

System Level Safety Design and Planning



PRESENTED BY

David Rosewater - 09 - 30 - 2020

Project Team: David Rosewater (PI), Joshua Lamb, John Hewson, Vilayanur Viswanathan, Matthew Paiss, Daiwon Choi, Abhishek Jaiswal

SAND2020-9887 C



- Background and Objective
- Methods (Systems Theoretic Process Analysis)
 - Losses and Hazards
 - Safety control actions and Unsafe control
 - Loss scenario identification
- Results
 - Design objectives

Objective

Safe Deployment of Energy Storage Technologies

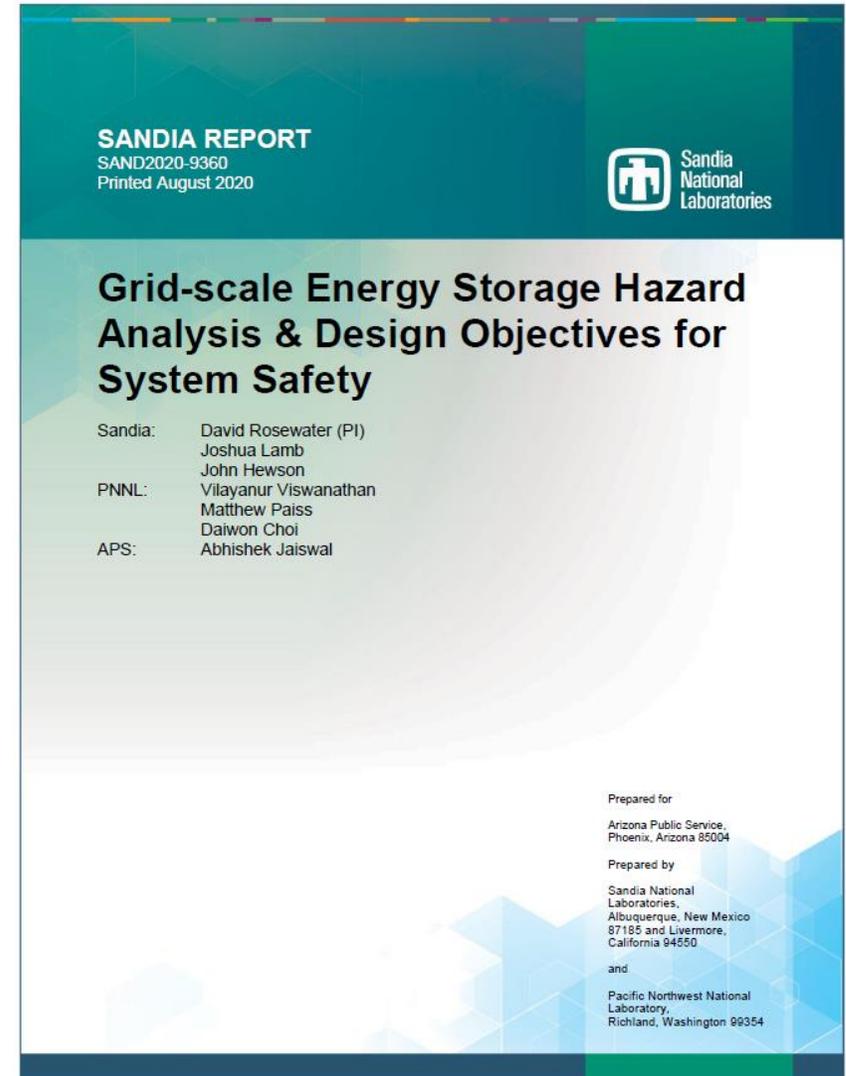
Objective

The objective of this research is to prevent fire and explosions in lithium-ion based energy storage systems. This work enables these systems to modernize US energy infrastructure and make it more resilient and flexible (DOE OE Core Mission).

The primary focus of our work is on lithium-ion battery systems. We apply a hazard analysis method based on system's theoretic process analysis (STPA) to develop **“design objectives” for system safety**. These design objectives, in all or any subset, can be used by utilities “design requirements” for issuing requests for proposals (RFPs) and for reviewing responses as a part of their procurement process. The design objectives can also serve as model standards for standard development organizations (SDOs) to consider in the course of their consensus-based work.

Similar Efforts:

- NFPA 855, Standard for the Installation of Stationary Energy Storage Systems
- UL 9540 Ed 2, ANSI/CAN/UL Standard for Energy Storage Systems and Equipment
- FDNY: 2020 NYC Fire Code –Section 608 STATIONARY STORAGE BATTERY SYSTEMS



Methods

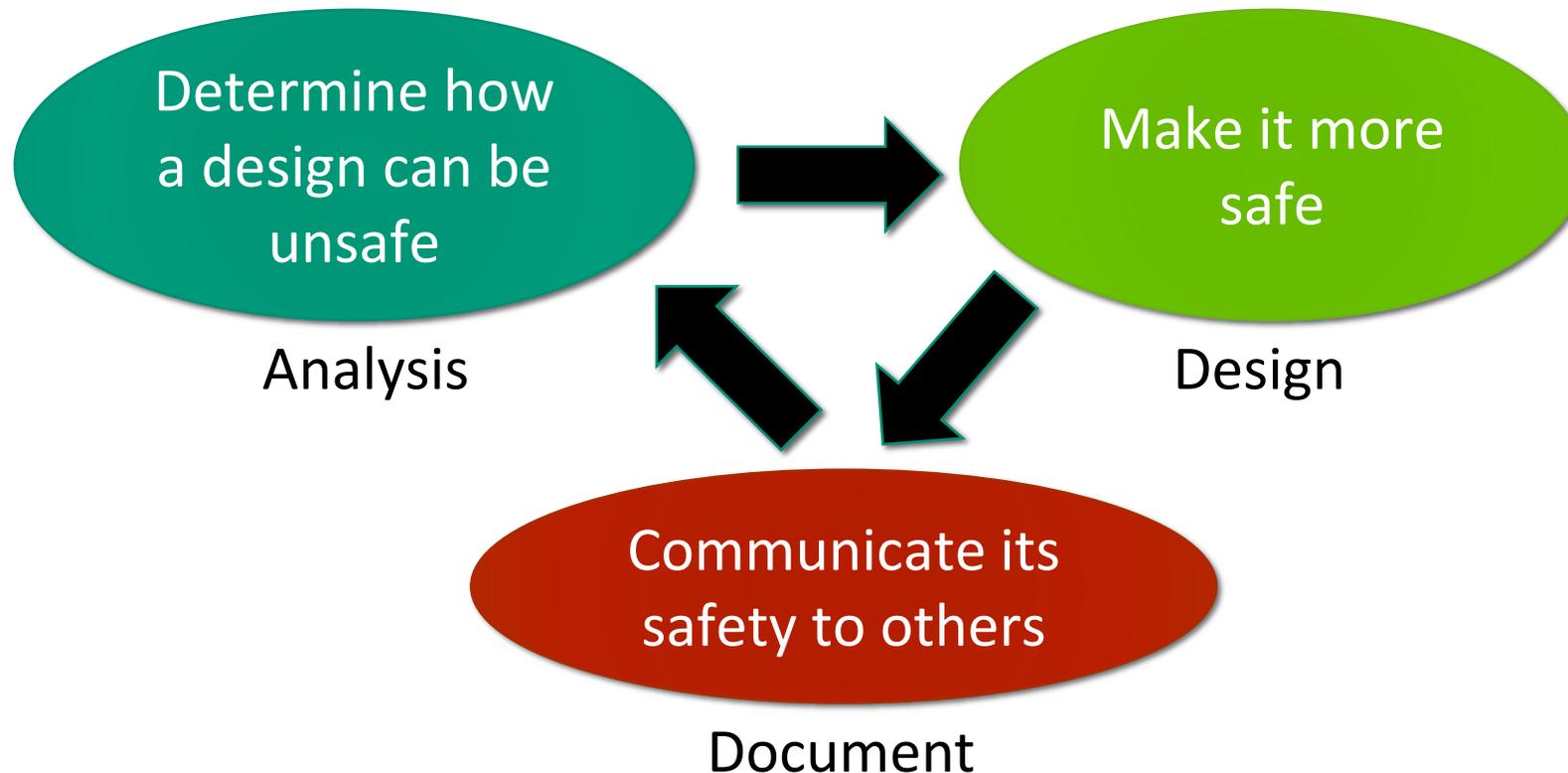
Hazard Analysis in Complex Control Systems

Hazard Analysis (Definitions)

Safety: Freedom from accidents

Hazard: System state that could lead to an accident

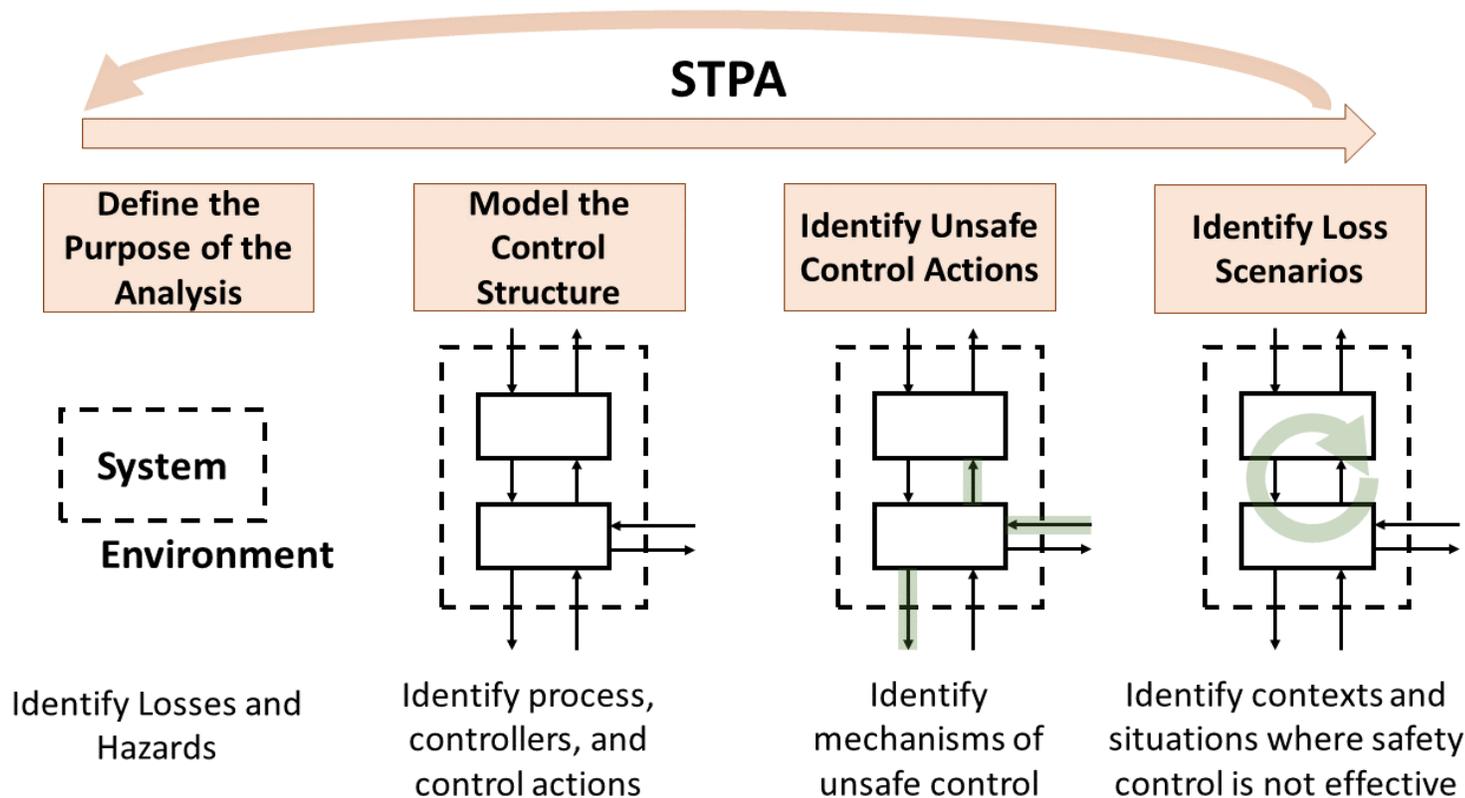
Hazard Analysis: Process of identifying hazards along with their causes and conditions



Methods: Systems Theoretic Process Analysis (STPA)



- Accidents occur when interactions violate **safety constraints**,
- The system enforces these constraints using **control**.



STPA is useful in situations where there are many “unknown-unknowns,” or hazardous situations that are difficult to predict before they happen.



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

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

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

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

Hazardous System State Definitions

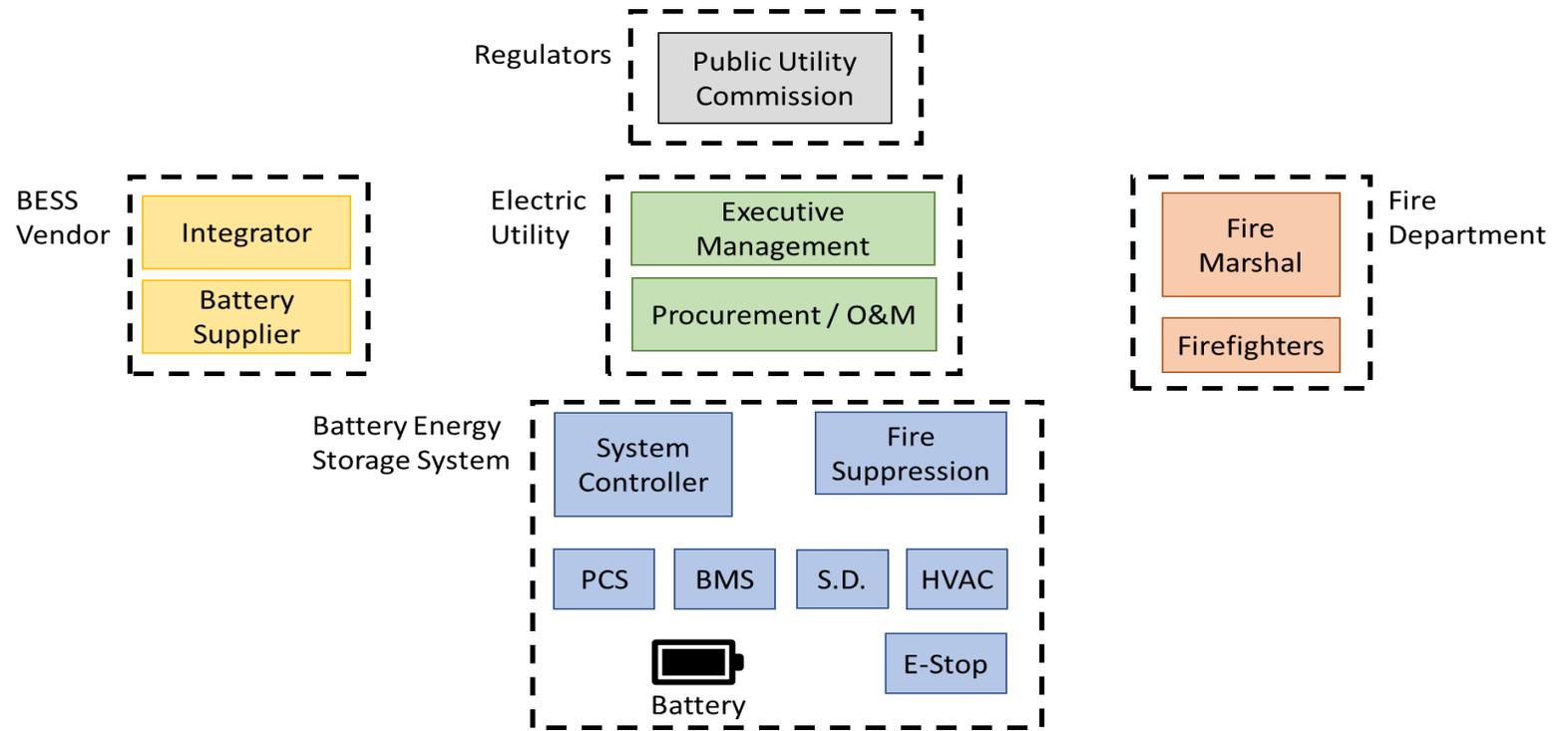
Hazard #	Definition
Hazard 1 [H1]:	an otherwise normal cell exceeds safe limits on voltage, current, or temperature [L1]
Hazard 2 [H2]:	off-gas concentration exceeds safe limit [L2]
Hazard 3 [H3]:	human exposure to a fire or an explosion [L3]
Hazard 4 [H4]:	human exposure to hazardous voltage or arc-flash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

9 Safety Control Structure



Each element within these safety control structures has some number of **inputs**, **outputs**, and **models** for how other components behave (in automated controllers these are engineered models, in humans these are mental models).

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



Example Control Actions and UCAs:

- Control action: Any physical or digital signal between elements in the safety control structure. Examples include:
 - The MODBUS communication of cell temperatures provided by the BMS to the system controller (#58 in Appendix C)
 - The utility issuing a Request for Proposals (RFP) to collect bids for a new battery system (row #21 in Appendix C)
- Unsafe control action (UCA): A control action that violates a safety constraint and generates a hazard
 - UCA-E58: Useful data must be appropriately timestamped. A mistimed temperature measurement could appear to reverse causes and effects in a post-mortem analysis. This could make causal analysis more difficult and could lead to extended system downtime [H6].
 - UCA-D21: Writing a complete RFP requires some knowledge of battery energy storage technologies. Being able to interpret the proposals received requires even more. Selecting a vendor who has a design that insufficiently enforces safety constraints could lead to a hazard [H1, H2].



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

Results

Design Objectives for System Safety



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

- **Safety critical information availability to firefighters**
 - Design objective 1.1 and/or,
 - Design objective 1.2
- **Safety of firefighter intervention**
 - Design objective 1.3
- **Thermal runaway prorogation resistance**
 - Passive design or,
 - Runaway does not violate safe temperature limits in other cells (more stringent)
 - Design objective 2.1 (cell-to-cell) and/or,
 - Design objective 2.3 (module-to- module)
 - Runaway does not initiate self-heating in other cells (less stringent)
 - Design objective 2.2 (cell-to-cell) and/or,
 - Design objective 2.4 (module-to- module)
 - Active design
 - Runaway does not violate safe temperature limits in other cells (more stringent)
 - Design objective 2.1-Active (cell-to-cell) and/or,
 - Design objective 2.3-Active (module-to- module)
 - Runaway does not initiate self-heating in other cells (less stringent)
 - Design objective 2.2-Active (cell-to-cell) and/or,
 - Design objective 2.4-Active (module-to- module)
- **External fire prevention/suppression**
 - Design objective 2.5 and,
 - Design objective 2.6
- **Explosion prevention**
 - Design objective 3.1 (passive ventilation) or,
 - Design objective 3.2 (active ventilation)
- **Explosion protection**
 - Design objective 3.3
- **Automated response to a fire and/or power outage**
 - Design objective 4.1 and,
 - Design objective 4.2 (subject to 4.1)
 - Design objective 4.3
- **Regular maintenance and ground fault management**
 - Design objective 4.4
- **Data integrity and accuracy**
 - Design objective 5.1



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

ACKNOWLEDGEMENTS

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

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

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

The full report can be found at:

<https://www.sandia.gov/ess-ssl/wp-content/uploads/2020/09/Rosewater-APS.pdf>

Questions?

Backup Slides

Safety is critical to the widescale deployment of energy storage technologies.

Bloomberg

Bloomberg

Hyperdrive

Explosions Threatening Lithium-Ion's Edge in a Battery Race

By Brian Eckhouse and Mark Chediak
April 23, 2019, 4:58 PM MDT Updated on April 24, 2019, 8:24 AM MDT

- ▶ Battery exploded at plant in Arizona; two others were shut
- ▶ Arizona utility regulator calls for 'thorough investigation'

Another lithium-ion battery has exploded, this time at an energy-storage complex in the U.S.

At least 21 fires had already occurred at battery projects in South Korea, according to BloombergNEF. But this latest one, erupting on Friday at a facility owned by a Pinnacle West Capital Corp. utility in Surprise, Arizona, marked the first time it has happened in America since batteries took off globally.

<https://www.bloomberg.com/news/articles/2019-04-23/explosions-are-threatening-lithium-ion-s-edge-in-a-battery-race>

There is a tendency to use the availability heuristic when considering risk.

To avoid this, consider how many batteries continue to operate without problems every day.

Greentech Media

gtm. Solar Grid Edge Storage Wind More Trending Podcasts Resources

APS and Fluence Investigating Explosion at Arizona Energy Storage Facility

The stakes are high for the energy storage sector after an explosion with an unknown cause left several firefighters injured.

KARL-ERIK STRONGSTA | APRIL 22, 2019



Earlier this year APS announced plans to build 850 megawatts of battery storage by 2025.

Fluence has dispatched a team of experts to help utility Arizona Public Service determine what caused an explosion at one of its grid-scale battery facilities. The explosion on Friday reportedly left four firefighters injured, including three who were sent to a burn center.

Firefighters responded to a call on April 19 after smoke was seen rising from APS' McMicken Energy Storage facility, one of two identical 2-megawatt/2-megawatt-hour grid-scale batteries the utility installed in 2017 in Phoenix's growing West Valley region.

According to local press reports, the firefighters were inspecting the facility's lithium-ion batteries when they were hit with an explosion. Several of the firefighters received chemical burns, the local fire department told the Arizona Republic.

The firefighters were later reported to be in stable condition.

APS, the state's largest investor-owned utility, said in a statement on Twitter that it is still investigating the cause of the "equipment failure."

<https://www.greentechmedia.com/articles/read/aps-and-fluence-investigating-explosion-at-arizona-energy-storage-facility#gs.gpky5k>

The Korea Times

TheKoreaTimes All Q f t y

Biz & Tech

Auto IT Game Manufacturing Retail & Food Energy

IT

Frequent fire raising concerns over safety of solar energy



A fire engulfs an energy storage system at a cement plant in Jecheon, North Chungcheong Province, Monday. / Courtesy of North Chungcheong Province Fire Service Headquarters

By Nam Hyun-woo

A series of fires in energy storage systems (ESSs) has been raising safety concerns, according to industry analysts, Tuesday.

With ESSs essential for optimizing energy efficiency, further accidents may compromise the feasibility of renewable power and hamper the government's bid to expand the use of cleaner energies.

According to the Ministry of Trade, Industry and Energy, it recommended individuals, companies and other organizations to stop using 584 uninspected ESSs across the country.

https://www.koreatimes.co.kr/www/tech/2018/12/133_260560.html

State-of-the-art Hazard Analysis Method

Probability Risk Assessment (PRA) assumes that accidents happen because the **stochastic** components of a system fail.

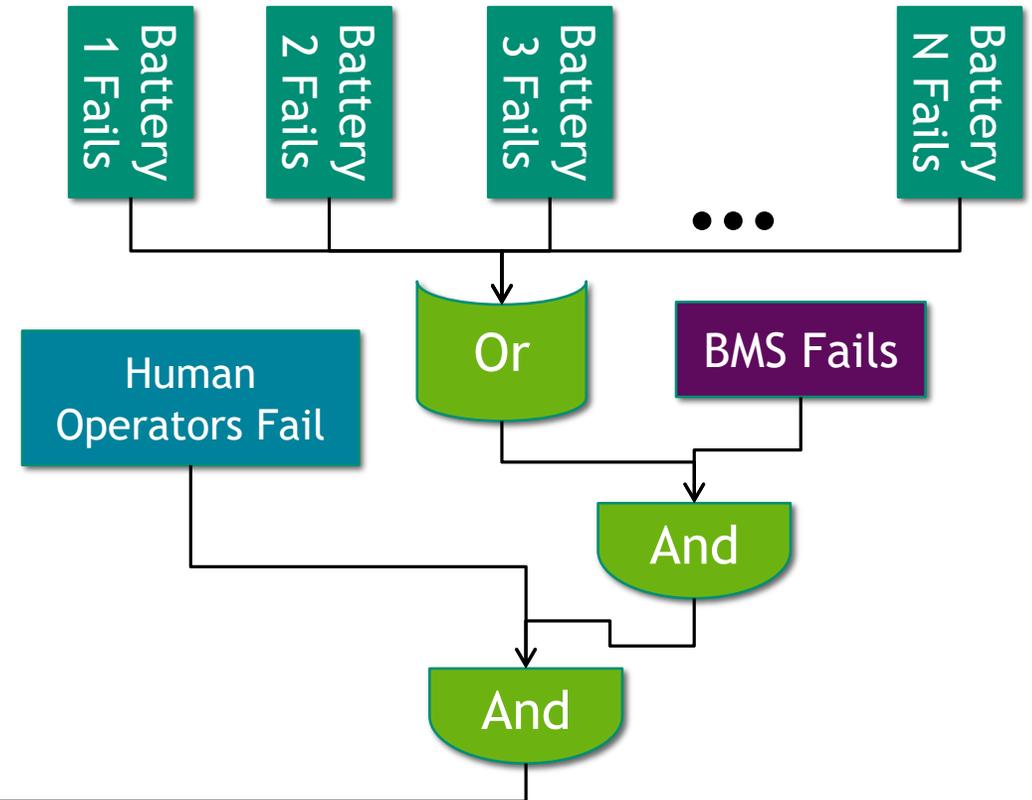
Analysis answers three questions:

What can go wrong?

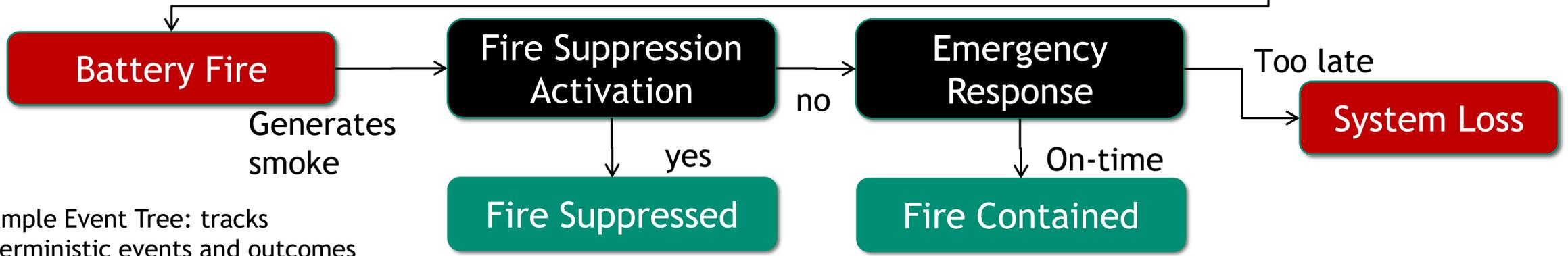
How likely is that?

How bad would that be?

Example Fault Tree: If...



PRA Consists of a combination of Event trees and Fault trees



Example Event Tree: tracks deterministic events and outcomes

Probability Risk Assessment (PRA)

Where it works well

Where there is a wealth of historical knowledge on all possible failure modes

Where the interface boundaries are static and clearly defined (finished products)

Problems with PRA

Hard to apply on serial number 001 in the design phase

Outcomes of analyses are often subjective rather than objective

Blame for accidents is often assigned to convenient scapegoats: Hardware failures, Human error, Software “failures”

Based on the assumption that Safety = Reliability



Many components, interacting in simple ways, can develop complex emergent patterns of behavior .

Carbon Analogy: Structure



Rob Lavinsky, iRocks.com – CC-BY-SA-3.0 [CC-BY-SA-3.0
(<http://creativecommons.org/licenses/by-sa/3.0/>), via Wikimedia Commons

Traffic Analogy: Emergence



By User:Diliff (Own work) [GFDL (<http://www.gnu.org/copyleft/fdl.html>), CC-BY-SA-3.0
(<http://creativecommons.org/licenses/by-sa/3.0/>) or CC-BY-SA-2.5
(<http://creativecommons.org/licenses/by-sa/2.5/>), via Wikimedia Commons

Sand Analogy: Hierarchy



By Shiraz Chakera <http://www.flickr.com/photos/shiraz/>
(<http://www.flickr.com/photos/shiraz/3387882509/>) [CC-BY-SA-2.0
(<http://creativecommons.org/licenses/by-sa/2.0/>), via Wikimedia Commons

“With systemic thinking, we recognize that "the cause" frequently lies in the very structure and organization of the system.” (Senge 1990)

“Safety is an emergent property that arises when system components interact with each other within a larger environment.”

(Leveson 2013)

Battery Cell Properties



Kristoferb [CC-BY-SA-3.0 (<http://creativecommons.org/licenses/by-sa/3.0>) or GFDL (<http://www.gnu.org/copyleft/fdl.html>)], via Wikimedia Commons

- ✓ Capacity
- ✓ Volatility
- ✓ Temperature
- ✓ Range
- ✗ Safety

“Safety” is not a property of a component

Battery System Properties



By Jelson25 (Own work) [CC-BY-3.0 (<http://creativecommons.org/licenses/by/3.0>)], via Wikimedia Commons

- ✓ Capacity
- ✓ Service Life
- ✓ Control
- ✓ Algorithm
- ✓ Safety

Safety is a system property

If safety is an emergent property, why/how do accidents happen?

Example: Thermal runaway prorogation resistance and External fire prevention/suppression



This set of design objectives defines a specific set of verifiable metrics that would prevent the propagation of thermal run-away within a battery module or system.

Two threshold options: “violate safe temperature limits,” or “initiate venting”

Two levels of integration: cell-to-cell, and/or module-to-module

Implementation options: Passive, or Active

<p>Design objective 2.1: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to violate the safe temperature limits of any nearby cells, relying only on passive design.</p>	<p>Design objective 2.2: In a battery module, the heat produced by a cell undergoing thermal runaway is insufficient, in magnitude and/or rate, to initiate venting in any nearby cells, relying only on passive design. See UL 1973 [28].</p>
<p>Design objective 2.3: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to violate the safe temperature limits of any cells in nearby modules, relying only on passive design.</p>	<p>Design objective 2.4: In a battery system, the heat produced by the propagation of thermal runaway through a module is insufficient, in magnitude and/or rate, to initiate venting in any cells in nearby modules, relying only on passive design. See UL 9540A [28] and NFPA 855 [30].</p>
<p>Design objective 2.1-1.4 Active: The system includes active propagation suppression design to meet one or more of design standards 2.1-2.4. To stop the propagation of thermal runaway using active suppression, the system design shall: 1) be able to identify when thermal runaway is occurring reliably, within a short enough time to, 2) activate emergency cooling to the affected cells/modules and those cells/modules subject to direct heat transfer from the affected cells/modules, and 3) apply sufficient cooling to satisfy one or more of design standards 2.1-2.4.</p>	<p>Design objective 2.5: Flammable materials are not stored within a defined proximity (e.g. 3 feet) of the batteries.</p> <p>Design objective 2.6: A fire suppression system, for preventing fires that are not-originating from batteries (e.g. power electronic/electrical fires) from spreading to the batteries, is included in the design and installed according to the appropriate NFPA standard for its type.</p>