix map the results of the analysis presented in the body of this document onto a set of more general questions about safety, risk, and lithium-ion battery systems. We have chosen to write in somewhat less formal language and express opinions more freely as these answers are intended for consumption by personnel with a broad range of technical backgrounds. This is done primarily for readability and summary so please refer to the body of this report for a more complete picture of these topics. Please note that any views or opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Q1: Cell failure via thermal runaway (or other similar failure modes): 1) what can be done to reduce the frequency as much as possible; and 2) what can be done to minimize the consequences of thermal runaway when it does occur?

1) The answer to this question comes in two parts, first is to answer the direct question about the manufacturing and testing methods used to avoid high energy failures of individual cells and second is the answer to the implied question about if reducing this frequency can be effective at reducing the system level risk of installing lithium-ion based energy storage systems. To reduce the frequency of a thermal runaway event, battery manufacturers spend a large amount of time and money to make uniform cells and prevent particle contamination. They also send regular batches to testing laboratories and have third party inspectors brought in to make sure that manufacturing standards are not slackened over time. This is to say that there is not much that a utility can do to verify or assess these standards other than ensuring that the manufacturer is large, has a good reputation, is certified to a quality control standard such as ISO 9001, and that any purchased cells are not counterfeit. As designs change over time and use environments can differ from application to application, the frequency of cell failures ends up having a large uncertainty. This could mean it is much higher or much lower than expected. Because of this uncertainty, efforts to reduce the frequency of failures tend to be more expensive, and less effective than efforts in system design to minimize the consequence of thermal runaway. Instead of focusing on the frequency of failures, it may be better to focus cell analysis efforts on the consistency or predictability of failure mechanisms. If the integrator knows exactly how much heat, at what rate, is produced during the worst-case thermal runaway, they can engineer the system to handle it gracefully (design objectives 2.1-2.4).
2) Much of this report has been an attempt to answer this question. The system can be designed to mitigate the impact of thermal runaway by preventing propagation of thermal runaway (design objectives 2.1-2.4), by preventing the buildup of combustible gases (design objectives 3.1, and 3.2), by ensuring that firefighters are informed of the hazards and able to respond safely (design objectives 1.1, 1.2, and 1.3), by designing the system to be recoverable after thermal runaway events (design objectives 4.1-4.3), and by ensuring system data can be trusted (design objective 5.1).

Q2: To what extent can the choice of lithium-ion chemistry or supplier reduce the incidence of cell failure via thermal runaway?

As discussed in Section 2.1 different lithium-ion chemistries can have very different potential energies released during thermal runaway. However, propagation of thermal runaway is a complex phenomenon. For example, tightly packed and insolated lithium-iron-phosphate cells, which have relatively low heat release rates, still have the potential to propagate thermal runaway if the heat dissipation is insufficient to keep temperatures of the of adjacent cells within a safe range. So yes, the choice of lithium-ion chemistry can have an impact on a safe system design, but it is only one factor. As for the choice of battery supplier, we discuss in our answer to Q1 how expensive and difficult it can be to ensure uniform battery manufacturing critical to the consistency of cell failure mechanics. Company size is not a direct proxy for manufacturing quality. However, a large number of cells manufactured per year can be a prerequisite for the statistical sample size needed to estimate vary rare cell failure rates precisely.

Q3: How much, if at all, can balance of system/system integration reduce the incidence of thermal runaway?

a. In particular, what is the potential role of cell/rack sensors, real-time monitoring, and predictive analytics in avoiding thermal runaway? Fire suppression design?

b. this could be a "big data" opportunity that has both system design and organizational capability implications.

a) Much of this report has been an attempt to answer this question. The system can be designed to mitigate the impact of thermal runaway by preventing propagation (design objectives 2.1-2.4), by preventing the buildup of combustible gases (design objectives 3.1, and 3.2), by ensuring that firefighters are informed of the hazards and able to respond safely (design objectives 1.1, 1.2, and 1.3), by designing the system to be recoverable after thermal runaway events (design objectives 4.1-4.3), and by ensuring system data can be trusted (design objective 5.1).

Fire suppression has a complex impact on the prevention of propagation, as well as the buildup of combustive gases (see loss Scenario 4 in Section 0). Elimination of open flame can reduce heat transfer and slow or even halt propagation. However, the open flam is consuming flammable gases and hence extinguishing it could generate the conditions for an eventual explosion. Rather than thinking of fire suppression as a way of mitigating thermal runaway, instead it can be viewed as a method of preventing an externally lit fire from spreading to the battery racks (e.g. an electrical fire in the power conversion system). While it can be important in a system design it is also critical to engineer the system to prevent propagation of thermal runaway (design objectives 2.1-2.4).

b) This is an area of fast-moving research, and the methods used in other "big data" systems may indeed be reapplied to this problem space. However, we caution you that the efficacy of analytical methods is quite often limited by the precision of data collection. Many of the methods that are being proposed to assess the health or safety of batteries in real-time rely on expensive, laboratory grade, sensors that may not be sailable to grid sized systems. Alternatively, some designs rely on many more, relatively cheap, temperature sensors to ensure that self-heating is detected quickly, and the system can respond to minimize the impact. As the research on optimal sensor density, placement, and accuracy is ongoing we cannot give concrete guidance.

Q4: What are the scale, containment, venting and fire suppression options for mitigating thermal runaway consequences from a health and safety perspective and from an equipment damage perspective?

In our analysis, losses L1 and L2 refer to equipment damage (see Section 2.2.1). The design objectives related to those losses are meant to address containment, venting and fire suppression options and design. Similarly, L3 refers to the health and safety perspective. Much of this report has been an attempt to answer these questions. The system can be designed to mitigate the impact of thermal runaway by preventing propagation (design objectives 2.1-2.4), by preventing the buildup of combustible gases (design objectives 3.1, and 3.2), by ensuring that firefighters are informed of the hazards and able to respond safely (design objectives 1.1, 1.2, and 1.3), by designing the system to be recoverable after thermal runaway events (design objectives 4.1-4.3), and by ensuring system data can be trusted (design objective 5.1).

The scale of the installation was not directly considered in our analysis. However, scale can have a large impact on the cost of implementing the design objectives above, as well as on the risk associated with their efficacy. To consider this question we will analyze how the propagation prevention and explosion prevention design objectives would be different between two otherwise identical systems configured in 1) a single large building with multiple battery systems, or 2) multiple smaller buildings, each with one battery system. We will then extrapolate this to the decision of system scale in general.

- Considering the firefighter interaction design objectives: the information supplied would need to be the same, hence design objectives 1.1 and 1.2 would not change between the two scales. The actions that firefighters could take safely, would be very different. In modular buildings the potentially hazardous environment would be limited to a single building. They would be able to limit the spread of a fire by applying water to nearby buildings, or simply let the fire run its course. In a single large structure, firefighters may not be able to safely enter the building, and hence may not be able to act to limit the spread of a fire from one battery system to the next. This would imply an increased reliance on passive design and automated systems.
- Considering the propagation prevention design objectives: design objectives 2.1/2.2 (cell-to-cell) and 2.3/2.4 (module-to-module) would not be impacted by the scale of the enclosure. Active propagation prevention designs in objective 2.1-2.4 Active might be affected depending on their acting mechanism. Targeted foam or coolant deployment systems would require a different design, but the design objective would not be affected. A large building may require an additional design objective for the prevention of fire propagation between battery systems. This could be accomplished by a large air gap or a firewall between systems.
- Considering the explosion prevention design objectives: this is primarily where the design impacts would be seen. In a large warehouse, the ratio of internal volume to potential ventilation rate could potentially be much higher than for modular buildings, meaning it would take a larger total number and percentage of the cells to vent to reach the LFL. However, the potential severity of an explosion would also be much larger. Given the increased magnitude of a potential event, deflagration ventilation would be more critical, so a backup ventilation system may be needed. Combining the air volume of many smaller structures into one large structure has the potential to reduce the likelihood of an explosion

while increasing is severity. Impact on overall risk would depend on the specifics of the design.

- Considering the operational recovery design objectives: a fire in one smaller building would not require an emergency shutdown in nearby system, nor would they require a post mortem analysis to bring back to full operation. A large building with multiple batteries may need such action, which would increase the cost of false positives or small events. This may require a design objective for a staged emergency shutdown where other batteries in the system continue to operation unless there is enough reason to perform emergency action. Either approach could increase the risk of long downtimes.

The bottom line is that the design objectives could help to mitigate the impact of a battery fire regardless of system scale. Scale would impact how the system archives the design objectives. In general, some design objectives would be easier to implement (cheaper and lower risk), while others would be more difficult (more expensive and higher risk). Specifically, with larger scale the design objectives for firefighter interaction and operational recovery would be more difficult, those for explosion prevention would be easier, and those for propagation and data integrity would not change.

Q5: Considerations for siting of the facility, neighborhood elements / risks, chosen technology (lithium ion or other), system size (number of racks per system), containerized vs. non-containerized, vented or non-vented, fire suppression, personnel and first responder training

In general, as we understand currently, the smoke from a lithium-ion battery fire is as toxic to human health as a fire in a similar mass of common plastics. However, sometimes the safest/best firefighter response to a propagating battery fire is to simply let the fire consume the active material, thereby dissipating the stored energy, while protecting nearby structures. This may mean that a battery fire will produce smoke for a longer duration than fires in plastics. As toxic impact to human health is based on both severity and duration of exposure a battery fire in a neighborhood could have a greater impact than a fire in a comparable mass of plastics. Because of this, it is recommended that siting policy consider the smoke produced during conflagration, whether generated by thermal runaway or external fire, and the population potentially exposed to the smoke. This consideration impacts duel-occupancy structures, locations where evacuation options are limited, and a location's proximity to vulnerable populations such as schools or elderly care facilities.

The risk that a battery fire spreads to nearby structures should also be considered. Rules structuring the placement of large, oil-filled transformers can offer reasonable guidance on how to structure the siting/offset requirements that could be applied to battery systems. These rules should be based on the total volume of fuel and how much heat it produces during a fire. For a given battery type these data can be found in the abuse test data for the cell, multiplied by the number of cells per enclosure. Fire barriers can also be considered (similar to oil-filled transformer siting requirements).

The risk of an explosion should also be considered in the design as well as location of the system (see design objective 3.3 in Section 2.3.3).

APPENDIX B. HUMAN CONTROLLER DESCRIPTIONS

Public Utility Commission

Safety Responsibilities: Utility oversight, collect information from public
Mental Models:

- Public safety (and the public's perception of safety)
- System operating constraints and cost
- Importance/value of energy storage

Executive Management

Safety Responsibilities: Corporate policy, setting expectations and goals
Mental Models:

- The safety review process for BESS procurement
- Financial, legal, and safety risk

Procurement / O&M Operations and Maintenance

Safety Responsibilities: Establishing system requirements, compliance of BESS with applicable codes and standards, safely operating the BESS, Monitoring BESS for faults and warnings, perform regular maintenance, interface with first responders in case of a incident
Mental Models:

- Battery failure modes and hazards
- Codes and standards applicable to BESS
- First responder knowledge and behavior
- Current state of the BESS

Integrator

Safety Responsibilities: BESS design, installation, commissioning
Mental Models:

- Safe operating limits for battery cells and modules
- Battery failure modes and hazards
- First responder knowledge and behavior

Battery Supplier

Safety Responsibilities: Cell design, Module design, manufacturing, type testing, and factory acceptance testing
Mental Models:

- Safe operating limits for battery cells and modules
- Battery failure modes and hazards
- First responder knowledge and behavior

Fire Marshal

Safety Responsibilities: Authority having jurisdiction permitting/approval
Mental Models:

- Codes and standards applicable to BESS
- Battery failure modes and hazards
- First responder knowledge and behavior

Firefighters

Safety Responsibilities: avoid hazards, protect life/health, protect property, execute procedures
Mental Models:

- Battery failure modes and hazards
- Current state of the BESS

APPENDIX C. UNSAFE CONTROL ACTION DESCRIPTIONS

This section lists every identified unsafe control action (UCA) found in step three of STPA: identify unsafe control actions. Each identifies its own location, and the hazard(s) it could cause or contribute to. They are grouped by color as shown below.

BESS Procurement	BESS Design, installation, and commissioning	Firefighter Training and Response	System Response to Spontaneous Cell Fire	Post incident response and recovery

PUC Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Policy	UCA-C4: Not setting policy for procurement could prevent the widescale deployment of energy storage technologies [H6]	UCA-E4: Setting procurement targets for energy storage technologies applies pressure to utilities to deploy battery storage systems faster than they otherwise would. If this pressure is not accompanied with additional financial support this could stretch resources thin and lead to a hazard [H1, H2]	N/A	N/A

Integrator Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
BESS design	N/A (not providing leads to no system)	UCA-E7: A BESS should be designed to prevent or suppress the propagation of thermal runaway. It should also be designed to prevent the build-up of combustive vent gasses. If it is not designed to do this, then it could lead to a hazard [H1, H2]	N/A	N/A
Proposal (response to RFP)	N/A (not providing leads to no system)	UCA-E8: The proposal should specify how the BESS design prevents the propagation of thermal runaway and the build-up of combustive gasses. If it does not specify this then the utility cannot review it. [H1, H2]	N/A	N/A

BESS installation and commissioning	N/A (not providing leads to no system)	UCA-E9: There are many sensors and control actions that are needed for the system controller to enforce safety constraints on the batteries and suppress the propagation of thermal runaway. Commissioning involves checking that each sensor and control action works as expected. If commissioning is incomplete then there may be sensors that are not provided the needed data or actuators that are ineffective. Either could lead to a hazard [H1, H2]	N/A	N/A
BESS emergency action plan	UCA-C10: The emergency action plan describes how the automated systems are designed to work with and around first responders in a variety of scenarios. Not providing an action plan means that there is uncertainty when responding to an incident that could lead to a hazard [H3, H4, H5]	UCA-D10: The emergency action plan describes how the automated systems are designed to work with and around first responders in a variety of scenarios. Providing a incomplete or inaccurate emergency action plan could lead to a hazard [H3, H4, H5]	N/A	N/A
Battery Supplier Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Cell design	N/A (not providing leads to no system)	UCA-E13: Cells should be designed to fail consistently within some known parameters, if not gracefully. A cell design that has large variations in heat release rate or vent gas volume would be difficult to integrate into a system and could lead to a hazard [H1]	N/A	N/A

Cell specifications	UCA-C14:The cell specifications include limits on voltage, current, and temperature. Not providing specification could lead to a hazard [H1]	UCA-E14: The cell specifications include limits on voltage, current, and temperature. Providing incorrect limits could lead to a hazard [H1]	N/A	N/A
Executive Management Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Policy (related to procurement of BESS)	N/A (not providing leads to no system)	UCA-D18: Policy dictates 1. the procurement review process, and 2. the utility's risk tolerance. If the review process is too quick, then a hazard may develop from the procured system [H1]. If the review process is too long, the utility may not meet its procurement targets [6]. the same applies for risk tolerance.	N/A	N/A
Procurement O&M Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Request for Proposals	N/A (not providing leads to no system)	UCA-D21: Writing a complete RFP requires some knowledge of battery energy storage technologies. Being able to interpret the proposals received requires even more. Selecting a vendor who has a design that insufficiently enforces safety constraints could lead to a hazard [H1, H2]	N/A	N/A
Permitting (code compliance)	N/A (not providing leads to no system)	UCA-D22: codes and standards offer a set of requirements that if met protect the system from many kinds of hazards. Not complying with relevant codes and standards could lead to a hazard [H1, H2]	UCA-E22: Permitting delay could lead to a lack of the services that energy storage can provide [H6]	N/A
Operations	UCA-C23: Not operating the system could lead to a lack of the services that energy storage can provide [H6]	Not hazardous	UCA-E23: Operating the system before commissioning could lead to a hazard [H1]	N/A

Maintenance	UCA-C24: Not conducting regularly scheduled Maintenance could lead to a hazard [H1]	UCA-D24: Conducting Maintenance incorrectly could lead to a hazard [H1]	Delay is the same as not providing	N/A
Provide information to firefighters	UCA-C25: Firefighters are not expected to be experts in energy storage technologies and their hazards. Knowledge of risks is primarily conveyed through training but can be supplemented by asking questions of the utility POC. [H3, H4, H5].	UCA-D25: Providing wrong information, or providing it in such a way as to make it difficult for a firefighter to generate a useful mental model of the hazards, could be counterproductive to protecting life and property. [H3, H4, H5, H6].	Delay is the same as not providing	N/A

Fire Martial Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Permit Approval/Rejection	N/A (not providing leads to no system)	UCA-D28: A city Fire Martial is not expected to be an expert in energy storage technologies. They are knowledgeable about the hazards and environments that firefighters are trained for. Approving a system installation that firefighters do not have adequate training for could cause a hazard when firefighters respond to an incident in the system. [H3, H4, H5].	UCA-E28: Permitting delay could lead to a lack of the services that energy storage can provide [H6]	N/A

Firefighter Policy and Training	UCA-C29: While firefighter training will not make them experts in energy storage technologies, the hazards of battery systems are not unique. Hence much of the training around other hazardous environments can be applied to battery storage systems. Not providing training in chemical fires, hydrogen rich environments, and electrical fires, could lead to them being under-prepared for battery fires. Not providing training to recognize that a battery fire could contain chemical, explosive and electrical hazards could cause them to exposed to those hazards unknowingly [H3, H4, H5]	UCA-D29: Inaccuracies or misrepresentations in training could lead to misinterpretation of hazards when responding to a battery fire [H3, H4, H5].	Delay is the same as not providing	UCA-F29: A retraining schedule must be planed for keeping knowledge current with the fast pace of technological change. New safety systems and cell chemistries may render training material out of date. [H3, H4, H5].
Firefighters Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Physical Actions	UCA-C32: Firefighters are expected to take action to protect life and property. Physical actions, such as entering the system, may be needed to a. protect life [H3, H4, H5], or property [H6].	UCA-D32: Physical actions, such as entering the system, may expose firefighters to hazardous conditions [H3, H4, H5].	UCA-E32: If life is in danger, then late action is the same as inaction [H3, H4, H5]. However, early action can be dangerous to the firefighters [H3, H4, H5].	N/A
Questions to utility POC	UCA-C33: Firefighters are not expected to be experts in energy storage technologies and their hazards. Knowledge of risks is primarily conveyed through training but can be supplemented by asking questions of the utility POC. [H3, H4, H5].	Not hazardous	UCA-E33: Asking for information should be done before taking action [H3, H4, H5].	N/A
System Controller Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Power Setpoint	UCA-C36: Needed for operation [H6]	UCA-D36: a power setpoint too high can cause over current [H1], or charging at too high a rate above a safe temperature [H1]	Not hazardous	UCA-F36: Depending on the control mechanism for the inverter a stuck power setpoint could cause overcharge, or over discharge [H1],

Temperature Setpoint	UCA-C37: Needed for operation [H6]	UCA-D37: Environment temperature can be unsafe for the cells if it is set too high or too low [H1]	Not hazardous	Not hazardous
Activate Fire Suppression	UCA-C38: Not activating fire suppression could lead to thermal runaway propagation [H1]	UCA-D38: If people are present, then fire suppression could be hazardous to them [H5]	Delay is the same as not providing	Stopped too soon is the same as not providing
External communication and data	UCA-C39: firefighters responding to an event need information about the current state of the system. Not providing it could lead them to misinterpret hazards [H3, H4, H5]	UCA-D39: Falsely indicating a safe environment would lead firefighters to misinterpret hazards [H3, H4, H5]	Delay is the same as not providing	Stopped too soon is the same as not providing
System shutdown	UCA-C40: If there is an active voltage hazard in the system, then disconnecting it from the grid could remove this hazard. Otherwise it could be hazardous to someone in the system [H4].	UCA-D40: Disconnecting the system controller, BMS, and all of the sensors from the grid may lead to a loss of data access that would make it difficult to know what the current state of the system is. If firefighters do not have access to this information then they may be exposed to a hazard [H3, H4, H5]. Loss of data also makes it difficult to recover from a incident.	Delay is the same as not providing, too early is the same as providing	UCA-F40: If power is restored while the voltage hazard is still present then people in the system could be exposed to it [H4].
HVAC Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Heating	UCA-C42: If one or more cells are cold, performance will be limited [H6]	UCA-D42: A HVAC system could impose unsafe temperatures on cells [H1]	Delay is the same as not providing	N/A
Cooling	UCA-C43: if one or more cells are overly hot, performance will be limited [H6] alternatively, cells could exceed safe temperatures which could lead to thermal runaway [H1]	UCA-D43: A HVAC system could impose unsafe temperatures on cells [H1]	Delay is the same as not providing	N/A
Ventilation	UCA-C44: if the rate of off-gas generation exceeds the rate of ventilation, gas may build up to combustive concentrations [H2]	UCA-D44: If it is hotter or colder than the safe operating temperature outside of the enclosure then excess ventilation could lead to early cell failure [H6]	Delay is the same as not providing	N/A

Fire Suppression Outputs	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Oxygen Starvation	UCA-C47: Not suppressing an open flam could lead to more rapid cell failure propagation [H1]	UCA-D47: If people are present, then this type of fire suppression could be hazardous to them [H5]	Delay is the same as not providing	UCA-F48: Insufficient suppression could be ineffectual
Emergency Cooling	UCA-C48: Removing heat from cells slows the rate of propagation, not providing it could be hazardous [H1]	UCA-D48: If people are present, then this type of fire suppression could be hazardous to them [H5]	Delay is the same as not providing	UCA-F48: Insufficient cooling could be ineffectual

PCS Outputs	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Voltage	UCA-C51: Needed for operation [H6]	UCA-D51: Overvoltage, or undervoltage are both hazardous [H1]	Not hazardous	UCA-F52: Applying voltage for too long leads to overcharge [H1] or over discharge [H6]
Current	UCA-C52: Needed for operation [H6]	UCA-D52: Overcurrent can be hazardous on both charge and discharge [H1]	Not hazardous	UCA-F52: Applying current for too long leads to overcharge [H1] or over discharge [H6]

BMS Outputs	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Battery voltage	UCA-C56: Not providing voltage measurements during either normal operation or an event makes it difficult for the system to respond appropriately. [H1, H2]	UCA-D56: If the voltage provided to the system controller is lower than the true voltage then the controller may fail to respond to a high voltage event. [H1, H2]	UCA-E56: to be useful data must be appropriately timestamped. A mistimed voltage measurement could look anti-causal in post mortem analysis.	Stuck measurements are the same as Providing causes a hazard
Battery current	UCA-C57: Not providing current measurements during either normal operation or an event makes it difficult for the system to respond appropriately. [H1, H2]	UCA-D57: If the current provided to the system controller is lower than the true current then the controller may fail to respond to a high current event. [H1, H2]	UCA-E57: to be useful data must be appropriately timestamped. A mistimed current measurement could look anti-causal in post mortem analysis.	Stuck measurements are the same as Providing causes a hazard
Battery temperature	UCA-C58: Not providing temperature measurements during either normal operation or an event makes it difficult for the system to respond appropriately. [H1, H2]	UCA-D58: If the temperature provided to the system controller is lower than the true temperature then the controller may fail to respond to a high temperature event. [H1, H2]	UCA-E58: to be useful data must be appropriately timestamped. A mistimed temperature measurement could look anti-causal in post mortem analysis.	Stuck measurements are the same as Providing causes a hazard

Battery protection contactor	UCA-C59: The protection contactor is designed to take a string off-line if it exceeds limits on voltage, current, or temperature. If it fails to operate under these conditions one or more cells could enter the self heating state. [H1, H2]	UCA-D59: Opening the contactor should not be hazardous if the contactor is rated for the maximum expected current of the battery string. Closing the contactor could increase arc-flash hazard in connected components such as the PCS. [H4]	Delay is the same as not providing	UCA-F59: If the battery protection contactor is stuck then the battery system will not be able to operate. This also can make stranded energy difficult or impossible to drain off, even in undamaged batteries [H6]
Ground fault detected	UCA-C60: A ground fault could apply a hazardous voltage to the rack, or floor of a battery enclosure. Not knowing about it could expose people to said voltage [H4]	UCA-D60: If the system response could be hazardous, then falsely triggering it could generate an unnecessary hazard. If this happens often (nuisance alarms), then the alarm may be ignored, leading to a hazard when the alarm is not triggered during a fire. [H4, H5,H6]	Delay is the same as not providing	N/A
Smoke Detector Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Smoke detected contactor	UCA-C63: The purpose of the smoke detector is to identify the presence of smoke and trigger a fire suppression system. Smoke is a good indicator that one or more cells are in the one of the two venting states. [H1, H2]	UCA-D63: If the system response could be hazardous, then falsely triggering it could generate an unnecessary hazard. If this happens often (nuisance alarms), then the alarm may be ignored, leading to a hazard when the alarm is not triggered during a fire. [H4, H5]	Delay is the same as not providing	N/A
E-Stop Outputs	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**

Emergency Stop Contactor	UCA-C66: The purpose of the E-Stop button is to make the BESS safe to enter or inspect. Whatever actions must be taken to do this can only occur if the system controller knows that the E-Stop has been pressed.	UCA-D66: If the system response could be hazardous, then falsely triggering it could generate an unnecessary hazard. If this happens often (nuisance alarms), then the alarm may be ignored, leading to a hazard when the alarm is not triggered during a fire. [H4, H5]	Delay is the same as not providing	N/A

Battery Outputs (Normal)	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Voltage	UCA-C69: Voltage measurement is critical to managing safety. Not providing it could lead to over discharge, or overcharge which could lead to thermal runaway. [H1]	UCA-D69: DC voltage can be hazardous to people and equipment. [H4]	UCA-E69: to be useful data must be appropriately timestamped. A mistimed voltage measurement could look anti-causal in post mortem analysis. [H6]	UCA-F69: Voltage data from inside the system could be useful to firefighters responding to an incident. If the voltage measurement is stopped too soon then it would not be available to them. [H5]
Current	UCA-C70: Current measurement is critical to managing safety. Not providing it could lead to over discharge, or overcharge which could lead to thermal runaway. [H1]	Not hazardous	UCA-E70: to be useful data must be appropriately timestamped. A mistimed current measurement could look anti-causal in post mortem analysis. [H6]	N/A
Temperature	UCA-C71: Temperature measurement is critical to managing safety. Not providing it could lead to abuse conditions that could cause thermal runaway. However, measuring every cell's temperature is not necessarily practical. Hence, temperature is often monitored as an envelope (max/min), rather than by individual cells. [H1]	Not hazardous	UCA-E71: to be useful data must be appropriately timestamped. A mistimed temperature measurement could look anti-causal in post mortem analysis. [H6]	UCA-F71: Temperature data from inside the system could be useful to firefighters responding to an incident. If the temperature measurement is stopped too soon then it would not be available to them. [H4]
Heat (external fire)	No Hazard	UCA-D72: A fire started in nearby electronics, or other flammable material, could cause multiple cells to enter self-heating simultaneously. This condition could overwhelm any designed propagation prevention	N/A	N/A

		and might cause a fire to spread [H1]		
Battery Outputs (Self-heating)	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Voltage	UCA-C74: An internal short circuit, which causes self heating, can be preceded by a precipitous drop in cell voltage. Not measuring voltage could miss this onset event and the system may not respond appropriately. [H1]	UCA-D74: DC voltage can be hazardous to people and equipment. [H4]	UCA-E74: to be useful data must be appropriately timestamped. A mistimed voltage measurement could look anti-causal in post mortem analysis. [H6]	UCA-F74: Voltage data from inside the system could be useful to firefighters responding to an incident. If the voltage measurement is stopped too soon then it would not be available to them. [H5]
Current	UCA-C75: Current measurement is critical to managing safety. Not providing it could lead to over discharge, or overcharge which could lead to thermal runaway. [H1]	UCA-D75: Current causes heat generation in the battery that could exasperate self-heating. However, reduced state-of-charge can greatly reduce the energy in thermal runaway.	UCA-E75: to be useful data must be appropriately timestamped. A mistimed current measurement could look anti-causal in post mortem analysis. [H6]	N/A
Temperature	UCA-C76: Detecting self heating can be difficult. Especially when temperature sensors are placed sporadically throughout a system. Any active response system depends on detecting self heating and hence if temperature measurement is critical for these designs [H1].	Not hazardous	UCA-E76: to be useful data must be appropriately timestamped. A mistimed temperature measurement could look anti-causal in post mortem analysis. [H6]	UCA-F76: Temperature data from inside the system could be useful to firefighters responding to an incident. If the temperature measurement is stopped too soon then it would not be available to them. [H4]

Battery Outputs (Venting (with open flame))	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Voltage	UCA-C79: Not providing voltage measurements during an event can make it difficult to determine what went wrong after the fact. [H6]	UCA-D79: DC voltage can be hazardous to people and equipment. [H4]	UCA-E79: to be useful data must be appropriately timestamped. A mistimed voltage measurement could look anti-causal in post mortem analysis. [H6]	UCA-F79: Voltage data from inside the system could be useful to firefighters responding to an incident. If the voltage measurement is stopped too soon then it would not be available to them. [H5]
Current	UCA-C80: Not providing current measurements during an event can make it difficult to determine what went wrong after the fact. [H6]	N/A if a battery is venting then it is most likely open circuit meaning current cannot pass through it.	UCA-E80: to be useful data must be appropriately timestamped. A mistimed current measurement could look anti-causal in post mortem analysis. [H6]	N/A

Temperature	UCA-C81: Not providing temperature measurements during an event makes it difficult for the system to respond appropriate. [H1, H2]	UCA-D81: False temperature measurements elsewhere in the system could split resources unnecessarily [H1, H2]	UCA-E81: If the measurement is not associated with the correct cell, then the system response may be poorly directed. [H1]	UCA-F81: Temperature data from inside the system could be useful to firefighters responding to an incident. If the temperature measurement is stopped too soon then it would not be available to them. [H4]
Smoke and Vent-Gas	UCA-C82: Generally, sensors can detect the presence or absence of smoke. If the smoke does not reach the detector, or the detector fails to sense the smoke, then smoke triggered reaction would not activate properly [H1,H2, H5]	UCA-D82: The open flame burns of much of the combustive portion of the vent-gas, however, some gas always makes it though. This gas could still lead to concentrations exceeding explosive limits [H2]. If the system response could be hazardous, then falsely triggering it could generate an unnecessary hazard. If this happens often (nuisance alarms), then the alarm may be ignored, leading to a hazard when the alarm is not triggered during a fire. [H1, H2, H5]. If combined with ventilation, smoke and vent-gas could be toxic to people who live or work near the site [H5].	UCA-E82: Some detectors are sensitive enough to detect trace concentrations of vent-gas in the air. If one of these sensors is used it is possible to get an early indication that a cell is in thermal runaway. If the system response depends on this early sign, then providing it too late could lead to a hazard [H1]	UCA-F82: Fire response could depend on the state of the air-smoke-gas mixture in the enclosed area. If the smoke stops detecting smoke before the air is truly clear, then firefighters would not have an accurate sense of the current system state. [H3]
Heat	No Hazard	UCA-D83: With open flames, the heat produces by a single cell in thermal runaway is immense. An unsafe control action would be if heat exceeded the maximum design limit to prevent propagation [H1]	N/A	N/A
Battery Outputs (Venting (no open flame))	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**

Voltage	UCA-C86: Not providing voltage measurements during an event can make it difficult to determine what went wrong after the fact. [H6]	UCA-D86: DC voltage can be hazardous to people and equipment. [H4]	UCA-E86: to be useful data must be appropriately timestamped. A mistimed voltage measurement could look anti-causal in post mortem analysis. [H6]	UCA-F86: Voltage data from inside the system could be useful to firefighters responding to an incident. If the voltage measurement is stopped too soon then it would not be available to them. [H5]
Current	UCA-C87: Not providing current measurements during an event can make it difficult to determine what went wrong after the fact. [H6]	N/A if a battery is venting then it is most likely open circuit meaning current cannot pass through it.	UCA-E87: to be useful data must be appropriately timestamped. A mistimed current measurement could look anti-causal in post mortem analysis. [H6]	N/A
Temperature	UCA-C88: Not providing temperature measurements during an event makes it difficult for the system to respond appropriate. [H1, H2]	UCA-D88: False temperature measurements elsewhere in the system could split resources unnecessarily [H1, H2]	UCA-E88: If the measurement is not associated with the correct cell, then the system response may be poorly directed. [H1]	UCA-F88: Temperature data from inside the system could be useful to firefighters responding to an incident. If the temperature measurement is stopped too soon then it would not be available to them. [H4]
Vent-Gas	UCA-C89: Generally, sensors can detect the presence or absence of smoke. If the smoke does not reach the detector, or the detector fails to sense the smoke, then smoke triggered reaction would not activate properly [H1,H2, H5]	UCA-D89: With no open flame, the combustive gases are generated at a much higher rate, which could lead concentrations that exceed the low explosive limit [H2]. If the system response could be hazardous, then falsely triggering it could generate an unnecessary hazard. If this happens often (nuisance alarms), then the alarm may be ignored, leading to a hazard when the alarm is not triggered during a fire. [H1, H2, H5]. If combined with ventilation, vent-gas could be toxic to people who live or work near the site [H5].	UCA-E89: Some detectors are sensitive enough to detect trace concentrations of vent-gas in the air. If one of these sensors is used it is possible to get an early indication that a cell is in thermal runaway. If the system response depends on this early sign, then providing it too late could lead to a hazard [H1]	UCA-F89: Fire response could depend on the state of the air-smoke-gas mixture in the enclosed area. If the smoke stops detecting smoke before the air is truly clear, then firefighters would not have an accurate sense of the current system state. [H3]

Heat	No Hazard	UCA-D90: Even if there is no open flame, cells that are venting from thermal runaway generate tremendous excess heat. This control action would be unsafe if the heat exceeded the designed specification for heat release [H1]	N/A	N/A

Outputs (Post incident)	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Voltage	UCA-C93: The energy stored in cells after an incident can start to slowly heat a cell until it goes into thermal runaway. This is normally shown in a falling voltage. Monitoring voltage will sometimes give a leading indicator of a cell that is going into self-heating [H1, H6]. Additionally, draining a cell into a load can reduce the stranded energy to a relatively safe level.	UCA-D93: DC voltage can be hazardous to people and equipment. [H4, H6]	UCA-E93: if voltage data are delayed for sufficient time then the cell could already be undergoing thermal runaway by the time a response is available. [H1, H6]	No hazard
Temperature	UCA-C94:The energy stored in cells after an incident can start to slowly heat a cell until it goes into thermal runaway. Temperature monitoring during this time is important and if it is not provided then an appropriate response may not be taken once self heating starts. [H1, H6]	No hazard	UCA-E94:If temperature data is delayed for sufficient time then the cell could already be undergoing thermal runaway by the time a response is available. [H1, H6]	No hazard
Heat	No Hazard	UCA-D95: Batteries can continue to produce heat long after an event. If heat is allowed to accumulate (say through installation) then the temperature could build to exeat safe temperatures in near by cells. [H1, H6]	UCA-E95: Cells that are thought to have achieved a safe state can develop internal shorts up to a month after an incident. [H1, H6]	No hazard

This page left blank

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Babu Chalamala	08811	bchalam@sandia.gov
Dan Borneo	08811	drborne@sandia.gov
Charles Hanley	08810	cjhanle@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Imre Gyuk	Imre.Gyuk@hq.doe.gov	U.S. Department of Energy

This page left blank

This page left blank

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Pacific Northwest National Laboratory is the U.S. Department of Energy's premier chemistry, environmental sciences, and data analytics national laboratory—managed and operated by Battelle since 1965, under Contract DE-AC05-76RL01830, for the DOE Office of Science.