ESIC Energy Storage Reference Fire Hazard Mitigation Analysis

3002023089

ESIC Energy Storage Reference Fire Hazard Mitigation Analysis

3002023089

Technical Update, December 2021

EPRI Project Manager

M. Rosen

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigators
N. Warner, Energy Safety Response Group
M. Bowes, Energy Safety Response Group
M. Simpson, EPRI
E. Minear, EPRI
D. Long, EPRI
M. Rosen, EPRI

This report describes research sponsored by EPRI. EPRI would like to acknowledge contributions from the following:

Key Contributors: Tom DeLucia (NEC), Roger Lin (NEC), Tom Kaun, and Ben Kaun (EPRI).

Energy Storage Implementation Practices collaborative supplemental participants: Hydro One, Duke Energy, Southern Company, Puget Sound Energy, Tennessee Valley Authority, and National Grid who supported the development of the expanded appendix material.

Energy Storage Integration Council (ESIC) Safety Task Force participants:

Ben Kaldunski, EPRI
Brian O'Connor, NFPA
Byron Ellis, Entergy
Chris Searles, BAE Batteries USA
Darren Jang, National Research Council Canada
Demy Bucaneg, Hawaiian Electric
Gabriel Andaya, Southern California Edison
Ian Hoag, PacifiCorp
Jens Conzen, Jensen Hughes
Kevin Fok, LG Chem
Matthew Paiss, Pacific Northwest National Laboratory
Michal Lisowyj, Omaha Public Power District
Morgan Smith, EPRI
Nicholas Jewell, LG&E and KU Energy
Randall Stacy, Nexceris
Ryan Franks, CSA Group
Sam Gillie, Hawaiian Electric
Sooyeol Kim, KEPCO
Stephanie Shaw, EPRI
Steve Cummings, Nexceris
Tom Simchak, Energy Storage Association
Tommy Jacoby, Swinerton Renewable Energy
Wahhaj Irfan, Commonwealth Edison
William Ivans, Verisk ISO

This publication is a corporate document that should be cited in the literature in the following manner:

ESIC Energy Storage Reference Fire Hazard Mitigation Analysis. EPRI, Palo Alto, CA: 2021. 3002023089.

ABSTRACT

Following a series of energy storage fire-related incidents in 2018 and 2019, the Energy Storage Integration Council (ESIC) engaged its Safety Task Force to highlight current industry gaps and challenges related to safety. After finding few public assessments of energy storage system fire causes, consequences, and mitigations, the task force engaged industry expertise to develop a set of reference hazard mitigation analyses. The resulting diagrams illustrate likely failure modes for a generic energy storage system, which may help to curb or eliminate the hazard, by applying a 'bowtie' approach in which threats link to hazards and eventual effects through barriers.

This report details the process and provides a reference for future applied site-specific assessments, suggesting a common format and a common language to improve confidence among stakeholders when developing, procuring, and operating safe energy storage systems. This 2021 update incorporates safety design and site evaluation learnings, and includes expanded descriptions of the threats, barriers, and consequences to further support clear, objective discussions between stakeholders.

Keywords

ESIC
Energy Storage
Safety
Fire
Thermal Runaway
Hazard Mitigation Analysis

ABBREVIATIONS AND ACRONYMS

AHJ	Authority Having Jurisdiction
BMS	Battery Management System
BoP	Balance of Plant
BoS	Balance of System
EPRI	Electric Power Research Institute
ESIC	Energy Storage Integration Counsel
ESMS	Energy Storage Management System
ESS	Energy Storage System
FACP	Fire Alarm Control Panel
HAZMAT	Hazardous Material
HVAC	Heating Ventilation and Air Conditioning
NFPA	National Fire Protection Agency
PCS	Power Conversion System
PLC	Programmable Logic Controller
QC	Quality Control
SOC	State of Charge
SOP	Standard Operating Procedures
TR	Thermal Runaway

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
OVERVIEW OF THE REFERENCE HAZARD MITIGATION ANALYSIS

1.1 Background

In 2019, the Energy Storage Integration Council (ESIC) relaunched the Safety Task Force following a series of energy storage fire-related incidents that highlight current industry gaps and challenges related to safety. Several utilities identified a specific need for supplemental guidance to enhance the safety of both planned and deployed systems in a rapidly evolving market. Additionally, stakeholders, including utilities, vendors, and integrators, expressed challenges experienced when communicating safety requirements and the value of safety features during procurement. The ESIC Safety Task Force determined that a reference hazard mitigation analysis (HMA) would help facilitate objective planning for product and project safety.

Since the initial release of the ESIC Reference Fire Hazard Analysis in September 2019, there have been approximately 20 known ESS-related failure events across the globe[1]. These incidents have occurred in systems ranging from 500 kWh to 1,200 MWh, and have resulted in massive property damages, injuries to first responders, and even deaths. The primary gaps in safety identified during these incidents included failure during commissioning, inadequate fire protection systems, and lack of robust first responder training. This update incorporates findings and lessons learned from these incidents to provide guidance and support to project stakeholders.

1.2 Scope and Organization of this Report

This report describes a set of failure and risk scenarios characteristic of lithium ion ESS failures, as well as mitigative protections aimed at supporting utility industry self-evaluation of ESS risk throughout the project procurement, development, deployment, and operational processes. While the current state of this document is centered around lithium ion ESS failures, it is intended to be expanded upon to include guidance on other energy storage technologies as they become more prevalent in the market.

This report is organized as follows:

- Section 2 provides an overview of hazard mitigation analyses and the bowtie methodology utilized for this report.
- Section 3 provides an overview of primary consequences characteristic of lithium ion ESS failures (Section 3.1), as well as high-level overviews of the most prevalent hazard scenarios associated with them. These scenarios include:
  - Cell Internal Failure (Section 3.2)
  - Non-Cell Thermal Risks (Section 3.3)

[1] https://storagewiki.epri.com/index.php/BESS_Failure_Event_Database

- Controls Failure (Section 3.4)
- Electrical Risks (Section 3.5)
- External and Environmental Risks (Section 3.6)

  Each hazard above is supplemented by an accompanying bowtie diagram visualizing the pathways of failure propagation, as well as a table of brief descriptions of the associated threats, barriers, and consequences. A unique identifier is given to each table item so that it may be quickly referenced between diagrams and in the associated appendices, and are noted as follows: Threats [A], Threat Barriers [B], Consequences [C], Consequence Barriers [D].

- Detailed descriptions of all threats, threat barriers, consequences, and consequence barriers are provided in Appendix A through D, respectively, and are organized to correspond to the identifiers given in the bowtie diagrams and associated scenario tables.

1.3 How to Apply this Reference Hazard Mitigation Analysis

The information provided in this report should equip the reader with a functional understanding of the primary consequences and hazard scenarios associated with of lithium ion ESS failures and is intended to help support communication of risks between stakeholders throughout the lifecycle of an energy storage project. While this reference hazard analysis utilizes the bowtie methodology as a framework for risk assessment, other methodologies may offer other strengths or weaknesses. This should be considered when developing or reviewing any risk assessment.

During procurement, utilities can request specific information about the safety of the energy storage components, integration, and operational processes. The barriers identified in this reference analysis were incorporated into the ESIC Energy Storage Technical Specification Template. The template asks responders to describe how their proposed offering addresses the barrier in question. This will enable responders to highlight safety features and enhancements. Additional information during procurement also better enables utilities to assess the safety of the systems and make informed decisions. The reference hazard mitigation analysis helps to put the safety discussion in the context of threat and consequence pathways.

During deployment and integration, this can be used to support discussions with the authority having jurisdiction (AHJ) or other permitting authorities. Some state or local codes required hazard mitigation analysis as part of the permitting process. It may also inform commissioning procedures to ensure the barriers are operating as intended.

During operations, there are several human factors that can impact the likelihood or severity of the consequence. This reference hazard can support the development of operating procedures and processes to ensure barriers continue to operate as intended.

2
METHODOLOGY

2.1 Risk Assessment and Considerations

Risk assessments can take on many different forms and functions, each with its own strengths and weaknesses. In general, these follow a common process of risk identification, risk analysis, and risk evaluation – the goal of which is to provide an understanding of risks, their causes, consequences, and mitigative strategies in place to prevent further propagation of failure.

Recent codes and standards such as International Fire Code (IFC) and NFPA 855: Standard for the Installation of Stationary Energy Storage Systems have incorporated requirements for hazard mitigation analysis which include several fault conditions to be assessed, though a single assessment methodology to be used is not specified. Furthermore, the fault conditions listed in these are general in nature and limited with respect to the full range of potential hazard scenarios associated with energy storage systems – notably those associated with lithium ion ESS.

Several other important considerations when developing or reviewing a hazard mitigation analysis include:

- **Intended Audience / End User**

  One of the most important considerations when developing a hazard mitigation analysis is who the intended audience is. For instance, content prepared for a local authority having jurisdiction (AHJ) responsible for approving an ESS installation may be very different from that being prepared for research and development purposes. Other examples of industry stakeholders who may be reviewing hazard mitigation analyses include utilities / independent power providers, project developers, vendors, system integrators, and other subject matter experts or researchers.

- **Project Lifecycle**

  As noted in Section 1.3, hazard mitigation analyses may apply across several stages of a project lifecycle. It is not uncommon for significant changes in equipment or siting to be made and it is therefore important to account for any of these changes. It may be beneficial for hazard mitigation analyses to be developed at different stages of project development such as design phase, installation phase, etc., to account for changes in project specifications. An important stage in a project's lifecycle to develop a unique hazard mitigation analysis is prior to commissioning. In this stage, safety systems may not be in place so there may be reduced barriers to hazardous events.

- **Available Documentation**

  It is important that all relevant documentation is made available when developing a hazard mitigation analysis, as insufficient or outdated information may leave gaps in safety or may not represent the most current state of the project. All project documents including site layout, engineering drawings, test reports, certifications and listings, and fire protection engineering studies or other substantiating documents should be provided.

2.2 Bowtie Methodology

The ESIC Safety Task Force chose bowtie modeling for the reference analysis, as its simple diagrammatic nature is useful for describing an analyzing the pathways of a risk from threats to consequences, and to assess the mitigative barriers placed in between. While already a common, industry-accepted risk analysis tool used in the maritime, oil & gas, and utility industries, the bowtie model has proven useful in enabling informed project design and permitting in the energy storage industry.

Bowtie analysis can be thought of as a combination of the logic of a fault tree analyzing the cause of an event (represented by the knot of a bowtie) and an event tree analyzing the consequences. On the left side of the bowtie diagram are a range of identified threats which may result in a common failure or "top" event, from which more severe potential consequences may arise. Barriers (which may exist in the form of physical hardware, protection measures, or be representative of larger concepts or protocols) are placed to mitigate propagation of failure on both the threat and consequence side of the diagram.

An example bowtie diagram, along with the associated threats, consequences, and barriers is displayed generically in Figure 2-1.

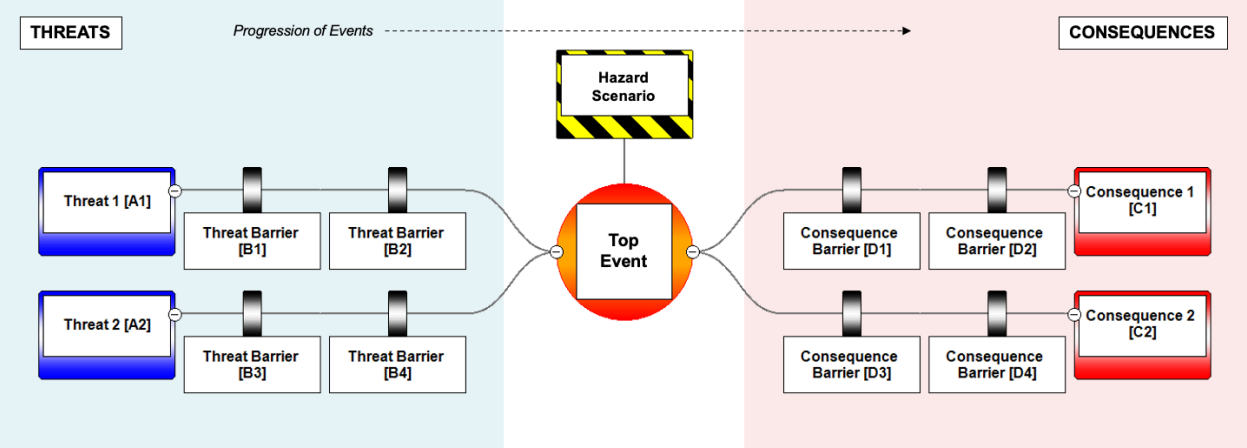

Figure 2-1
Example Bowtie Diagram

It should also be noted that, being qualitative in nature, the bowtie method provides a level of flexibility for risk assessment in situations where limited safety or failure data is available and it is difficult to assign quantitative probabilities with a significant degree of confidence (as is the current state of the energy storage industry at this time). As more data around ESS failures is collected, more quantitative methods of risk assessment may become applicable and widely used.

2.2.1 Top Event

The top event – depicted as the center point in the middle of the bowtie diagram – represents a deviation from the desired state during normal operations (in this case, a thermal runaway or cell failure event), at which point control is lost over the hazard and more severe consequences ensue. This event happens before major damage has occurred, and it is still possible to prevent further damage.

Perhaps the most critical event associated with lithium ion batteries is the occurrence of cell failure leading to thermal runaway and subsequent propagation to nearby cells, leading to greater consequences such as fire or even explosion, as described in Section 3.1.

2.2.2 Threats

There often may be several factors that cause a "top event". In bowtie methodology, these are called threats. Each threat itself has the ability to cause the top event. Examples of threats are hazardous temperature conditions, BMS failure, and water damage from condensation, each leading to cell failure (the top event for many of the following bowtie diagrams for lithium ion ESS failures).

Threats may not necessarily address a fully involved system fire or severe explosion, but rather smaller, precursor events which could lead to these catastrophic consequences. Some threats occur without any intervention, such as defect propagation or weather-related events, while others represent operational errors (either human or system-induced). Often threats may also be consequences of even earlier-stage threats, spawning a new bowtie model that includes the threat at the center point or right side of the new bowtie. The diagrams that follow include careful selection and placement of each of the elements to best capture the perspective of system owners and operators responsible for ensuring safe operation.

2.2.3 Consequences

Consequences are the results of a threat pathway reaching and exceeding its top event. For the models described here, the top events were selected as the event in which proactive protections give way to reactive measures mostly related to fire protection systems and direct response. As the top event then is defined as either "cell failure" or propagating cell failure, the consequences in the models described assume a condition exists in which flammable gas is being released into the system or a fire is burning within the system.

Consequence pathways include barriers that may help to manage or prevent the consequence event. Threat pathways are often consequence pathways from a separate hazard assessment, as is the case with thermal runaway. In other words, thermal runaway may result from many different threats at the end of a separate hazard pathway (if not properly mitigated) and may also be the threat that could result in several other consequences. The task force identified a set of common consequences representing areas of key concern to utilities, energy storage system operators, and first responders.

2.2.4 Barriers

In order to control risks, mitigative "barriers" are placed to prevent propagation of failure events across the system. A barrier can be any measure taken that acts against an undesirable force or intention, in order to maintain a desired state, and can be included as proactive threat barriers or reactive consequence barriers.

Each barrier in these models is more indicative of a concept that may include a single approach or may consist of a complex series of combined measures. Similarly, the analysis may not include barriers required to prevent the threats at the far left of the diagram (which would be placed even further left) to ensure the models do not extend infinitely, though the incorporation of these variables into site-specific safety evaluations may provide additional benefit. This list

does not contain all possible solutions and in some designs, these barriers may not exist at all. Many of the same barriers apply to a number of threats.

Barriers may mitigate hazards or consequences in a variety of ways. For example, common barriers to thermal runaway include active electrical monitoring and controls, redundant failure detection, and even passive electrical safeties (such as over-current protection devices and inherent impedances). Should these systems fail to detect the threat, shutdown the system, or otherwise prevent thermal runaway from occurring, the hazard may persist.

2.3 Assessment

2.3.1 Criticality

Criticality values can be assigned to further assess the significance of the failure of any of the mitigative barriers provided. This assessment may take on many different forms and may be qualitative, semi-qualitative, or quantitative in nature, depending on the overall goals of the hazard mitigation analysis. As discussed in Section 2.1 – given the limited availability of ESS-related failure data – it has become increasingly common to see criticality defined either qualitatively or semi-qualitatively.

In addition to a strong foundational and conceptual knowledge of the ESS in question (and constituent components / barriers), context is key to assessing the criticality of barriers set in place to mitigate failure propagation across the system. Many factors come into play when designating a criticality value – for instance, a given barrier may be less critical if there are many additional barriers provided in the same failure pathway (or more critical if it is the sole barrier preventing further propagation of failure). Criticality may also change over the course of an event, becoming potentially more or less critical, depending on the stage of failure and the design of the system.

2.3.2 Effectiveness

The effectiveness of barriers may also be assessed, providing even more context to a given hazard scenario. This effectiveness value would indicate how well a barrier performs – or is expected to perform – based on available data and / or expert judgement. Like criticality values, these are most commonly defined either qualitatively or semi-quantitatively.

It should be noted that, similar to criticality, the effectiveness of a given barrier may change drastically as the stage of failure across the system progresses and equipment or other mitigative barriers fail. Several examples describing these situations are given in Section 3.1.

3
PRIMARY HAZARD SCENARIOS

3.1 Primary Consequences of ESS Failure

The dynamics of a lithium ion ESS failure is extremely complex and the pathway of failure events may vary widely based on mitigation approaches utilized, in addition to even small changes in environmental or situational conditions. The following diagram depicts the primary consequences of a potential large-scale lithium ion ESS failure stemming from a battery cell failure (though other failure scenarios may certainly occur, ultimately leading to similar consequences). These primary consequences serve as the basis for the majority of the consequence sides of the following hazard scenarios, and may range from single cell combustion to fully-engaged fire, explosion, in addition to a number of environmental issues such as water runoff contamination or toxic smoke plumage.

In some cases, the endpoint of a consequence is itself not the end of the event, and a single-cell failure resulting in off-gas can easily evolve to a multi-cell failure with fire and ultimately a multi-module fire or worse. Thus, with consequences, as with threats, common barriers may be evaluated differently depending on the consequence they are associated with, and consequence pathways should not be assumed to be similar despite being comprised of similar barriers. As an example, though detection, ventilation, and suppression systems are barriers in almost all consequence pathways, their effectiveness may be greatly dimished (if not completely nullified) as the stage of failure progresses and equipment may become damaged. Similarly, barriers may become less or more critical depending on the stage of failure and the design of the system. As a further example, water-based suppression may not prove effective at a single-cell failure while a gas-phase agent may suppress combustion and limit the convective failure. As the scale of the fire increases, however, gas-phase agents may only exacerbate the situation while water-based agents may more effectively manage the heat transfer. Ultimately, each consequence pathway should be evaluated separately and uniquely based on the consequence condition.

Finally, it should be noted that while large-scale fire testing and commitment of considerable resources to the study of energy storage safety issues has drastically improved the industry's understanding of failure modes, threats, consequences, and general safety, many failure modes and corresponding responses remain uncharacterized. Unknown failures may also potentially arise, though a separate consequence pathway is not explicitly designated in the list of primary consequences in this section.

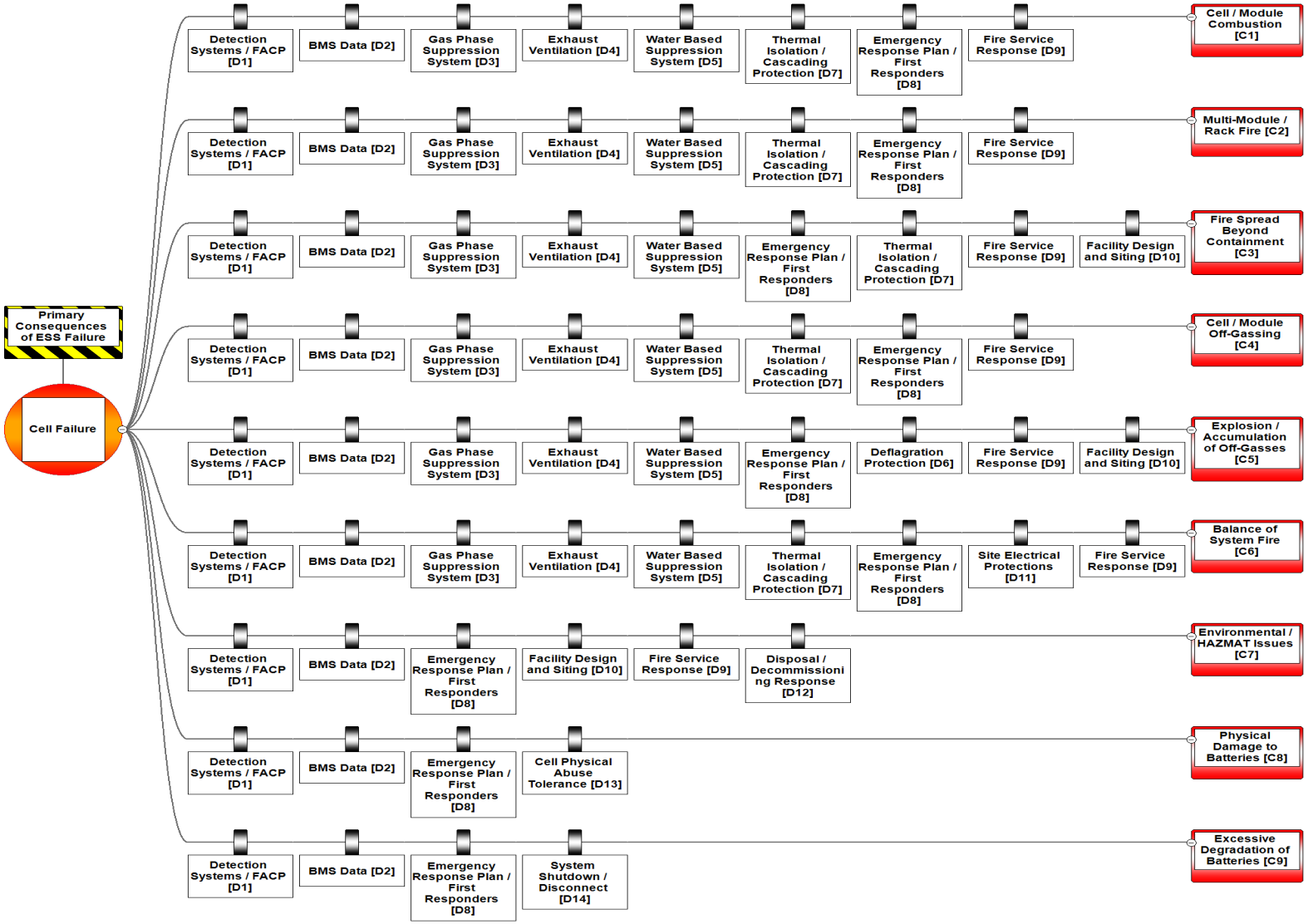

Figure 3-1
Primary Consequences of ESS Failure

Table 3-1
Primary Consequences of ESS Failure

Consequences – *Primary Consequences of ESS Failure*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.
C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.
C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *Primary Consequences of ESS Failure*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data** Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.

D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.
Consequence Barriers – *Primary Consequences of ESS Failure (continued)*	
D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders** System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.
D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

3.2 Cell Internal Failure

The quintessential cause of thermal runaway, cell internal failure, as defined here, refers to internal failure of the cell that may result in thermal runaway, but is not brought about by external stimuli. This failure mode includes internal manufacturing defects, dendrite formation, separator failure, or any other failure which emanates from within the cell. Unlike failures brought about by external stimuli and which may be mitigated or managed prior to thermal runaway, internal defects can be difficult to detect or manage in operating systems and frequently result in thermal runaway with little to no warning. Further, internal cell failures may quickly expand beyond their initial threat pathway, causing fires and other failures which will quickly spread to adjacent cells and beyond.

However, while this failure mode does frequently result in thermal runaway, not all failures result in thermal runaway just as not all thermal runaways result in a fire. Internal defects in cells not resulting in thermal runaway may result in drastic changes in cell impedance, resulting in ohmic heating, voltage drops, or other adverse thermal or electrical conditions. Cells experiencing internal failure without thermal runaway may still pose serious risks to operation and should be identified, bypassed or removed as quickly as possible.

Also note that the top event for this hazard is not cell failure, as that itself is the threat. Instead, the top event in this hazard is propagating cell failure. To that end, this hazard model serves to examine what is essentially the consequence of every other hazard model by looking at how single and multicell events can be managed as threats before propagating to consequences which must be addressed.

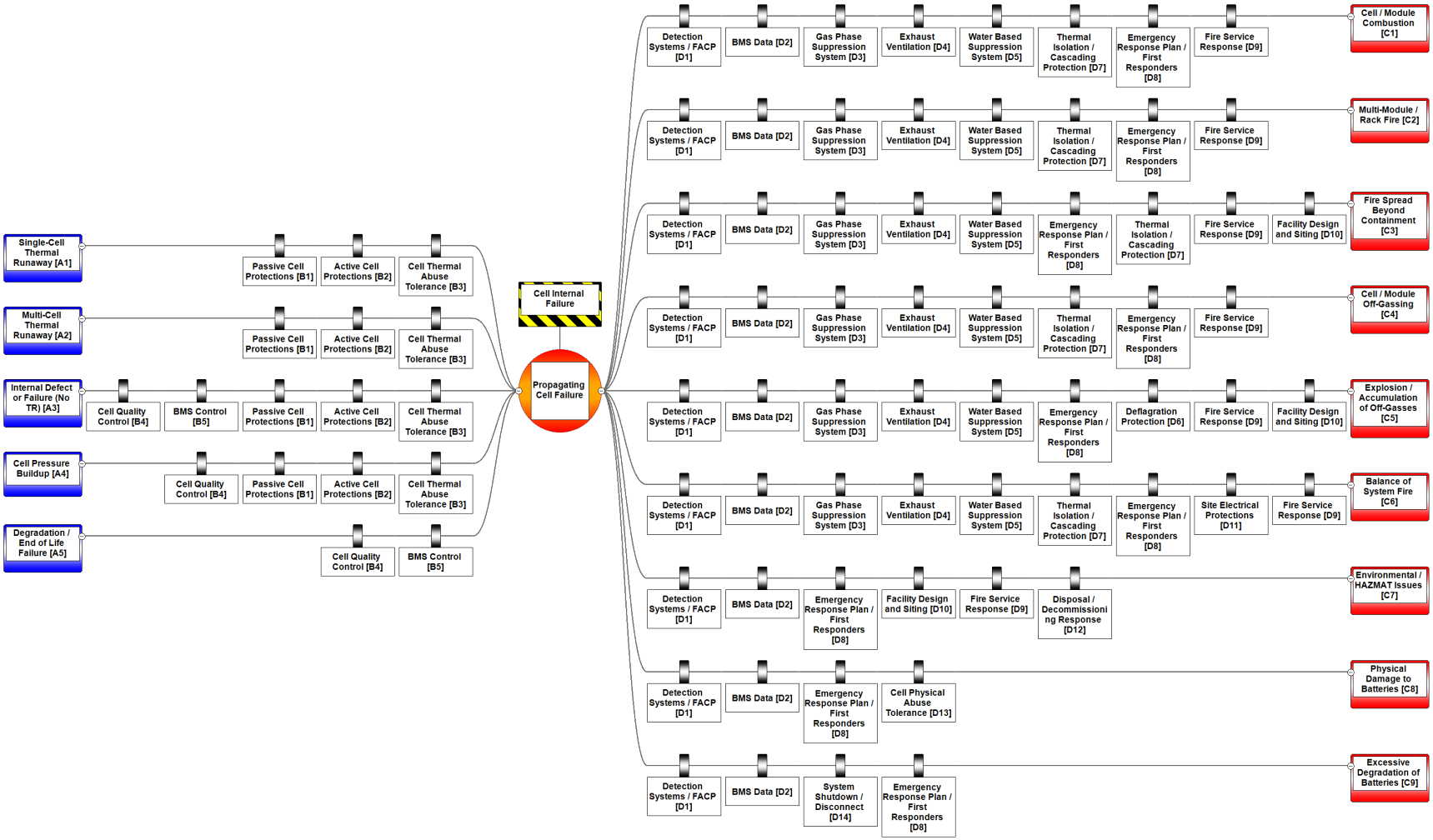

Figure 3-2
Cell Internal Failure

Table 3-2
Cell Internal Failure - Threats and Consequences

Threats – *Cell Internal Failure*	
A1	**Single-Cell Thermal Runaway** A single cell has entered thermal runaway resulting in flames and combustion or production of flammable or explosive gases.
A2	**Multi-Cell Thermal Runaway** Multiple cells have entered thermal runaway or begun burning.
A3	**Internal Defect or Failure (No Thermal Runaway)** A cell has failed as a result of an internal defect, creating a short circuit, open circuit, or other electrical condition or off-gas but not entering thermal runaway.
A4	**Cell Pressure Buildup** A cell has begun to build internal pressure as a result of gas generation. The cell has not yet failed or vented this gas.
A5	**Degradation / End of Life Failure** A cell or cells have reached end of life, resulting in an adverse electrical condition which could exacerbate imbalance or other adverse electrical conditions.
Threat Barriers – *Cell Internal Failure*	
B1	**Passive Cell Protections** System design, passive materials, or other design elements incorporated to passively protect neighboring cells from localized cell failure. This also includes the likelihood of cell-to-cell propagation based on system design.
B2	**Active Cell Protections** Active cell protections which may mitigate thermal runaway such as module fans, liquid cooling systems, module scale suppression systems, or other mitigation measures.
B3	**Cell Thermal Abuse Tolerance** Ability of the cells to withstand thermal abuse without going into failure themselves.
B4	**Cell Quality Control** Overall quality of the cell such that internal defects are minimized and cells maintain rigidity and shape during operations. Also includes tight tolerances with respect to degradation and new capacity.
B5	**BMS Control** Includes monitoring and shutdown/isolation capabilities of the affected BMS/module or system if necessary.
Consequences – *Cell Internal Failure*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.

C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.
Consequences – *Cell Internal Failure (continued)*	
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.
C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *Cell Internal Failure*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data** Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.
D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.

D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
Consequence Barriers – *Cell Internal Failure (continued)*	
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders** System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.
D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

3.3 Non-Cell Thermal Risks

Lithium ion batteries are susceptible to a number of thermal failures which may begin externally as a result of exposure to dangerously high temperatures. This may be the result of operation in elevated ambient temperatures or in cases where high temperatures within the modules or electrical system have developed. These high temperatures result in adverse conditions that may increase the likelihood of internal cell failure and may exist at different levels, coming about as a result of numerous conditions such as hot spots in modules as a result of poor packaging design or on busbars as a result of loose connections. Perhaps even more importantly, inadequate temperature monitoring at this level – a common design flaw seen in some systems – may allow such issues to form or worsen without detection.

At the container level, an HVAC failure may allow container ambient temperatures to reach dangerously high levels. Though sensors should reliably detect this issue and stop the system, this has not occurred in all cases. In some cases, HVAC failure allowed ambient temperatures to quickly reach unsafe levels though cell temperatures rose slower because of the thermal mass of the system. This can still pose a hazard, necessitating monitoring of both cell and ambient conditions to avoid problems before they worsen. Further, poor HVAC designs may heat or cool systems unevenly, resulting in hotspots.

Even in cases where the battery or individual cells are not directly exposed to high temperatures, the presence of such temperatures in other parts of the system may yield equally adverse events. In one instance, cyclical exposure to dangerously high temperatures posed minimal risk to the storage technology but potentially caused failure in the electronics, which allowed an overcharge that resulted in a fire and a complete loss of the system. Further, in cases where high temperatures exist damage may still be done to the batteries in the form of accelerated health degradation, or aging. While discussion of battery aging and degradation are beyond the scope of this document, elevated temperatures pose considerable risk to the normal operation of the battery by way of inducing excessive degradation. In cases where this degradation is uneven, the loss of energy capacity may result in an increasingly difficult to control, and even unstable system. This state may ultimately lead to failure, potentially catastrophic, if not managed.

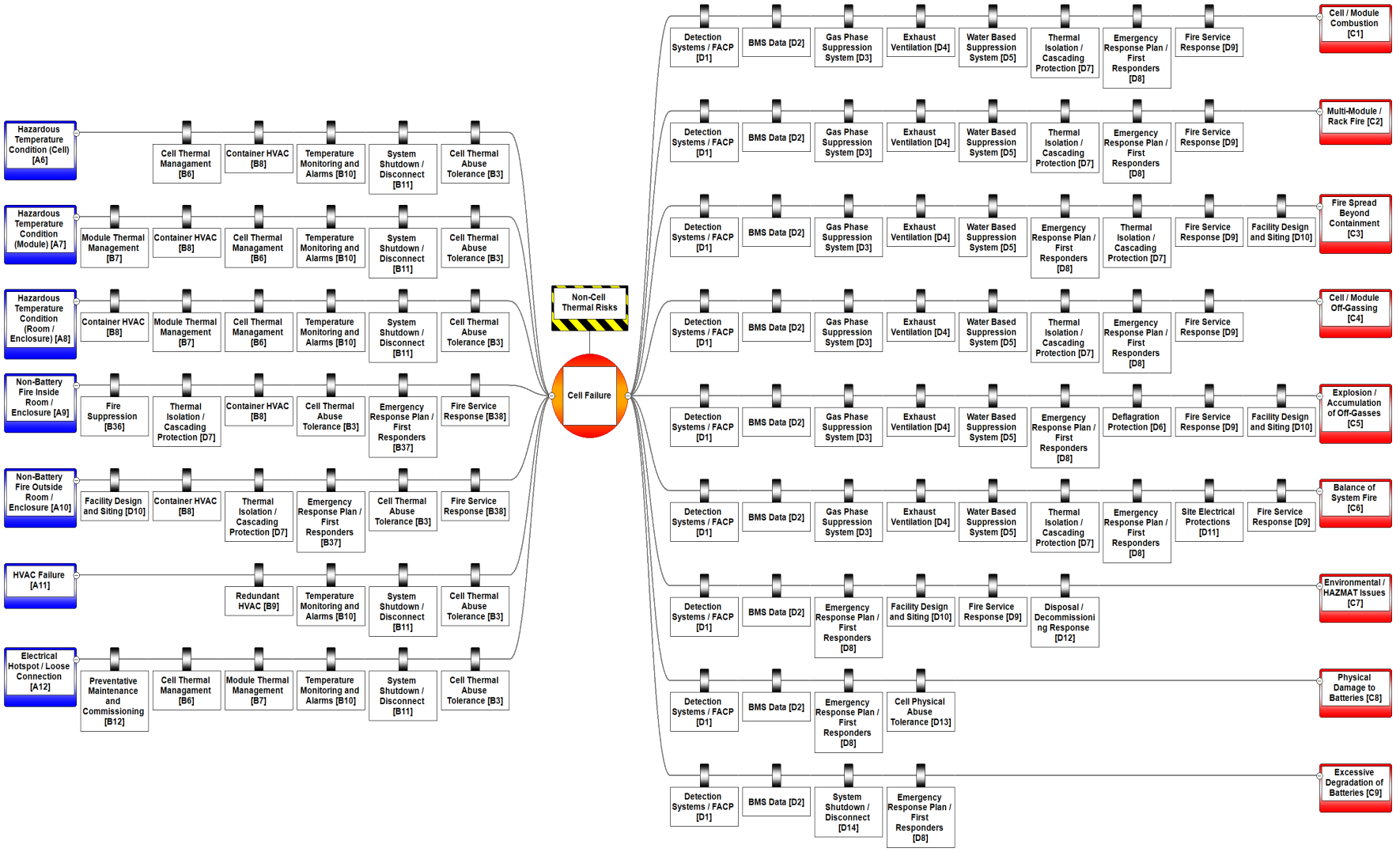

Figure 3-3
Non-Cell Thermal Risks

Table 3-3
Non-Cell Thermal Risks - Threats and Consequences

Threats – *Non-Cell Thermal Risks*	
A6	**Hazardous Temperature Condition (Cell)** *High temperature at the cell level during normal operations without thermal runaway.*
A7	**Hazardous Temperature Condition (Module)** *High temperature in the module during normal operation without failure / thermal runaway.*
A8	**Hazardous Temperature Condition (Room / Enclosure)** *High temperature in the room or enclosure from normal operations.*
A9	**Non-Battery Fire Inside Room / Enclosure** *Fire in container from balance of system that results in dangerously high temperatures inside the enclosure.*
A10	**Non-Battery Fire Outside Room / Enclosure** *A fire impinging on the outside of the container or a fire in an isolated and insulated part of the enclosure, such as a fire in a PCS room on the other side of a proper fire wall.*
A11	**HVAC Failure** *Mechanical or electrical failure of the HVAC system that will result in high temperatures throughout system.*
A12	**Electrical Hotspot / Loose Connection** *Loose connections in the system may increase resistance and cause hotspots. Hotspots may form in other ways for unknown reasons. These hotspots will then conduct via bus bars or mechanical contact into cells.*
Threat Barriers – *Non-Cell Thermal Risks*	
B3	**Cell Thermal Abuse Tolerance** *Ability of the cells to withstand thermal abuse without going into failure themselves.*
B6	**Cell Thermal Management** *Active and passive controls put in place to manage cell temperature. Includes passive materials like Phase change material, module fans, liquid cooling system or passive systems dependent on system HVAC.*
B7	**Module Thermal Management** *Thermal management at the module scale including effectiveness of system HVAC at this level, passive materials, fans, and liquid cooling.*
B8	**Container HVAC** *Heating, ventilation, and air conditioning for the overall container designed to maintain overall system temperature and humidity levels.*
B9	**Redundant HVAC** *Design, sizing, and hardware physical redundancy of the HVAC system such that failure of one or multiple units does not result in adverse conditions within the container or system.*

Threat Barriers – *Non-Cell Thermal Risks (continued)*	
B10	**Temperature Monitoring and Alarms** *Thermal monitoring within the container including BMS, fire alarm thermal monitoring, and any BoS temperature monitoring.*
B11	**System Shutdown / Disconnect** *Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.*
B12	**Preventative Maintenance and Commissioning** *Proper maintenance and monitoring of the system in conjunction with adequate commission and site acceptance testing to reduce likelihood of loose connections or other transportation or construction defects.*
B36	**Fire Suppression** *Fire suppression inside battery compartment which may address BoS fire without adverse effect on batteries. Potentially separate from battery fire suppression.*
B37	**Emergency Response Plan / First Responders** *System operator plan to handle any and all emergency events external to battery cells from propagating to the cells themselves. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.*
B38	**Fire Service Response** *Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.*
Consequences – *Non-Cell Thermal Risks*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.
C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.
C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues**

	A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *Non-Cell Thermal Risks*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data** Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.
D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.
D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders** System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.

D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

3.4 Controls Failure

The loss, failure, or abnormal operation of an energy storage control system (controllers, sensors, logic / software, actuators, and communications networks) will directly impact the proper function of the system. As the types, designs, and architectures of systems deployed and in development varies widely, so too do the control schemes and architectures. As such, the barriers in this chapter in many cases are condensed down to single concepts which may numerous barriers and barrier types and could be broken out as such. This section lists and explains the threats associated with a hazard resulting from a failure in an energy storage control system.

While obvious examples of failure in the control system (such as the mechanical failure of a relay or the electrical failure of an electronics component may result in the inability of the system to function properly), inadequate design of the control system may pose an even greater risk. As an example, a system of paralleled racks which contains no physical disconnects with which to isolate itself from the grid is not only dependent on the power electronics to isolate it, but also lacks an ability to isolate malfunctioning racks from their neighbors. As a result, not only is this system susceptible to a single point of failure in the power electronics, but it may also not adequately protect itself in case of an external short circuit. Therefore, it is important when assessing control system risks not only to look at the resiliency of the individual control hardware components and software, but the effectiveness of controls throughout the integrated systems.

As the size of the system grows, so too does the complexity of the system and the need for multiple layers of control systems. An examination of a single containerized system may reveal, as an example, four or more levels, or layers, of control systems. These controls layers include:

1. A module-level management or monitoring system which may or may not possess the ability to report adverse cell conditions, isolate the module, shut down the entire rack or system, and manage the balancing of the cells within the module.
2. A rack-level management system which may or may not possess the ability to perform some or all of the following: monitor all modules for adverse conditions, shut down or isolate the rack, shut down the entire system, and manage the balancing at either the cell and/or module level.
3. An overall system controller, commonly referred to as an energy storage management system (ESMS) controller, monitors all racks, and potentially any PLC (programmable logic control), fire control, or other balance of system controllers to determine if the ESS should be shut down or otherwise placed in a safe condition based on conditions at the site level and on equipment beyond the battery itself.

4. All other balance of system controllers including utility PLC controllers, fire control systems, ESS PLC controllers, site security systems and any other balance of system or plant controller which may operate based on ESMS signals or which may impact the functioning of the ESMS.

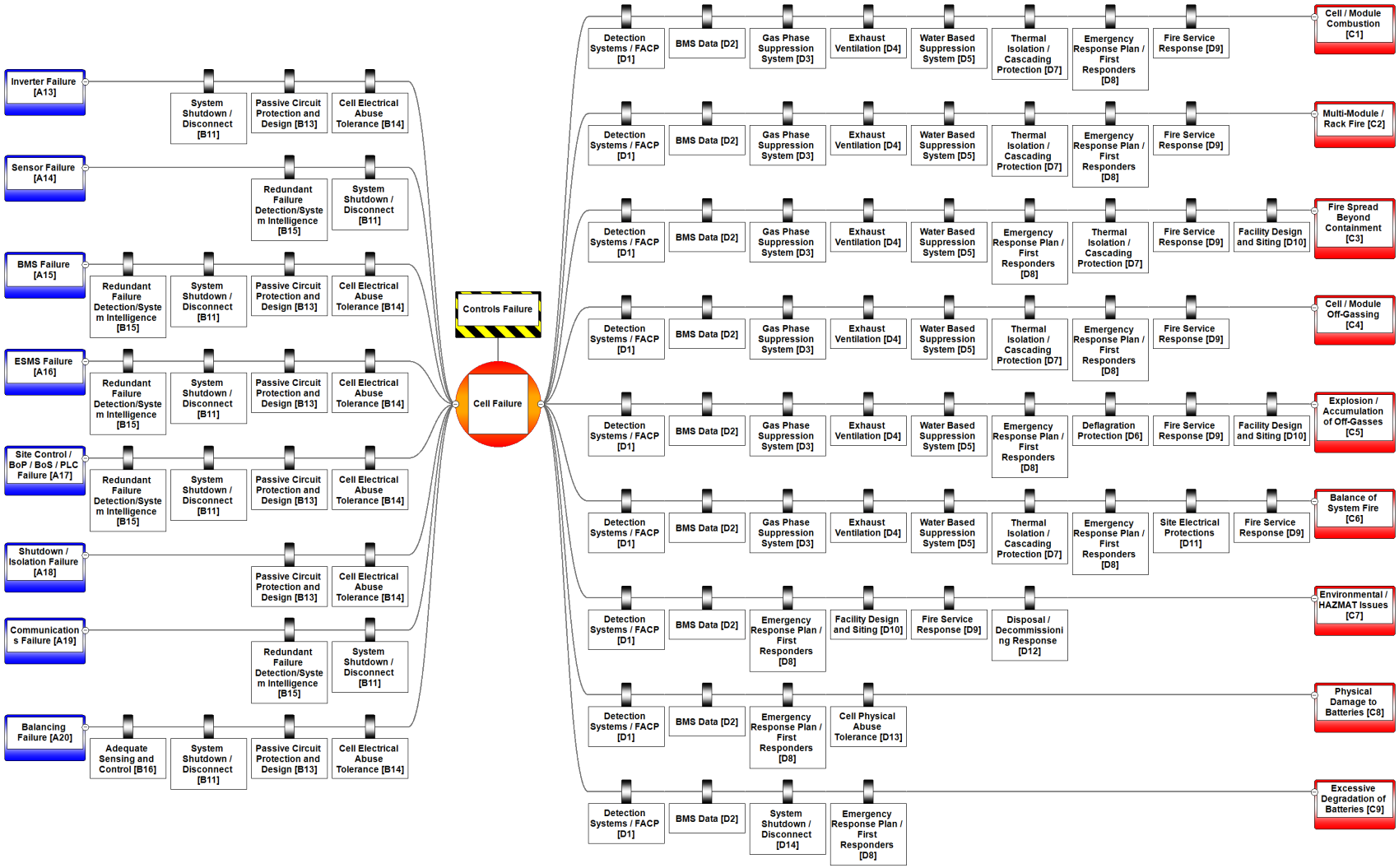

Figure 3-4
Controls Failure

Table 3-4
Controls Failure - Threats and Consequences

Threats – *Controls Failure*	
A13	**Inverter Failure** Inverter or power electronics fail in a way that poses risk to the batteries. Could include a lock up in the "On" position which drives overcharge.
A14	**Sensor Failure** A sensor inside the system fails, resulting in incorrect reporting of system properties.
A15	**BMS Failure** Cell / module level monitoring and control fails, resulting in inability to shut down, report adverse conditions, properly monitor, balance or protect the system resulting in adverse condition.
A16	**ESMS Failure** Failure of the controller at the rack or system level which results in adverse condition to the system.
A17	**Site Control / BoP / BoS / PLC Failure** Failure of the site controller or other balance of system controller resulting in adverse condition to the system.
A18	**Shutdown / Isolation Failure** Failure of the system to shut down or isolate itself when an adverse condition is detected.
A19	**Communications Failure** Failure of the system to properly report an adverse condition to local or remote monitoring, resulting in adverse condition.
A20	**Balancing Failure** Failure of the system at the cell, module, or rack level to maintain balance, resulting in unstable or unbalanced system. This will result in premature end of life condition or adverse safety condition.
Threat Barriers – *Controls Failure*	
B11	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.
B13	**Passive Circuit Protection and Design** Current interrupt devices, breakers, fuses or other passive surge arresting elements which may open the circuit in the case of failure and general resilience of design to withstand adverse electrical conditions. Note hazard condition and component and that not all protections apply to a certain failure.
B14	**Cell Electrical Abuse Tolerance** Ability of the cell to withstand electrical abuse such as overcharge, over discharge, high currents, or other adverse electrical abuse.
B15	**Redundant Failure Detection / System Intelligence**

	Ability of system to determine a sensor has failed, to operate safely without that sensor to shut down, or operate safely indefinitely without sensor. This may include Checksums, additional sensors, or the ability to pull data from other sensors.
Threat Barriers – *Controls Failure*	
B16	**Adequate Sensing and Control** Aggregate of the ability of the BMS to detect cell imblanace and to properly return system to balance if possible. This includes adequately sized passive or active balancing scheme.
Consequences – *Controls Failure*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.
C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.
C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *Controls Failure*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data**

	Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.
D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.
Consequence Barriers – *Controls Failure*	
D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders** System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.
D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

3.5 Electrical Risks

By nature of being an electrical system, an ESS is subject to many of the same failures that plague all electrical devices. While battery failure rates are not currently published or well understand, power electronics failure rates are better understood and are not just plausible but can and do occur. To that end, management of and protection against such failures are required. Though many of the issues covered previously in the Controls Failure hazard may also be considered electrical or be based on the result of electrical failures, electrical risks apply more specifically to components and purely electrical failures.

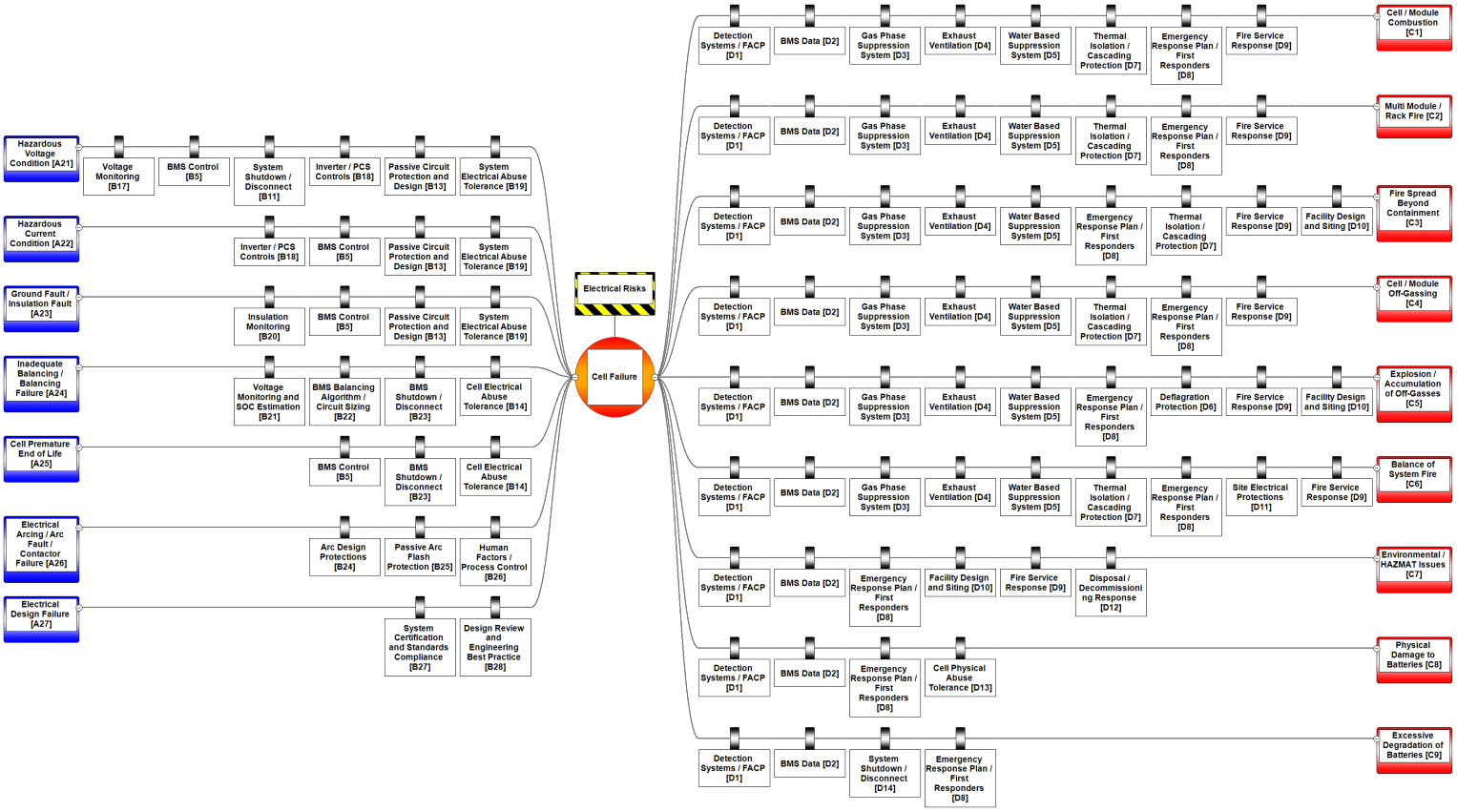

Figure 3-5
Electrical Risks - Threats and Consequences

Table 3-5
Electrical Risks - Threats and Consequences

Threats – *Electrical Risks*	
A21	**Hazardous Voltage Condition** This could include high line voltages, high voltages from the PCS, floating ground issues, or other high voltage issues at the cell, module or rack level.
A22	**Hazardous Current Condition** This includes high current issues from the PCS or interconnection.
A23	**Ground Fault / Insulation Fault** This could include localized shorting of cells, shorting between modules, shorting of entire racks or systems and ground fault shorting.
A24	**Inadequate Balancing / Balancing Failure** This includes cells that become imbalanced within a module, modules out of balance with other modules in a string or strings/racks out of balance with the rest of the system. This could be a result of uneven usage, inadequate balancing design, or uneven thermal management.
A25	**Cell Premature End of Life** Cell degrades prematurely such that it reduces effective capacity of parallel groups, results in high resistance or open circuit in series strings.
A26	**Electrical Arcing / Arc Fault / Contactor Failure** Switch failures, arcing issues.
A27	**Electrical Design Failure** Overall poor electrical design which may allow for ground loops, floating, voltages, etc., which would force errors.
Threat Barriers – *Electrical Risks*	
B5	**BMS Control** *Includes monitoring and shutdown / isolation capabilities of the affected BMS / module or system.*
B11	**System Shutdown / Disconnect** *Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.*
B13	**Passive Circuit Protection and Design** *Breakers, fuses, or other passive surge arresting elements which may open the circuit in the case of failure and general resilience of design to withstand adverse electrical conditions. Note hazard condition and component and that not all protections apply to a certain failure.*
B14	**Cell Electrical Abuse Tolerance** *Ability of the cell to withstand electrical abuse such as overcharge, over discharge, high currents, or other adverse electrical abuse.*
B17	**Voltage Monitoring** *Overall effectiveness of the voltage monitoring scheme of the system. Includes resilience to errors, error checking, and other measurement intelligence.*

Threat Barriers – *Electrical Risks*	
B18	**Inverter / PCS Controls** *Includes monitoring, shutdown/isolation capabilities, and transient protections.*
B19	**System Electrical Abuse Tolerance** *Refers to ability of the overall system collectively to withstand adverse electrical abuse such as overcharge or dead shorts without failure.*
B20	**Insulation Monitoring** *Continual, or active, monitoring of insulation integrity, ground versus float voltage, and other practices to prevent insulation or isolation degradation.*
B21	**Voltage Monitoring and SOC Estimation** *This may apply at the cell, module, and rack level. While voltage monitoring may be useful, more advanced methods such as coulomb counting may be used as well.*
B22	**BMS Balancing Algorithm / Circuit Sizing** *Ability of the BMS and balancing system to adequately balance the circuit including sizing of the balancing resistors or transistors.*
B23	**BMS Shutdown / Disconnect** *Ability of the BMS to isolate affected modules or strings without shutting down the entire system, if unneeded.*
B24	**Arc Design Protections** *Design considerations intended to limit the ability of arc flash to occur in the system. Also includes proper design and selection of components which are capable of handling such events.*
B25	**Passive Arc Flash Protection** *Physical protections and hardware designed to protect against or to limit arc flash.*
B26	**Human Factors / Process Control** *Quality control or other processes put in place to prevent mishandling of systems that may result in adverse or hazardous conditions or mishandling.*
B27	**System Certifications and Standards Compliance** *Risk assessment and functional safety are key processes for safe deployment of ESS.*
B28	**Design Review and Engineering Best Practice** *In addition to analysis required by product standards, good engineering practice should require design review such that design mistakes and weaknesses are identified and corrected in a timely and efficient manner.*
Consequences – *Electrical Risks*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.
C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.

Consequences – *Electrical Risks*	
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.
C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *Electrical Risks*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data** Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.
D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.
D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.

Consequence Barriers – *Electrical Risks*	
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders** System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.
D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

3.6 External and Environmental Risks

External and environmental risks deal with a multitude of issues which may cause immediate, acute failure within the system or which may accumulate over time, decreasing performance or posing imminent risk. These models mainly focus on systems in use or environmental issues which may occur during normal operating conditions, but also include issues during transportation, construction, and maintenance, when the system is vulnerable by way of deactivated or not yet installed protection systems. Specific barriers may be inactive or ineffective if an incident occurs prior to commissioning of the system.

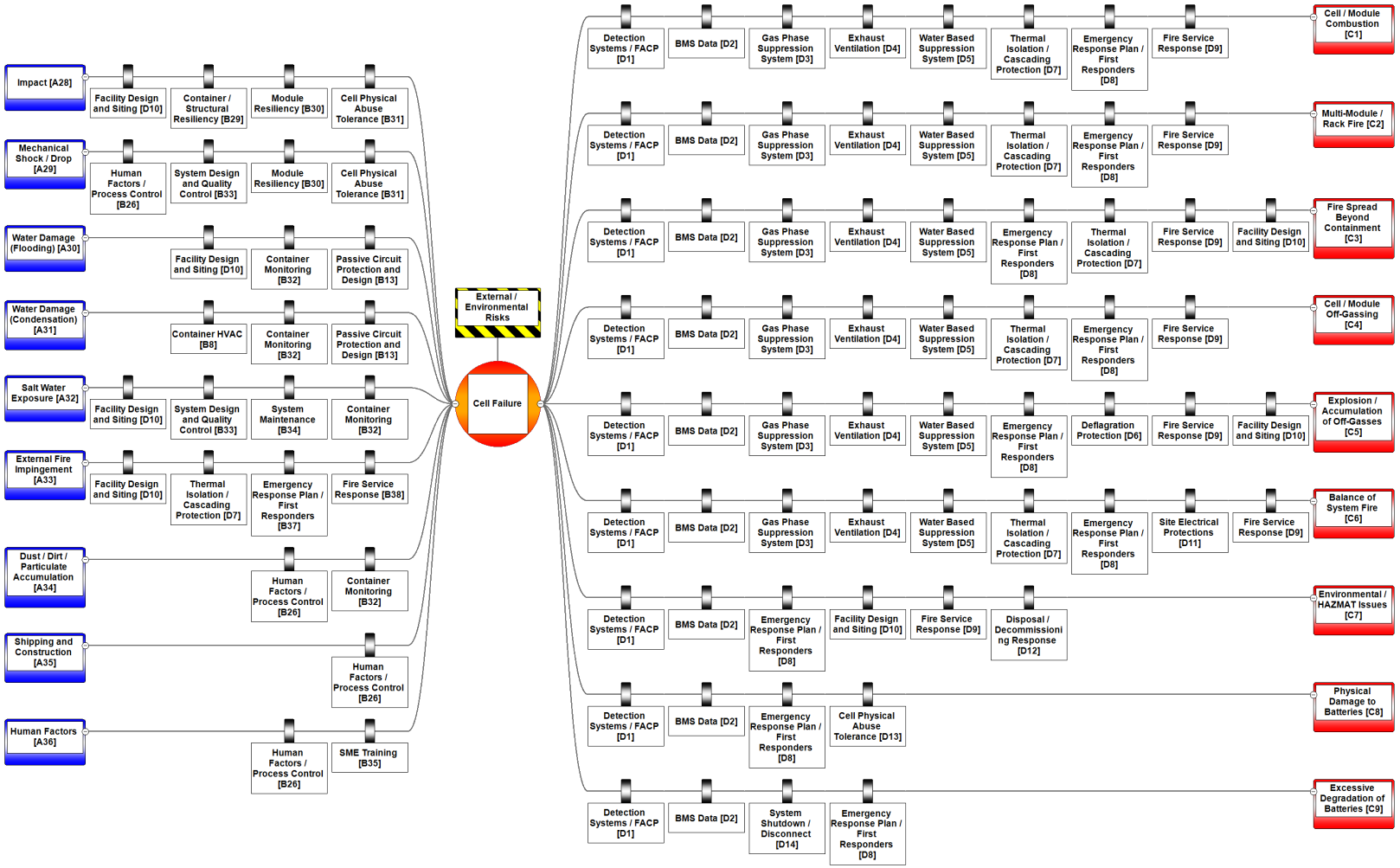

Figure 3-6
External and Environmental Risks

Table 3-6
External and Environmental Risks - Threats and Consequences

Threats – *External and Environmental Risks*	
A28	**Impact** *Something has struck, sharply or as blunt force, the battery system, causing mechanical damage or deformation.*
A29	**Mechanical Shock / Drop** *The system, rack or module is subject to mechanical shock or drop, mechanical jarring or damaging the system.*
A30	**Water Damage (Flooding)** *The system is flooded with water as a result of suppression failure or natural forces.*
A31	**Water Damage (Condensation)** *The system is subject to uncontrolled condensation of water via HVAC failure, inadequate design, internal condensation of moisture, or from natural reasons.*
A32	**Saltwater Exposure** *Long term exposure of the system to salt fog, water, or otherwise salty condition that will result in long term corrosion with electrical activity.*
A33	**External Fire Impingement** *An external fire that is impinging on the system from outside the containment.*
A34	**Dust / Dirt / Particulate Accumulation** *Accumulation of dust, dirt, or particulate that results in an adverse condition inside the system. This could be fan or HVAC failure, shorting, or something else.*
A35	**Shipping and Construction** *An issue occurs with the system during shipping or construction that results in an adverse condition that may or may not be detected or protected via active controls during normal operations. Such an event may include an acute incident which results in cell failure or an event which results in cell failure over a longer time frame but within the time frame of the construction or maintenance event in which full system protections are not active.*
A36	**Human Factors** An adverse condition caused by the result of human interaction, error, or imperfection.
Threat Barriers – *External and Environmental Risks*	
B8	**Container HVAC** *Heating, ventilation, and air conditioning for the overall container designed to maintain overall system temperature and humidity levels.*
B26	**Human Factors / Process** *Quality control or other processes put in place to prevent mishandling of systems that may result in adverse or hazardous conditions or mishandling.*
B29	**Container / Structural Resiliency** *Resiliency of the system and container of the system to withstand impacts or strikes.*

Threat Barriers – *External and Environmental Risks*	
B30	**Module Resiliency** *Resiliency of the individual modules to withstand impacts, shocks, or other mechanical abuse.*
B31	**Cell Physical Abuse Tolerance** *Ability of the cell to withstand thermal, physical, or mechanical abuse.*
B32	**Container Monitoring** *Monitoring within the container which may detect high humidity, water condensation, water leakage, salinity in humidity, and other adverse water conditions.*
B33	**System Design and Quality Control** *Protections, design considerations, and manufacturing QC such that system may withstand such shocks.*
B34	**System Maintenance** *Proper preventative maintenance to minimize the impact of adverse, long term or slow acting environmental effects resulting in degradation.*
B35	**SME Training** *Proper training procedures, availability of subject matter expertise and system competence, and clear jurisdictional hierarchy for managing situations.*
B37	**Emergency Response Plan / First Responders** *System operator plan to handle any and all emergency events external to battery cells from propagating to the cells themselves. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.*
B38	**Fire Service Response** *Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.*
Consequences – *External and Environmental Risks*	
C1	**Cell / Module Combustion** A battery cell or module has failed and is now producing flame or combusting.
C2	**Multi-Module / Rack Fire** Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.
C3	**Fire Spread Beyond Containment** A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.
C4	**Cell / Module Off-Gassing** A cell or module has failed or entered thermal runaway and is now producing off-gas.
C5	**Explosion / Accumulation of Off-Gasses** Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.

C6	**Balance of System Fire** A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
Consequences – *External and Environmental Risks*	
C8	**Physical Damage to Batteries** Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.
C9	**Excessive Degradation of Batteries** As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.
Consequence Barriers – *External and Environmental Risks*	
D1	**Detection Systems / FACP** Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.
D2	**BMS Data** Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.
D3	**Gas-Phase Suppression System** Inert gas or aerosolized gas-based agent designed for fire suppression.
D4	**Exhaust Ventilation** Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.
D5	**Water-Based Suppression System** Water based suppression system including NFPA 13 sprinklers, NFPA 15 sprayers, deluge systems, or NFPA 750 water mist systems designed to suppress fire.
D6	**Explosion Protection** NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.
D7	**Thermal Isolation / Cascading Protection** Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from “initiating” enclosures to nearby enclosures.
D8	**Emergency Response Plan / First Responders**

	System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.
D9	**Fire Service Response** Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.
D10	**Facility Design and Siting** Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.
Consequence Barriers – *External and Environmental Risks*	
D11	**Site Electrical Protections** Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.
D12	**Disposal / Decommissioning Response** Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.
D13	**Cell Physical Abuse Tolerance** Ability of the cell to withstand thermal, physical, or mechanical abuse.
D14	**System Shutdown / Disconnect** Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.

4
CONCLUSION

As the number of energy storage installations – and thus failure incidents – increases across the globe, it is vital that the associated risks are adequately assessed and communicated at all levels of project procurement, deployment, and operations. The hazard scenarios identified by the ESIC Safety Task Force and associated bowtie diagrams outlined in this reference hazard analysis provide a foundational understanding of the primary failure modes and consequences characteristic of lithium-ion ESS and may be serve as useful tools for assessing risk and conveying information to local authorities, fire departments, and other project stakeholders.

Given the limited amount of ESS failure data currently available, it remains difficult to accurately assess the probability of such failures to occur. However, as more testing and future incidents take place, more quantifiable risk assessment approaches may be possible.

While the focus of this report is on lithium-ion battery systems, a similar methodology can be utilized for other emerging energy storage technologies, in which technology-specific threats, consequences, and mitigative barriers are identified and assessed. It is anticipated that these technologies shall be included in future iterations of the ESIC Reference Hazard Mitigation Analysis as they become more prevalent in the market.

A
DETAILED THREAT DESCRIPTIONS

#	Threat Description	Hazard Scenario
A1	**Single-Cell Thermal Runaway** *A single cell has entered thermal runaway resulting in flames and combustion or production of flammable or explosive gases.* Frequently, the scenario described when discussing lithium ion battery safety is a single cell entering thermal runaway as the result of an internal defect, though this is certainly not the only way a cell can go into thermal runaway. Single cell thermal runaway is rarely detectable. If no ignition source is presented, the failure may result in the generation of hazardous and explosive gases that could lead to other hazards. If an ignition source is present, the byproducts may combust and result in fire. Once this event has occurred, it may be managed as a consequence, though may also be managed as a threat with the potential to stop propagation and end the event.	Cell Internal Failure
A2	**Multi-Cell Thermal Runaway** *Multiple cells have entered thermal runaway or begun burning.* Depending on failure mode, multicell thermal runaway is a possibility. Whether the result of the overcharge of a parallel cell group or the early results of a propagating cell failure, multicell thermal runaway is a credible failure mode that should be considered in design as well as in BMS design., Multicell thermal runaway may still prove manageable and containable in some cases and cessation prior to module propagation could allow for preservation of the system without suppression.	Cell Internal Failure
A3	**Internal Defect / Failure (No Thermal Runaway)** *A cell has failed as a result of an internal defect or dendrite formation, creating a short circuit, open circuit, or other electrical condition or off-gas but not entering thermal runaway.* In this instance, a cell may be dead on arrival or may house an internal defect which did not result in thermal runaway but has resulted in the electrical failure of the cell, either by reducing the capacity of the cell relative to its neighbors, creating a dead short or creating an open circuit event. In many cases, cells continue to hold voltage through initial venting prior to thermal runaway and may even cycle somewhat normally. The system may fail to detect the fault. For large parallel systems, the loss of the cell's capacity may mean reduced capacity for that group and balancing issues while a dead short may result in ohmic heat production over time which will heat adjacent cells creating additional failures. Depending on the configuration, a cell failure may result in the opening of the circuit, rendering the entire module or rack useless. It may also increase resistance of the string. A dead short in the cell would result in a noticeable decrease in voltage and could cause other cascading issues.	Cell Internal Failure
A4	**Cell Pressure Buildup** *A cell has begun to build internal pressure as a result of gas generation. The cell has not yet failed or vented this gas.*	Cell Internal Failure
A5	**Degradation / End of Life Failure** *A cell or cells have reached end of life, resulting in an adverse electrical condition which could exacerbate imbalance or other adverse electrical conditions.* The threat posed by premature degradation of a cell is in line with the threats posed by balancing failures, where an imbalance in capacity or performance among cells would	Cell Internal Failure

	require active management to prevent the ever-decreasing capacity from driving the cell group from low SOC to high SOC quickly and would drive further increasing degradation by placing additional work on parallel cells. Battery degradation may also result in increased cell impedance which may increase heat generation.	
A6	**Hazardous Temperature Condition (Cell)** *High temperature at the cell level during normal operations without thermal runaway.* This hazardous temperature threat is a condition in which cells within a module are exposed to high temperatures just short of thermal runaway. This may be the result of hotspots, an HVAC failure, heavy operation, or excessive degradation or increased impedance. Regardless of cause, high cell temperatures pose grave risk to the cell by increasing the likelihood of thermal runaway or increasing cell degradation. More dangerously, increased cell temperatures in poorly sensed or designed modules may go undetected. In other cases, poor module performance may result from slow heat dissipation if proper safety systems limit module operation.	Non-Cell Thermal Risks
A7	**Hazardous Temperature Condition (Module)** *High temperature in the module during normal operation without failure / thermal runaway.* At the module level, inadequate thermal design of the overall system, or poor performance of cooling systems, may result in cases where a module, sets of modules, or entire racks operate at elevated or uneven temperatures relative to other modules or racks within a system. Cells with manufacturing defects or other environmental considerations may also result in elevated cell and module temperatures. In many cases with stationary systems, where individual cell cooling is not performed, modules are the smallest scale which includes some manner of active or passive protection and the first level in which a controlled response beyond shutdown may occur. To this end, barriers against this threat include the effectiveness of detection, cooling systems, and the protection systems as well as their status following emergency situations.	Non-Cell Thermal Risks
A8	**Hazardous Temperature Condition (Room / Enclosure)** *High temperature in the room or enclosure from normal operations.* The largest scale of hazardous temperature condition, dangerously elevated room/container temperatures pose serious risk to system safety. High temperatures through the entire space will equate to high temperatures throughout all modules and thus cells, further increasing the risk of thermal runaway. Non-uniform thermal management means hot spots may be even hotter than usual. Thermal detection schemes may need to account for these conditions, even though the hotspots may exceed detection thresholds more frequently, possibly results in system outages. These events are frequently caused by HVAC failures but may also be the result of poor thermal management of co-located power electronics, intense duty cycles, or environmental conditions such as record high ambient temperatures or fire impingement.	Non-Cell Thermal Risks
A9	**Non-Battery Fire Inside Room / Enclosure** *Fire in container from balance of system that results in dangerously high temperatures inside the enclosure.* A non-battery fire could include wire insulation failing as the result of hotspots, a fire in the power electronics, or fire from another fuel source in the enclosure, such as cardboard boxes or a trashcan. While traditional fire suppression methods should quickly manage the flames, residual heat or delays in activating such methods may result in high heat in the room or high heat exposure for some parts of the system.	Non-Cell Thermal Risks
A10	**Non-Battery Fire Outside Room / Enclosure**	Non-Cell Thermal Risks

	A fire impinging on the outside of the container or a fire in an isolated and insulated part of the enclosure, such as a fire in a PCS room on the other side of a proper fire wall. Depending on the site, an outside fire is likely more common than a non-battery fire inside the container. This would include a power electronics or other failure in an adjacent structure or space separated by a wall. For containerized systems this could also include fire in an adjacent container, fire from an adjacent structure or wild lands fire. This failure is more likely to induce uniform heating on the battery space, or at a minimum increased heating at the rack level, and lead to hazardous conditions at that scale. Beyond typical fire suppression, which may not be effective if the fire remains outside, HVAC and thermal management in the container may delay failure inside the container or space.	
A11	**HVAC Failure** *Mechanical or electrical failure of the HVAC system that will result in high temperatures throughout system.* HVAC failure is a common occurrence in ESS installations. Many ESS integrators and system owner/operators have reported problems related to HVAC failures, typically related to mechanical failures. While some HVAC manufacturers may produce more reliable systems than others, no systems are immune to failure. However, beyond the failure of the HVAC itself, some HVAC designs have been shown to be inadequate. They either create clear temperature gradients across the systems or containers or lack proper redundancy and cannot handle increasingly hot summers and ambient conditions along with the internal heat generated by the batteries' regular operational duty cycles.	Non-Cell Thermal Risks
A12	**Electrical Hotspot / Loose Connection** *Loose connections in the system may increase resistance and cause hotspots. Hotspots may form in other ways for unknown reasons. These hotspots will then conduct via bus bars or mechanical contact into cells.* Electrical hotspots within a device may propagate through thermally conductive busbars and materials, resulting in the direct heating of cells. This is not uncommon in consumer products, though it has not yet the documented cause of failure in large stationary batteries. These systems are increasingly assembled in factories in the US or Asia and then shipped via oceangoing ship, train, or truck, which subjects the systems to vibration, shaking, and shocks and may result in loosening of components. While adequate site acceptance testing may detect these issues, some may be undetectable based on several factors and may also be equally unfixable. In other cases, poor thermal design may result in a battery in which heat is generated or dissipated unevenly, resulting in hot and cold sections of a module or system which may or may not be detected or managed. These imbalances may result in uneven degradation at a minimum or in adverse temperatures which may increase the risk of thermal runaway during cycling. Management of this threat pathway involves proper engineering practices for thermal design, proper commissioning, and maintenance practices to insure proper electrical connections, adequate active or passive thermal monitoring, alarms to stop operation if such conditions are reached and an ability to properly shutdown the system. Some chemistries have shown via testing to be more resilient to thermal abuse than others, but often still require active thermal management.	Non-Cell Thermal Risks
A13	**Inverter Failure** *Inverter or power electronics fail in a way that poses risk to the batteries. Could include a lock up in the "On" position which drives overcharge.* Inverter failure is a common failure mode known to occur with regularity based on IEEE power electronics failure rates. This failure should, as a result of UL standards (UL	Controls Failure

	1741), the National Electrical Code (NEC, NFPA 70), and best practice be easily managed in a properly designed system. However, some systems may lack a physical disconnect point between the battery and the inverter or power control system, a failed inverter could result in a short or other adverse electrical condition.	
A14	**Sensor Failure** *A sensor inside the system fails, resulting in incorrect reporting of system properties.* As control system is only as effective as its ability to measure and provide feedback – the failure of a sensor may result in adverse conditions in a system unable to properly measure its own state. While shown as a single threat in this model, in practice, this threat pathway could and should be repeated for each sensor type to look at how all potential sensor failures could impact the system. This could include separate threat pathways for cell level voltage sensors, module or rack voltage sensors, thermocouples / thermistors in the modules and in the container, current sensors, and any other critical sensors.	Controls Failure
A15	**BMS Failure** *Cell / module level monitoring and control fails, resulting in inability to shut down, report adverse conditions, properly monitor, balance, or protect the system resulting in adverse condition.* Like Sensor Failure, BMS Failure represents a category of threats and threat pathways that may be analyzed as a whole, in aggregate, via a single threat, or split over a number of different specific failure modes/threats depending on the nature in which the modes are mitigated. While Sensor Failure may apply to any number of levels of the system controller and architecture, BMS failure applies specifically to the BMS, which is defined by the fire code as the controller interacting directly with the battery cells. In a containerized system, it most likely exists at the module and potentially rack level. Failures may be software related (e.g., hang up in operation), hardware related (e.g., failure of a balancing circuit or loss of a sensor), or a combination of both where the entire system fails to behave nominally.	Controls Failure
A16	**ESMS Failure** *Failure of the controller at the rack or system level which results in adverse condition to the system.* ESMS failure deals with the Energy Storage Management System as a whole, which is also defined by fire code, or the ultimate aggregation of the controllers at the highest level, which in the case of a containerized system would be the controller of all the racks. The controller is unlikely to handle individual cell response at this level but may function on a binary “go / no go” signal or signals from each rack and is less concerned with small, module level issues where it can simply isolate the affected string or rack and continue to function. This controller, if implemented properly, should also manage string or rack to rack balancing and assess the available capacity of each rack or string under its control. Failure at this level could result in unknown interactions between racks or between the battery and power electronics. As controls at this level are also frequently responsible for mechanical contactors and other parts of the overall system, failure at this level may result in the inability of the system to adequately isolate itself in the case of other failures.	Controls Failure
A17	**Site Control / BoP / BoS / PLC Failure** *Failure of the master site controller or other balance of system controller resulting in adverse condition to the system or inability to detect or protect against adverse conditions under their purview.* While failure of this controller itself is unlikely to result in immediate risk to the system, failure of this controller will likely compromise the ability of the system to adequately shutdown and isolate itself as well as monitor and control interactions between systems. In some cases, if this controller is needed for intervention, failure has likely	Controls Failure

	already occurred or the system is experiencing massive, system wide issues, thus the master site controller may be necessary for adequate isolation from the grid or other AC or DC sources among other actuations. In some architectures, this controller also serves as the interface between systems such as the BMS, ESMS, power electronics, fire control panel, site wide monitoring, and alarm systems and the outside world and may, along with the other individual controllers, be monitored or controlled remotely.	
A18	**Shutdown / Isolation Failure** *Failure of the system to shut down or isolate itself when an adverse condition is detected.* This may be the result of poor design or the result of a failure of electrical or mechanical protections designed to open power circuits within the system. In the case of many currently deployed systems, there are no automated mechanical contacts in the circuit between the power electronics and battery, and the circuit cannot be safely isolated without manual intervention. Shutdown and isolation are key requirements for safe intervention on a failing system, therefore inability to properly shutdown or isolate may impact the ability of the system to stop propagation of electrical-based failures or render itself safe for human intervention.	Controls Failure
A19	**Communications Failure** *Failure of the system to properly report an adverse condition to local or remote monitoring, resulting in adverse condition.* Failure of the communications system can result in failures within the system neither being properly reported internally or externally, or properly managed. A total loss of system communication as a result of a catastrophic system failure would mean no other information about the system was communicated outwards. This would result in poor or complete loss of situational awareness during an emergency, unreported failure, or longer-term damage to the system which may manifest as failure later. Further, though rare, some systems are dependent on communication with a remote-control center for normal operation and would cease to function properly without communication. A loss of communication does not yet have an industry best practice response, with some systems continuing to run for some period of time and some systems shutdown immediately. Neither answer is right or wrong and is dependent on a number of other criteria.	Controls Failure
A20	**Balancing Failure** *Failure of the system at the multicell, module, or rack level to maintain state of charge (SOC) balance, resulting in an unstable or unbalanced system. This may result in premature end of life condition or adverse safety condition.* Electrical component failure or poor design may result in a failure to maintain proper SOC balance of the module, rack, or system. While this failure itself is unlikely to lead to immediate failure, it will likely result in imbalance throughout the system, which will reduce the effective capacity of the system and result in uneven use (and heat generation) through the system, resulting in reduced lifetime and increased “instability.”	Controls Failure
A21	**Hazardous Voltage Condition** *This could include high line voltages, high voltages from the PCS, floating ground issues, or other high voltage issues at the cell, module, or rack level.* In this case, the voltage on the batteries is increased or decreased to unsafe levels beyond the voltage limits. A number of issues could cause either scenario and such scenarios have been directly attributed to large scale ESS fire.	Electrical Risks
A22	**Hazardous Current Condition** *This includes high current issues from the PCS or interconnection.* This condition in particular covers this issue between the power electronics and batteries with adverse current conditions, though not shorted conditions. This event	Electrical Risks

	could be a power electronics failure resulting in higher-than-expected currents during charge and discharge but not greater than the limits of passive protection mechanisms like fuses.	
A23	**Ground Fault / Isolation Fault** *This could include localized shorting of cells, shorting between modules, shorting of entire racks or systems and ground fault shorting.* Unintended ground faults and insulation faults resulting in shorts that produce adverse, high current events. Similar to short circuiting, these events have been directly attributed to large scale ESS fire.	Electrical Risks
A24	**Inadequate Balancing / Balancing Failure** *This includes cells that become imbalanced within a module, modules out of balance with other modules in a string or strings / racks out of balance with the rest of the system. This could be a result of uneven usage, inadequate balancing design, or uneven thermal management.* Similar to the other balancing threats described, this threat is intended to focus on the electrical repercussions of battery imbalance. With differences in states of charge comes differences in voltage depending on architecture. While this can be mitigated with adequate isolation or power electronics, this situation in inadequately designed and managed systems could result in adverse behavior or conditions.	Electrical Risks
A25	**Cell Premature End of Life** *Cell degrades prematurely such that it reduces effective capacity of parallel groups, results in high resistance or open circuit in series strings.* Premature end of life will result in an electrical component acting with drastically less energy capacity than expected, resulting in imbalance, with drastically greater resistance than expected, resulting in thermal issues, or with drastically less resistance than expected, resulting in unintended shorting. In all cases, this loss of life will produce electrical and control instability and likely have an adverse impact, electrically or thermally, to adjacent components.	Electrical Risks
A26	**Electrical Arcing / Arc Fault / Contactor Failure** *Switch failures, arcing issues.* The arc flash potential of a DC system remains unvalidated for voltage and fault current ranges applicable to many stationary energy storage systems. Further, short circuits leading to contactor failure, have been directly attributed to large scale system failures and fires.	Electrical Risks
A27	**Electrical Design Failure** *Overall poor electrical design which may allow for ground loops, floating, voltages, and other adverse electrical effects which would force errors.* Intended as a catch all for any and all bad electrical design practices and failures.	Electrical Risks
A28	**Impact** *Something has struck, sharply or as blunt force, the battery system, causing mechanical damage or deformation.* This is defined as something striking a system (e.g., inadvertent forklift strike or a vehicle hitting the system as part of a deliberate attack). As physical damage to the batteries can result in either immediate or delayed cell failure and fire, such event may pose grave risk if unmanaged and drive protection as required in all fire codes for the system.	External / Environmental Risks

A29	**Mechanical Shock / Drop** *The system, rack or module is subject to mechanical shock or drop, mechanical jarring or damaging the system.* This threat covers the delayed risks from a dropped system as well as issues arising from mechanical shock to a system, such as a sudden jarring force (like an adjacent explosion) or an earthquake. Such an event could result in loosening of electrical connections or other failures and though likely less severe than impact, may still result in adverse conditions, especially delayed issues. Damage from this failure mode is covered by many product standards, such as UL 1973 and UN38.3.	External / Environmental Risks
A30	**Water Damage (Flooding)** *The system is flooded with water as a result of suppression failure or natural forces.* Though frequently placed on raised concrete pylons or engineered pads, systems built in flood planes or below grade are subject water damaged via flooding should it occur. Systems exposed to flooding are at high risk of fire and explosion, as has been observed in both electric vehicles and electric ferries. This damage poses two risks, one from the risk of short circuit, and the other from degradation to components and corrosion from exposure to water.	External / Environmental Risks
A31	**Water Damage (Condensation)** *The system is subject to uncontrolled condensation of water via HVAC failure, inadequate design, internal condensation of moisture, or from natural reasons.* Whether this is condensate building on cool surfaces which falls onto the system, or the formation of condensate on sensitive parts, the presence of water and moisture within electrical systems is not best practice in these systems (outside of intentional liquid cooling systems or those related for damp environments). HVAC issues such as inadequate HVAC, HVAC failures, or poor HVAC design, have been observed in ESS and may result in unintended humidity and the formation of liquid water in the system.	External / Environmental Risks
A32	**Saltwater Exposure** *Long term exposure of the system to salt fog, water, or otherwise salty condition that will result in long term corrosion with electrical activity.* Prolonged exposure to saltwater and saltwater fog is known to cause corrosion on metallic systems. ESS are typically vulnerable galvanic corrosion issues with saltwater exposure and enhanced degradation of exposed terminals and other components. Proper maintenance and monitoring should be performed to ensure system longevity.	External / Environmental Risks
A33	**External Fire Impingement** *An external fire that is impinging on the system from outside the containment.* Systems built near combustible materials, or adjacent buildings are at risk of being exposed to fire should these flammable structures or loads catch fire.	External / Environmental Risks
A34	**Dust / Dirt / Particulate Accumulation** *Accumulation of dust, dirt, or particulate that results in an adverse condition inside the system. This could be fan or HVAC failure, shorting, or something else.* Dependent on location and maintenance, the accumulation of dust, dirt, or other particles may result in eventual failure. Examples include reducing the effectiveness of thermal management, causing failure of moving parts or switches, or creating electrical shorts. While these issues have been theorized to have caused problems leading to fires in systems, this has not been proven conclusively. Regardless, the heavy accumulation of such debris is not in line with best practice and should be avoided.	External / Environmental Risks
A35	**Shipping / Construction**	External / Environmental Risks

	An issue occurs with the system during shipping or construction that results in an adverse condition that may or may not be detected or protected via active controls during normal operations. Such an event may include an acute incident which results in cell failure or an event which results in cell failure over a longer time frame but within the time frame of the construction or maintenance event in which full system protections are not active. This hazard covers more generic damage to the batteries during and construction, maintenance, and shipping which may result in delayed failures during normal operations. While this threat may have a lower likelihood than Impact or Mechanical Shock or Drop, a lack of operational experience with the ESS may introduce other, unforeseen issues as deployment of systems built overseas or at remote facilities and then transported increases.	
A36	**Human Factors** *An adverse condition caused by the result of human interaction, error, or imperfection.* This broad reaching category is intended to cover any accident directly attributable to human intervention. Human factors include any and all variables humans induce in the systems they interact with. Examples include a visitor bumping into a button, switch, or wire; a technician dropping a wrench on terminals; and an operator missing a warning signal.	External / Environmental Risks

B
DETAILED THREAT BARRIER DESCRIPTIONS

#	Threat Barrier Description
B1	**Passive Cell Protections** *Current interrupt devices, fuses, or other passive elements which may open the circuit in the case of failure and general resilience of design to withstand adverse electrical conditions.* In cases where the circuit is unable to adequately isolate itself, such as when no physical disconnect exists, the final barrier to avoiding catastrophic failure is passive circuit elements which may open the circuit at a number of locations. These would include breakers, fuses, current interrupt devices (CIDs), and pressure fuses or diaphragms which open individual cells prior to failure. Depending on the nature of the failure, these elements may have mixed success in achieving these goals. For example, an inverter failure resulting in a short circuit or ground fault may draw sufficient current to trip a fuse or breaker, but an inverter which has lost voltage sensing capabilities may not result in the trip or failure of breakers or fuses because the batteries charge at their normal current rate. In the second scenario, the system could operate well beyond their safe voltage (assuming no active monitoring or control from the batteries) which may drive the cells into thermal runaway if left unchecked. The final passive cell protection barrier resides in the cells themselves, where pressure activated fuses or CIDs would open the individual cell circuits when a pressure increases as a result of gas generation from overcharge tripped the pressure device. These devices are only found in certain cell types.
B2	**Active Cell Protections** *Active cell protections which may mitigate thermal runaway such as module fans, liquid cooling systems, module scale suppression systems, or other mitigation measures.* A wide-ranging category that includes any type of actively monitored or controlled mechanism intended to protect against the effects of thermal runaway, whether it be actively preventing the cell from entering thermal runaway or actively mitigating thermal runaway once it occurs. This could include liquid cooling systems, direct injection suppression systems, fans, or other types of active protection schemes.
B3	**Cell Thermal Abuse Tolerance** *Ability of the cells to withstand thermal abuse without going into failure themselves.* Thermal abuse tolerance applies to the ability of the chemistry in question to fail when exposed to high temperatures. It is typically not considered a strong barrier without sufficient testing to demonstrate. Case by case results suggest some cells of a certain chemistry may resist high temperatures better than other chemistries, but this should not be assumed that this applies to the chemistry as a whole. Additionally, even more thermally tolerant chemistries may not withstand the temperatures of a fire or extreme heating during failure.
B4	**Cell Quality Control** *Overall quality of the cell such that internal defects are minimized and cells maintain rigidity and shape during operations. Also includes tight tolerances with respect to degradation and new capacity.* This barrier is intended as a catch all for considerations related to cell quality. This is likely to be outside the control of the end user of the system but covers the overall reliability of the cells with respect to internal failures and faults that may result in adverse conditions. In many cases, this barrier may be represented as a failure rate, such as 1 in 100 million. It is an exercise for the end user and their suppliers to determine how best to quantify this barrier.
B5	**BMS Control** *Includes monitoring and shutdown/isolation capabilities of the affected BMS / module or system.* BMS Control includes aspects of *BMS Shutdown / Disconnect* but also includes overall effectiveness of monitoring such that proactive measures may be taken, or warnings given, indicating imminent failure or

	adverse conditions. Utilized as a barrier on multiple threats, it is likely this barrier would be evaluated differently in each case based on the algorithmic response to the threat or failure in question.
B6	**Cell Thermal Management** *Active and passive controls put in place to manage cell temperature. Includes passive materials like Phase change material, module fans, liquid cooling system or passive systems dependent on system HVAC.* Effectiveness of cell temperature management, be it active or passive. Intended to cover the overall effectiveness of all (if any) methods employed by the system to manage individual cell temperatures. This could include liquid cooling, conductive or convective active cooling such as thermally regulated plates, or more passive approaches like simple air cooling.
B7	**Module Thermal Management** *Thermal management at the module scale including effectiveness of system HVAC at this level, passive materials, fans, and liquid cooling.* This barrier is intended to cover any active or passive mechanisms which manage the thermal properties of the modules. This could be a module-wide conductive cooling scheme, liquid cooling interfaces within the module, module fans, or other measures which are intended to cool the module as a whole more so than individual cells. Module thermal management may interact with or depend upon an enclosure-wide thermal management scheme.
B8	**Container HVAC** *Heating, ventilation, and air conditioning for the overall container designed to maintain overall system temperature and humidity levels.* HVAC failures have proven to be one of the most common failure modes in ESS and have been identified as the root cause for several of the battery fires in South Korea. While this barrier typically focuses primarily on temperature and managing heating from the electrical load, it should also account for high exterior temperatures and include humidity management and ventilation when the air conditioning is not running. It does not include emergency exhaust ventilation for managing the buildup of explosive gas or deflagration venting. Depending on the HVAC design, the loss of a single unit may result in adverse temperature conditions. Redundant HVAC is an additional barrier to mitigate the impact of the loss of a unit. Further consideration for the effectiveness of the barrier should include evaluation of the restriction of airflow through the unit. A lumped parameter model of heat generation that does not take into account the constricted nature of ESS racks and modules is likely to be inadequate for evaluating performance.
B9	**Redundant HVAC** *Design, sizing, and hardware physical redundancy of the HVAC system such that failure of one or multiple units does not result in adverse conditions within the container or system.* Additional HVAC can be added such that a single HVAC failure or a temperature event does not result in an adverse temperature condition. Multiple HVAC condensers or air handlers not always function as redundant HVAC. If the number of units installed is the number to maintain 100% of the required cooling load, redundancy has not been achieved. Likewise, if HVAC units feed directly into rack or specific modules, then redundant HVAC is unlikely to be effective as a single unit loss still results in a single point of failure unless the effected racks / modules can be isolated. Too much HVAC, however, can pose other issues. For example, an oversized system without proper controls can overcool the batteries (which could result in condensation or other adverse conditions) or at a minimum, result in excessive cycling and auxiliary power consumption by the HVAC.
B10	**Temperature Monitoring and Alarms** *Thermal monitoring within the container including BMS, fire alarm thermal monitoring, and any BoS temperature monitoring.* This barrier is the ability of the battery system or BMS to detect adverse thermal conditions within itself and alarm those issues outward. While many systems claim thermal protection, the presence of a single thermocouple or thermistor within a module may prove insufficient at detecting hot spots. Effective temperature monitoring would include high “resolution” detection of hot spots within a module. While

	measurement of every cell may not be required, monitoring should be done in a manner which offers an ability to detect high temperature zones within the battery.
B11	**System Shutdown / Disconnect** *Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controller's ability to shut down.* In many of the threat pathways, system shutdown and disconnect are provided as barriers against cell failure. In this case, this barrier may be approached from two perspectives, with the first the ability of the system to truly shut off only the affected and responsible operations, namely the battery itself, when such conditions are detected. This shutdown will stop ohmic and electrochemical heating thus stopping heat generation and may also increase the temperature at which thermal runaway would occur (by stopping internal heat generation). The second approach involves shutting down the entire system, including thermal management or cooling systems, when such an issue is detected. Though the coordination of thermal management systems offers benefits to managing system temperature, this coordination, if done improperly, results in the shutdown of the same systems necessary to manage the issue. While ceasing heat generation may be sufficient in many cases for reducing, or stopping, the risk of thermal runaway, deactivating the protection system along with the protected system may result in spreading of the heat and continued exposure to hazardous conditions. An Inverter Failure may trigger physical and electrical isolation of the power electronics from the energy storage system. This can be done by way of a mechanical switch / relay / contactor or any other active hardware component which will physically open the circuit. Electrical components such as FETs, IBGT's, or other power elements in the failed device may not reliably open the circuit as a failure of the device itself may result in failure of other components tied directly to the inverter. System shutdown and disconnect should be done automatically without human intervention, however manual switches may also exist in this protection scheme manual throw switches on individual racks or modules inside the container, E-stop buttons or switches, and remotely activated switches without automatic onsite control should only be considered for this barrier if manned 24/7 and if an alarm indicates a failure requiring response. Many vendors offer switches with view windows to visually verify physical disconnection and hasp mechanisms to lock out the equipment during maintenance, though these may be optional. Beyond the existence of physical disconnect points, the following actuating factors should be considered: Can a module level high voltage alarm result in a disconnect? Does the failure of the inverter result in the opening? If a physical disconnect point exists, but it cannot detect the inverter failure and instead relies on a cell failure before opening, the barrier may not prove effective. While there are likely few if no circumstances in which it is safe to operate without a functioning BMS (BMS Failure), isolation of the affected module in parallel systems or of the rack in serial configurations would allow the remainder of the ESS to operate without the need to shut down the entire system. This may only be accomplished in systems which possess the appropriate degree of control. The shutdown and isolation required following a Sensor Failure can be more complex than an electronic component. The loss of a sensor itself does not guarantee a system behavior that may lead to catastrophic failure, and in many cases the system could continue to operate safely without it. As such, it may not be necessary to shut down an entire ESS container following the loss of a single thermistor if intelligent software and redundant hardware make up for the loss of the input. Further, a complicated isolation or shut down schema may allow for the affected module to be removed from the circuit. While not practical in serially installed systems, multiple parallel racks or modules may allow such isolation depending on system design and the nature of the failure. More in line with inverter failure than BMS failure, a breakdown in function at the system or subsystem level operating on a single inverter is likely to result in the need for full system isolation from the power electronics in addition to isolation of individual strings or racks if power management between them cannot be managed or monitored as needed. It is unlikely isolation of individual strings or racks may correct the problem or result in adequate mitigation of it, and the entire system should be opened to prevent power transfer between racks if maintenance or emergency response is required.
B12	**Preventative Maintenance and Commissioning** *Proper maintenance and monitoring of the system in conjunction with adequate commission and site acceptance testing to reduce likelihood of loose connections or other transportation or construction defects.*

	Preventative Maintenance consists of the normally scheduled preplanned maintenance required for operation such as periodic inspections for function and operating limits, replacement of expendable parts such as air filters, and the necessary upkeep required for continued operation as well as the prompt repair of failures and failing components. Commissioning refers to the process of bringing the system online, performing inspections of the built system to ensure proper compliance with operating parameters, and the shakedown of "bugs" and issues from construction to normal operation. Through these processes, the system is brought to and maintained in good working order. These processes, along with real time monitoring during operation are critical to the error and fault free operation of the system and should be evaluated based on their effectiveness at maintaining such conditions.
B13	**Passive Circuit Protection and Design** *Breakers, fuses, or other passive surge arresting elements which may open the circuit in the case of failure and general resilience of design to withstand adverse electrical conditions. Note hazard condition and component and that not all protections apply to a certain failure.* Passive circuit design considerations at this level aim to minimize pathways between modules or racks in which energy from one may bleed into another during failure, unlike Passive Cell Protections where the holistic design of the system is considered at the cell level. Passive elements under this barrier are likely purely current driven, only capable of protecting against over current events by way of breakers and fuses. Passive design considerations at this level may include circuit design such that the failure of a BMS in one module does not result in an adverse condition in others. An example may include a BMS whose balancing system fails, resulting in short circuits. A poorly designed system may allow for excessive energy to be dissipated through this short by having a common ground that allows energy from other modules to also be dissipated through this failure. This failure mode was identified as a cause of the South Korea fires in 2018 and 2019. As a result of a design failure at the rack level, a ground fault in the rack was discharging the entire serial system, putting thousands of amps through a system designed for a few hundred amps.
B14	**Cell Electrical Abuse Tolerance** *Ability of the cell to withstand electrical abuse such as overcharge, over discharge, high currents, or other adverse electrical abuse.* The ability of the individual cells to withstand electrical abuse such as short circuit, overcharge, and overcurrent events without resulting in adverse conditions. This should not be considered a strong barrier. This barrier may include passive elements within the cells, as well as the cells' electrochemical ability to withstand these events. While some chemistries have shown more resilient to thermal exposure than others, it is less clear how those same chemistries withstand electrical abuse. As no testing standard yet exists to quantify the ability of the cell to withstand electrical abuse, this barrier, without consideration for passive elements, should typically be evaluated as weak.
B15	**Redundant Failure Detection / System Intelligence** *Ability of system to determine a sensor has failed, to operate safely without that sensor to shut down, or operate safely indefinitely without sensor. This may include Checksums, additional sensors, or the ability to pull data from other sensors.* This barrier is highly dependent on the sensor in question as well as the design, architecture, and operation of the system as a whole and the evaluation of the data collected within the confines of the system. As referenced in the definition, the loss of a cell level voltage sensor could be made up by comparing the known surviving voltage sensors with the total module voltage, allowing for the calculation of the cell voltage in question. While less than ideal, this method could be used to keep the system online during emergency situations or until maintenance can be performed. In another circumstance, rather than risk shutting down the system for a potential false negative, false positive, or other failed signal, redundant detection compared against similar sensors may allow sensor failure to be ignored and operation to continue. As an example, a high temperature signal without an accompanying high voltage signal could indicate a thermocouple failure, but a third sensor, such as an off-gas detector, IR, or additional voltage sensor could alert the system to a sensor failure and allow continued safe operation. This barrier may actually exist as multiple barriers in some systems, where both redundant sensors act as a hardware backup while intelligent software may also detect this failure digitally and devise a method for working around it safely.

	If the system is poorly designed, lacking such redundant capability with no mitigating protection, a BMS failure, whether hardware or software, may equally result in the Top Hazard Failures at the EMS level are unlikely to be mitigated by redundant sensors or detection systems. At this level, failure of this controller is likely handled by the balance of system PLC or the fire control panel which would issue a shutdown signal to the entire system, attempt to isolate the AC-DC circuit, and potentially open any utility connection such as a re-closer.
B16	**Adequate Sensing and Control** *Aggregate of the ability of the BMS to detect cell imbalance and to properly return system to balance if possible, including adequately sized passive or active balancing scheme.* This covers the overall "resolution" of data acquisition within a battery system including the ability of the system to reliably detect voltages and verify those measurements for the purpose of avoiding false positives. Sensors can be sensitive to ground faults and other errors. Therefore, the inability to identify a failure and initiate response can result in extremely adverse consequences such as over charge, over discharge, and improper balancing.
B17	**Voltage Monitoring** *Overall effectiveness of the voltage monitoring scheme of the system. Includes resilience to errors, error checking, and other measurement intelligence.* This includes adequate measurement of voltage throughout the system coupled with checks or redundant measurements such that a sensor failure cannot drive the system to an adverse condition. This includes monitoring of module, rack, and bus levels DC voltages as well as AC line voltages and any intermediary voltages.
B18	**Inverter / PCS Controls** *Includes monitoring, shutdown/isolation capabilities, and transient protections.* For electrical risks, this covers much of the inverter's ability to a manage adverse conditions as tested in UL1741 and less about the ability of the inverter or PCS' intelligence to detect adverse related to controls (such as an adverse current condition which is otherwise within an acceptable current range).
B19	**System Electrical Abuse Tolerance** *Refers to ability of the overall system collectively to withstand adverse electrical abuse such as overcharge or dead shorts without failure.* This considers passive design, any additional technologies or approaches which may manage adverse electrical behavior, and overall resiliency of the design such that hazardous or adverse conditions within the electrical system are mitigated prior to becoming hazardous to the batteries.
B20	**Insulation Monitoring** *Continual, or active, monitoring of insulation integrity, ground versus float voltage, and other practices to prevent insulation or isolation degradation.* Insulation monitoring is a common electrical maintenance best practice. Degradation of insulation for any reason runs the risk of current related failures anywhere in the system. This includes not just wire insulation but isolation on components and effectiveness of ground isolation during normal operation.
B21	**Voltage Monitoring and SOC Estimation** *This may apply at the cell, module, and rack level. While voltage monitoring may be useful, more advanced methods such as coulomb counting may be used as well.* Voltage monitoring or other techniques at the cell, module, and rack level may be used to measure SOC. Voltage and SOC measurements are key to the safe and efficient operation of the system, therefore the ability to determine this state reliably is necessary for operation. SOC estimation is essential for monitoring capacity of the system and for de-rating the system should temperature conditions require such a response. Rapid, unexpected changes in capacity could also be indicative of failures in the system. Should SOC estimation be a function purely of voltage, failures of the voltage sense would also result in inaccurate SOC estimation, potentially allowing the system to exceed certain protection limits again depending on the architecture of the system.

B22	**BMS Balancing Algorithm / Circuit Sizing** *Ability of the BMS and balancing system to adequately balance the circuit including sizing of the balancing resistors or transistors.* Similar to *Adequate Sensing and Control*, BMS balancing is related to the effectiveness of the balancing circuitry to manage balance of voltage between cells, modules, and racks. Unlike the previous barrier though, this barrier is related to the actual balancing algorithm itself, as well as the effectiveness of the hardware to balance the system. As an example, some systems possess passive resistors for balancing, but these resistors are capable of balancing less than .05% SOC in an hour, which would be critically ineffective in the case where a cell started degrading quickly.
B23	**BMS Shutdown / Disconnect** *Ability of the BMS to isolate affected modules or strings without shutting down the entire system, if unneeded.* BMS shutdown and disconnect is focused primarily on the ability of the system, while still active, to isolate itself or effected components while maintaining normal operation. Rather than rapid opening of emergency contactors and shutting down the entire system as in *System Shutdown / Disconnect*, a BMS shutdown may be thought of as a soft shutdown, or standby state where the only affected modules or racks are isolated. Ideally, the BMS, while maintaining function, should return these components to function when the event has been cleared or corrected.
B24	**Arc Design Protections** *Design considerations intended to limit the ability of arc flash to occur in the system. Also includes proper design and selection of components which are capable of handling such events.* Protections in the system, as required by local codes and safety best practice, to avoid arc flash or mitigate the effects if it occurs. While arc flash poses a greater risk to humans, the energy released could cause adverse damage which may further drive other failure modes.
B25	**Passive Arc Flash Protection** *Physical protections and hardware designed to protect against or to limit arc flash.* Passive arc flash protection is common design feature used to protect against arc flash in the AC and DC equipment and could be based on NFPA 70E requirements or other local or organizational electrical protection codes. While the supporting equipment (switchgear, contactors, balance of plant subsystems) may withstand the heat and current of an arc flash (blowing fuses and throwing breakers), the batteries themselves may be adversely affected by heat and potential projectiles should the arc flash occur near the batteries. Further, the current event itself, which may be on the order of several thousand or tens of thousands of amps may also unduly stress the batteries.
B26	**Human Factors / Process Control** *Quality control or other processes put in place to prevent mishandling of systems that may result in adverse or hazardous conditions or mishandling.* A catchall barrier that includes all possible failures and adverse conditions brought about by human interaction with the system. It also includes failures related to process and flow separate from the control system of ESS itself. This could be as simple as a technician dropping a wrench across the terminals or as complex as sophisticated maintenance procedure which fails to adequately address an otherwise trivial detail, such as failure to check the tightness of unreachable bolts or clean unexposed terminals.
B27	**System Certification / Standards Compliance** *Risk assessment and functional safety are key processes for safe deployment of ESS.* Throughout UL1973, UL9540, UL1741 and other US standards are a number of requirements for product analysis and review including failure mode and effects analysis (FMEA), safety integrity level (SIL) / layer of protection analysis (LOPA), and other failure modes and safety analysis. While the product standards themselves usually cover the minimum requirements for safety, the analysis required by the standard may serve as a basis for additional review and may indicate additional failure modes not tested for in the

	standards or covered exhaustively by this guide. Compliance with these standards, by fire code and best practice, shall be requisite for operation of an ESS and while compliance with those standards does not ensure strong barriers where relevant, data from the tests may be used to inform this analysis.
B28	**Design Review and Engineering Best Practices** *In addition to analysis required by product standards, good engineering practice should require design review such that design mistakes and weaknesses are identified and corrected in a timely and efficient manner.* This catchall barrier includes any and all engineering best practices, recommended best practices, standards of care, review process and analysis which are used to ensure a system is engineered to the best possible state based on realistic or practical expectations.
B29	**Container / Structural Resiliency** *Resiliency of the system and container of the system to withstand impacts or strikes.* While this depends on the threat and Facility Siting and Design, the enclosure envelope should be effective to protect against basic vandalism or low speed, accidental vehicle impacts such as construction equipment as well as high winds, hail, seismic vibrations, and other environmental forces.
B30	**Module Resiliency** *Resiliency of the individual modules to withstand impacts, shocks, or other mechanical abuse.* Similar to cell abuse tolerance, this barrier covers the overall strength and rigidity of a battery module as it relates to the ability of the module to withstand both impacts and shocks as well as the noise, vibration, and harshness which may be encountered over an ocean voyage or transportation in a semi-truck. Unlike cell abuse tolerance, which shouldn't be considered a strong barrier, module resiliency may be built in as part of commissioning with confidence that the modules should withstand transportation, maintenance, and construction without requiring reinspection. Regulations provide certification under UN38.3 that can be referenced for levels of resiliency during transportation for a certified product.
B31	**Cell Physical Abuse Tolerance** *Ability of the cell to withstand thermal, physical, or mechanical abuse.* This barrier considers the ability of a cell to withstand physical, thermal, or mechanical damage without resulting in an adverse condition. As all lithium ion battery chemistries have shown susceptibility to physical damage such as penetration and crush, this barrier is likely to be considered weak, depending on the threat faced. Some consideration may be given to the cell casing (e.g., cells comprised of hardened cases such as prismatic cells compared to a softer pouch cell). However, the threat faced will ultimately determine the effectiveness of the case as even many prismatic cells will not survive ballistic penetration, vehicle impact, or crush.
B32	**Container Monitoring** *Monitoring within the container which may detect high humidity, water condensation, water leakage, salinity in humidity, and other adverse water conditions.* In addition to the sensors, this barrier includes intelligence in the measurements which allows for prompt determination of adverse conditions, such as high humidity or dust, which poses a corrosion or electrical risk.
B33	**System Design and Quality Control** *Protections, design considerations, and manufacturing QC such that system may withstand such shocks.* A catchall barrier related to the overall quality of the build of the container, the integration of the system into the container, the ability of the system to withstand noise, vibration, and harshness (NVH) during transport and the overall design of the system for maintenance, construction, and transportation. This may also include container coatings and durability against degradation due to UV exposure, weather, and corrosion.
B34	**System Maintenance**

	Proper preventative maintenance to minimize the impact of adverse, long term or slow acting environmental effects resulting in degradation. Includes normally scheduled maintenance required for operation including periodic inspections for function and operating limits, replacement of expendable parts, and any necessary upkeep required for continued operation. Also includes prompt repair of failures and failing components.
B35	**SME Training** *Proper training procedures, availability of subject matter expertise and system competence, and clear jurisdictional hierarchy for managing situations.* Though required by fire codes such as NFPA 855, subject matter expert (SME) remains an undefined term and the quality and title of SMEs across the industry varies wildly. In addition to the undefined term, there is no nationally recognized standard or methodology for training or credentialing subject matter experts. In some cases, the SME may be more critical to the response of an ESS emergency than the first service, because the safety of the first responders and fire fighters also depends on the SME. This role should be evaluated carefully by all stakeholders when selecting an SME.
B36	**Fire Suppression** *Fire suppression inside battery compartment which may address BoS fire without adverse effect on batteries. Potentially separate from battery fire suppression.* Fire suppression as a threat management barrier deals with management of non-battery fires and the effective suppression of these fires before they can impact the battery itself. Further, it deals with the ability of this suppression approach to manage the non-battery fire in a way that does not compromise the battery, such as by dousing it with saltwater or exposing it to caustic substances which may cause degradation. However, fire suppression system discharge may be grounds for voiding the warranty, depending on the specific contract language. See Gas Phase Suppression System [D3] and Water Based Suppression System [D5] for fire suppression as a consequence barrier.
B37	**Emergency Response Plan / First Responders** *System operator plan to handle any and all emergency events external to battery cells from propagating to the cells themselves. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.* See D8 for full description with regards to Emergency Response Plan / First Responders as a consequence barrier.
B38	**Fire Service Response** *Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.* See D9 for full description with regards to Fire Service Response as a consequence barrier.

C
DETAILED CONSEQUENCE DESCRIPTIONS

#	Consequence Description
C1	**Cell / Module Combustion** *A battery cell or module has failed and is now producing flame or combusting.* A single cell failure resulting in combustion and flame is likely the result of thermal runaway. While several mitigating barriers exist to prevent this scenario from reaching its natural conclusion, should those barriers fail, it is possible this consequence will continue, evolving into any of the consequences listed in this section. Furthermore, spread to other nearby cells or modules may continue the propagation of failure throughout the system.
C2	**Multi-Module / Rack Fire** *Multiple modules have begun burning, resulting in a growing fire which may overcome internal suppression capabilities.* Fire within multiple modules or racks. Fire at this scale may be the result of propagation from a smaller event and may indicate failure of the suppression systems to contain it. As such, fire at this scale will be more dependent on the fire fighter response. Defensive postures may be needed to protect external exposures if firefighters struggle to reach the affected systems and manage the fire directly. Depending on system size, this fire may burn for several hours.
C3	**Fire Spread Beyond Containment** *A fire within the system has spread beyond the system containment, be it the container, room, or purpose-built structure.* In this case, fire has likely compromised the entire interior space of the enclosure or container and has now breached the container, posing immediate risk to adjacent equipment or facilities. Defensive firefighting is required while the nature of the breach is assessed to determine ability to use the opening to get suppressant into the container. A fire of this scale may burn for several hours.
C4	**Cell / Module Off-Gassing** *A cell or module has failed or entered thermal runaway and is now producing off-gas.* Battery off-gas is often highly flammable and typically consists of hydrogen, carbon monoxide, methane, and other flammable hydrocarbons. As such, this event may pose even greater risk than a single cell combustion, as the ability of batteries to maintain high temperatures in excess of autoignition temperatures for hours is well documented and the electrical nature of the systems adds additional ignitions sources. Poor air management may also result in delayed ignition scenarios when oxygen rich air is introduced into the space later. While small cylindrical cells may pose reduced risk by nature of their size, large format cells may possess enough electrolyte, and ultimately gas generation potential, to create a highly flammable environment from only a single cell. Similar to single cell failure with off-gas, an explosive mixture is likely to exist in the container. While this event may not directly result in module-to-module thermal runaway propagation, preliminary modeling in some systems has shown that a single module failure may still result in a uniformly explosive vapor cloud in a containerized system. As such, this failure may pose one of the greatest risks to first responders as the failure mode will create an explosive, oxygen depleted atmosphere potentially lacking the heat required for exterior detection or to drive smoke out of the system and provide warning of the environment inside.
C5	**Explosion / Accumulation of Off-Gasses** *Cell or module failure which may or may not have propagated has resulted in the accumulation of potentially explosive off-gas within the containment.* Even with a single cell, long after the risk of propagating failure has passed, off-gas may continue to linger in the area, especially in confined, poorly ventilated spaces. This gas may continue to pose deflagration risk. Even cooled or extinguished batteries may emit gas several hours following an event.

	The lack of ventilation observed in some systems means the ability to exhaust this gas may be lacking or nonexistent. The quantity of the gas itself, coupled with some common suppression methods, may result in oxygen depleted environments which make emergency response challenging or dangerous without adequate situational awareness.
C6	**Balance of System Fire** *A fire from a cell or multiple cells which results in a balance of system fire such as wire insulation, electrical components, or plastic inside the system.* In this instance, a small fire, results in damage to the balance of system, including wiring insulation, bus bars, plastic containment or other component or material. Such damage may pose significant risk as compromised wiring or components may result in arcing, shorting, or other high energy event or act as ignition source causing delayed fire or explosion.
C7	**Environmental / HAZMAT Issues** A large-scale system fire has resulted in an environmental or hazardous material incident which requires hazardous material response. Examples include toxic smoke / gas plumage, contamination of firefighting runoff water in a sensitive area, or leftover energetic hazardous materials which may require special handling.
C8	**Physical Damage to Batteries** *Batteries are subject to thermal, electric, or physical abuse which would make their continued use subject to higher risk.* In this case, physical damage includes mechanical, thermal, or electrical which may compromise the cell, leading to any of the failure modes discussed above.
C9	**Excessive Degradation of Batteries** *As a result of adverse conditions, batteries are subject to increased rate excessive degradation which will result in premature end of life.* SOH degradation and imbalance or any drastic change in electrical performance of the battery as a result of damage could create a number of problems with the operation of the battery.

D
DETAILED CONSEQUENCE BARRIER DESCRIPTIONS

#	Consequence Barrier Description
D1	**Detection Systems / FACP** *Includes heat, smoke, and gas detection systems, as well as other Fire Alarm Control Panel (FACP) / NFPA 72 devices. Effectiveness based on what is detected and how well, how information is conveyed, and robustness of sensors in case of failure.* This is an example of a barrier that is less a physical barrier and more a multiplier to the other barriers in the pathway. The effectiveness is based on the ability of the system and site to provide information and clarity of the failure. Poor situational awareness may weaken subsequent barriers in the same manner. As an example, firefighter response hampered by a lack of data may result in excessive propagation of a fire when earlier intervention may have saved greater portions of the system. This barrier consists of whatever data is available from within the energy storage system, (e.g., temperature, system voltage, SOC, currents, and connection status), as well as information from the fire control panel (e.g., smoke alarm status, thermal alarm status, gas detection, off-gas detection, and suppression status), and information from any third-party monitoring systems including separate gas and visual monitoring systems. In all cases. it is dependent on proper annunciation of this data on site or the availability of this data to first responders and operations personnel. It also includes knowledge available at the site in the form of subject matter experts (SMEs), site personnel, emergency response experts available via phone, and any additional knowledge which may be gained from within the system visually or digital documentation. All of this information is necessary for maximizing the efficiency of each subsequent barrier, whether it is automated or driven by human factors.
D2	**BMS Data** *Includes BMS measurements available to first responders, Network Operations Center (NOC), or other SMEs. Effectiveness based on what is detected and how well, how this information is being conveyed, and robustness of sensors in case of failure.* In the event of a failure event, BMS data may be available via Network Operations Center (NOC) or otherwise communicated to first responders. This information may provide insight into the current conditions of the system (e.g., temperature of cells / modules, SOC, voltage trends, etc.) – provided the system is still online – or the state of the system prior to loss of measurements. It should be noted that the NOC personnel or SMEs responsible for communicating the measurements to first responders should be well trained in the functionality of the BMS, the data points available, and able to extract actionable insights from the information provided by the BMS.
D3	**Gas-Phase Suppression System** *Inert gas or aerosolized gas-based agent designed for fire suppression.* Gas phase suppression systems have been installed, many at the factory, in a number of systems deployed around the world. The intent is to provide fire suppression capability in lieu of installing a water-based system which would require additional, and potentially costly, plumbing. The “tradition” of installing these systems has persisted even after initial test data suggested they may not properly address fire in the batteries themselves in their current configurations. Gas based systems, which may be effective against “balance of system” or non-battery fires, may be backed up by water-based suppression for fire in the batteries and supported by adequate ventilation to promptly remove the agent if it is ineffective at suppression (i.e., the system continues to increase in temperature). The concern around gas phase agents, is the explosion risk they may introduce. Suppressing combustion with a gas phase suppressant without controlling thermal runaway propagation allows for off-gas generation while depleting oxygen levels. Affected batteries, which may remain hot for hours, could provide an ignition source if oxygen is reintroduced back into the space.

	Without large-scale fire testing to support it, gas phase agents should not be considered a strong or effective barrier against battery fires. However, they are expected to perform adequately against other fires in the battery space and may, in limited cases, manage convective heat propagation. Additionally, gas-based system discharge may be grounds for voiding the warranty, depending on the specific contract language.
D4	**Exhaust Ventilation** *Effectiveness of exhaust ventilation to remove battery off-gas, heat, and smoke which may result in adverse atmospheric conditions.* ESS failures often produce an immense quantity of gas. While numbers vary as additional data comes available, proprietary testing to date has shown the gas produced per unit of energy is approximately on the order of 1-3 liters/Ah during pre-combustion thermal runaway. The concern is the explosive nature of this gas, which is oxygen depleting (based on volumetric ratio) due to the quantity released, especially in confined spaces. This gas is prone to stratification as well depending on failure mode, temperature, and ventilation effectiveness. This explosive risk is compounded by the fact that pre-combustion off-gas is composed heavily of hydrogen gas, which becomes explosive at 4% concentration and is prone to high-pressure deflagration and potentially detonation. As a result, these events have proven difficult to manage, and even labs and test facilities, staffed by experts in safety and destructive testing, have still experienced explosions and other loss of control situations despite best efforts and past experiences. With these facts considered, exhaust ventilation is critical to managing an energy storage incident. Many jurisdictions require compliance with NFPA 68 (Standard on Explosion Protection by Deflagration Venting), and best practice would suggest that designs also incorporate measures to reduce the level of flammable gas in the enclosure via ventilation to avoid the explosion, It should be noted that even with ventilation, the tight confines within an ESS can create areas of poor air flow, and localized explosions within a system are possible where small pockets of gas build up from even a single cell failure. Further, while not yet demonstrated via additional large-scale testing, preliminary test results indicate that automated, water-based suppression may be more effective at managing energy storage fire when used in conjunction with effective exhaust ventilation. Effective exhaust barriers require right-sized penetrations in the container designed with consideration for the specific chemistry and failure test results of the specific energy storage product for that site. The solution may require self-opening mechanical louvers, small exhaust fans used for temperature control, and pressure relief louvers directed outward and upward from of the container capable of handling the high flow rates needed during wider scale failure.
D5	**Water-Based Suppression System** *Water-based suppression system includes systems covered under NFPA standards NFPA 13 for sprinklers, NFPA 15 for sprayers, deluge systems, or NFPA 750 for water mist systems designed to suppress fire.* This suppression agent is the only suppression methodology prescriptively called out in the fire code. Automated water-based suppression has been shown to be capable of managing the heat exposure which can reduce the risk posed to adjacent exposures and objects. While test data is lacking, preliminary research shows that suppression systems may more effectively manage battery fires by spraying water directly into the effected systems. Though the heat released by lithium ion battery systems is high, it is the gas production, deep seated nature of the fire, and the tight, densely packed, and protected structure of the systems that makes extinguishment difficult. While not 100% effective, as re-ignitions have occurred in preliminary testing, water has been shown to be the most effective agent for managing ESS fires by removing the heat generated.
D6	**Explosion Protection** *NFPA 68, NFPA 69, or other deflagration protection based on UL9540A test results.* Deflagration or explosion as a result of combustion, expansion, or detonation, poses severe risks to life and property near an ESS. The off-gas emitted by all lithium ion batteries with an organic electrolyte is composed primarily of hydrogen, carbon monoxide, carbon dioxide and flammable hydrocarbons. Therefore, the release of gas from even a small number of cells can pose significant danger. As a result, many fire codes now require deflagration protection designed with system-specific test results from product standards tests such as UL 9540A. While systems going into the field in compliance with this code should

	have this barrier as a strength, many systems in the field today lack even a basic ability to protect themselves from this buildup of explosive gas or ability to withstand the actual deflagration itself.
D7	**Thermal Isolation / Cascading Protection** *Passive protection and thermal insulation that will limit thermal propagation not only between cells and modules within a rack or enclosure, but also from "initiating" enclosures to nearby enclosures.* This includes all protections between battery modules and/or racks which would limit the propagation of a fire outward to other modules / racks and likewise protect modules / racks in the case of external (or internal) fire which may impinge on the batteries. This does not include active suppression systems but instead covers protections such as passive barriers and materials, non-flammable plates, intumescent materials, and intelligent designs which include gas routing and other design features which manage heat release and absorption. A greater emphasis has been placed on cascading protections after recent high-visibility incidents in which fire spread to multiple ESS enclosures.
D8	**Emergency Response Plan / First Responders** *System operator plan to handle any and all emergency events. Effectiveness based on level of SME / first responder training, knowledge of the specific ESS undergoing failure, coordination with fire department, etc.* First responders refer to site personnel, corporate employees, local technicians, and subject matter experts (SMEs) who may be the first to detect or respond to failure or fault in the system and alert fire services. The term first responders in this case does not refer to fire fighters or other fire service personnel, but to those who will be reporting the event or directing the fire service in regard to the risks posed by the system. The guidance from these individuals, as well as the information contained in the emergency response plan, will serve as the initial human response to the incident and have the greatest chance of containing the incident, if it is containable, to a reduced state. Depending on time to detection, along with time to first response and fire service response, the incident may have progressed through multiple consequence pathways, as single cell failure can propagate to adjacent modules in beyond in a matter of minutes. The emergency response plan should address how these first responders, as well as the fire service, react to emergencies within the system. This may include a separate alarm management plan to address which information is essential for responders, critical thresholds of parameters, and potential hazards indicated by the alarms. The first responder's familiarity with the document as well as the overall effectiveness of the document may add or remove minutes or seconds to the response. Therefore, both the emergency response plan as well as the competence of the SME should be evaluated with respect to their effectiveness in interacting with the fire service. First responders may lack experience both with the technology and emergency response and the industry currently lacks best practices in formalized training and standard curriculum.
D9	**Fire Service Response** *Fire department response including active firefighting suppression. Effectiveness based on level of department knowledge and training to effectively respond both offensively and defensively during an ESS incident.* This barrier includes all aspects of the fire service response including the personnel, resources, knowledge, and overall comfort level brought to bear on the scene. Current industry training and emergency response planning point toward automatic dispatch of multiple trucks or departments/stations for ESS emergencies or multiple alarms in some jurisdictions. In these cases, clear incident command is necessary to ensure that departments properly trained on the system are able to drive response. Further, fire service response will be supported by SMEs, whose own knowledge can drastically impact the fire service response. Finally, situational awareness (e.g., Detection Systems / FACP) will act as the final multiplier, resulting in decisions which may save the currently impacted or adjacent systems or result in the loss of the entire project.
D10	**Facility Design and Siting** *Placement of the facility such that adverse environmental effects such as flooding, vehicle impact, and fire impingement are mitigated or avoided. Likewise, placement such that adverse effects from the system are limited to exposures.*

	This barrier is intended to include analysis of the system in its location with respect to localized environmental hazards, adjacent structures, fire loads, and personnel exposures, and other generic environmental threats either to the system as posed by the environment or to the environment as posed by the system. While a specific spacing may be suitable for most ESS, it may not be sufficient spacing from a large fuel storage depot or an ambulatory care facility. Further, proper siting should include the type of environment the system is built in such as a flood plain, a high traffic area, a wetland, or an area prone to fire.
D11	**Site Electrical Protections** *Protection for electrical systems such that a failure of the PCS or associated circuit does not result in adverse effects on the site balance of system electrical gear.* Includes site electrical protection measures noted in Electrical Risks and Controls Failure hazard scenarios.
D12	**Disposal / Decommissioning Response** *Combination of disposal and hazmat pre-planning and hazmat response on site. Dependent on nature and sensitivity of surroundings.*
D13	**Cell Physical Abuse Tolerance** *Ability of the cell to withstand thermal, physical, or mechanical abuse.* See B31 for full description.
D14	**System Shutdown / Disconnect** *Ability of system to actively shut itself down or disconnect itself. This is the aggregate of the BMS or inverter's shutdown ability as well as physical disconnects and the BoS controllers ability to shut down.* See B11 for full description.

E
ATTACHMENT

Bowtie Threats Consequences and Barriers Matrix

Bowtie Threats Consequences and Barriers Matrix

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together…Shaping the Future of Energy™

3002023089

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com