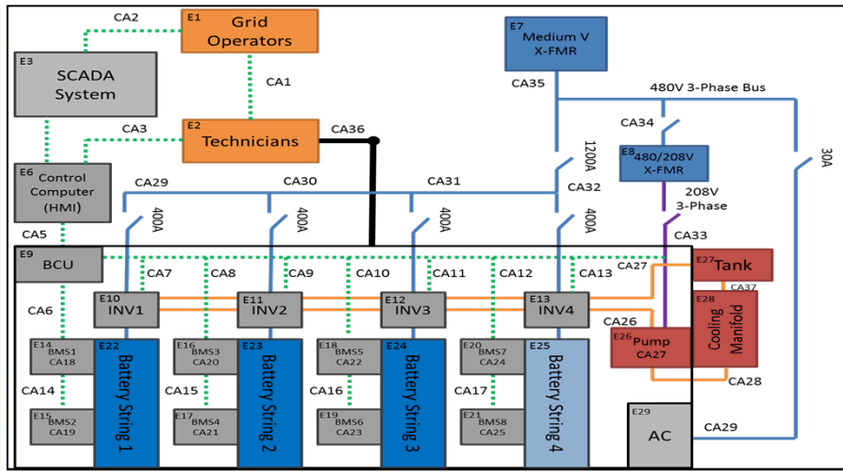
SAND2015-9950PE

Exceptional service in the national interest

Sandia National Laboratories

energy.sandia.gov



Energy Storage Hazard Analysis and Risk Management

10/16/2015 - David Rosewater

Presentation to Junior Seminar

Montana Tech, Butte MT

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

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

Outline

- Intro/Discussion of safety in batteries
- What is Energy Storage?
  - Technology
  - Value
  - History
  - Safety
- Safety Engineering
  - PRA
  - STPA/CAST
  - Example of CAST
- Parting Knowledge

What is Energy Storage?

Electrical Energy Storage Technologies

Sandia National Laboratories

Energy

- Pumped Hydro
- Compressed Air Energy Storage (CAES)
- Batteries
  - Sodium Sulfur (NaS)
  - Flow Batteries
  - Lead Acid
  - Advanced Lead Carbon
  - Lithium Ion
- Flywheels
- Electrochemical Capacitors

Power

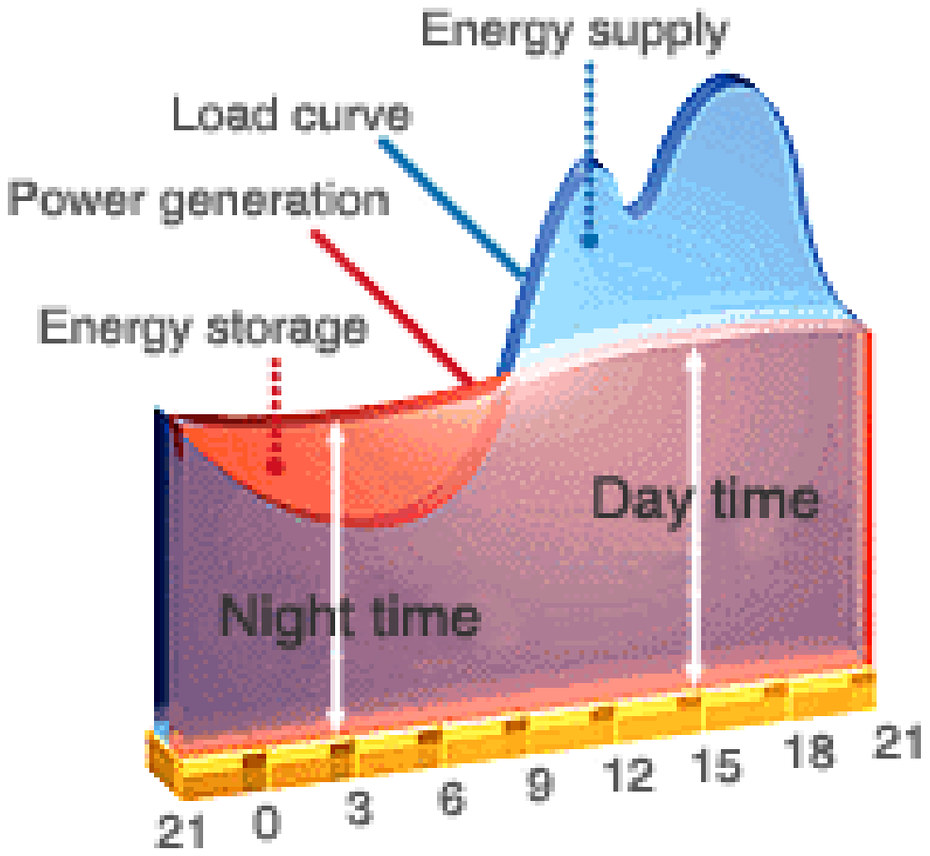
Pumped Hydro (Taum Sauk) 400 MW

Sodium Sulfur Battery 2 MW

Flywheels 1 – 20 MW

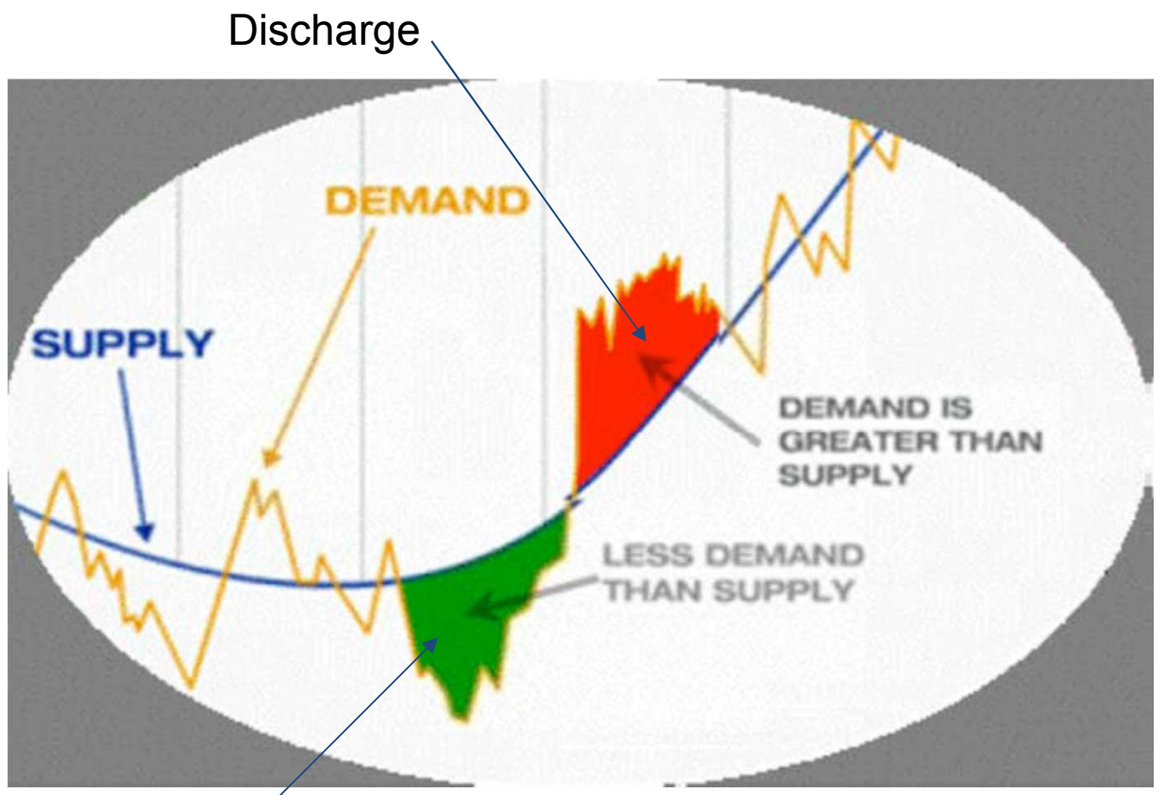
How Energy Storage Works

- Load leveling



Source: NGK Insulators, Ltd.

- Regulation



Source: Beacon Power Co.

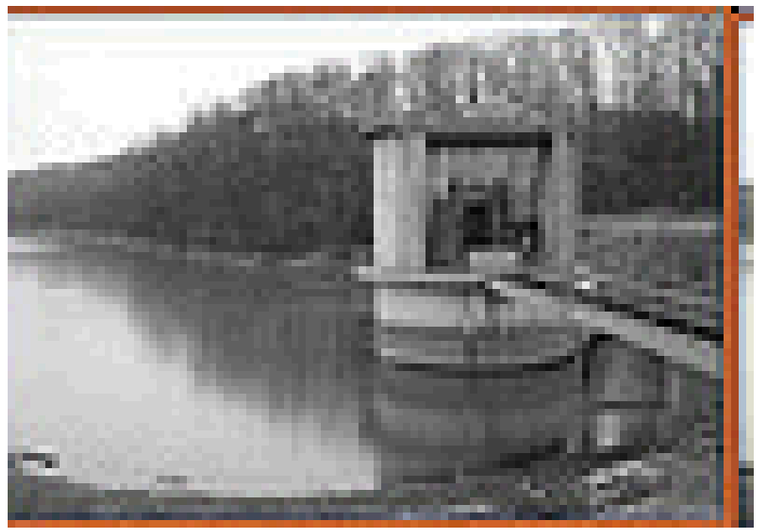
Storage moves energy through time.
Energy generated at one time can be used at another time.

Electricity Storage is Not New

- 1780’s "animal electricity" by Luigi Galvani
- 1799 Volta invented modern battery
- 1880s Private DC systems
- 1936 batteries adopted by industry in stationary devices, particularly in telegraph networks
- Lead-acid batteries original solution for night-time load

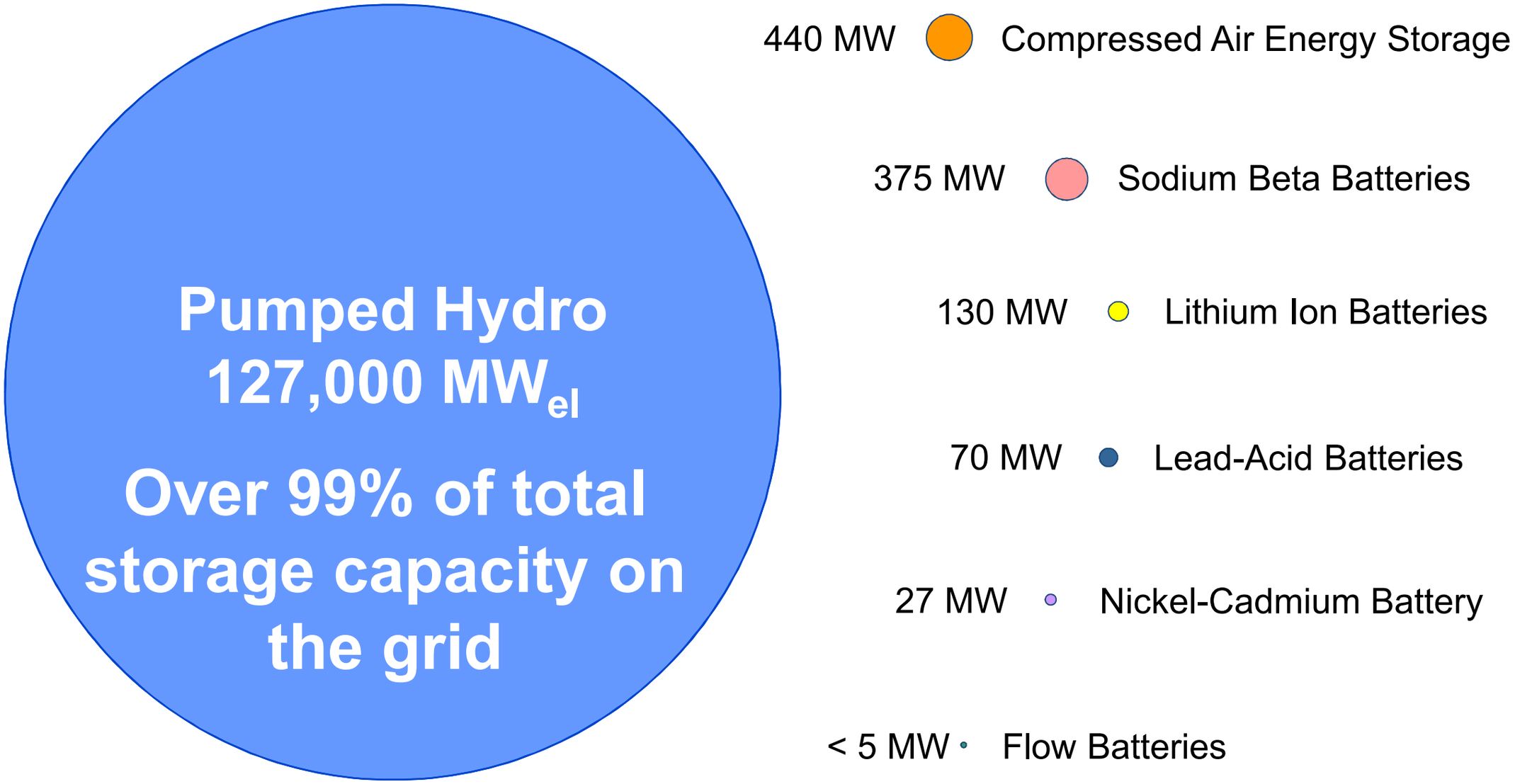
- Value of electricity storage in batteries
  - turn off generators during low-load periods
  - absorb excess electricity from generators for sale later
- The hydroelectric development of Niagara Falls in 1896.
  - Tesla and AC

First U.S. large-scale energy storage (31MW) in 1929 at Connecticut Light & Power Rocky River Plant



Storage on the grid today

Worldwide installed storage capacity for electrical energy (Sept. 2012)



Source: Fraunhofer Institute, EPRI

The Need for Energy Storage Safety Protocols

As an increasing number of energy storage systems are deployed, the risk of safety incidents increases.

Damage to Facilities

2012 Battery Room Fire at Kahuku Wind-Energy Storage Farm

- There were two fires in a year at the Kahuku Wind Farm
- There was significant damage to the facility
- Capacitors in the power electronics are reported to be associated with the failure.

Impact to First Responders

2013 Storage Battery Fire, The Landing Mall, Port Angeles WA

- First responders were not aware of the best way to extinguish the fire,
- It reignited a week after it was thought to be extinguished.

Sandia National Laboratories

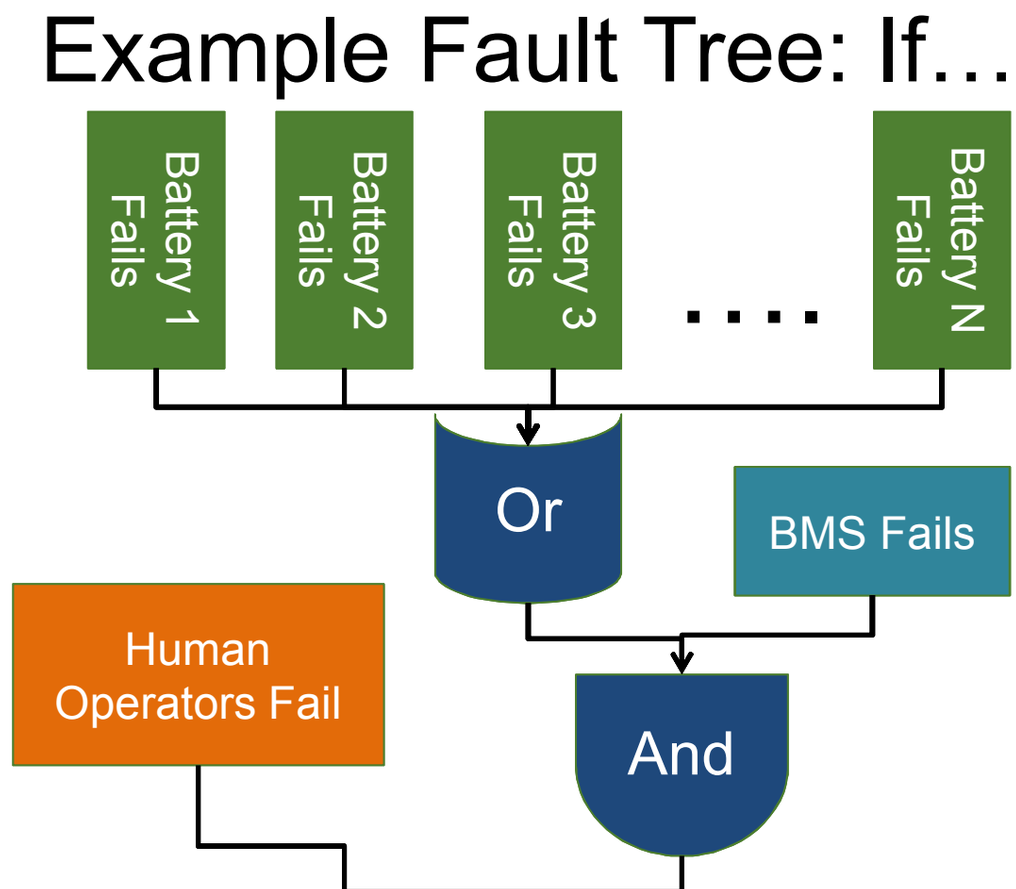
Safety Engineering

Probability Risk Assessment (PRA)

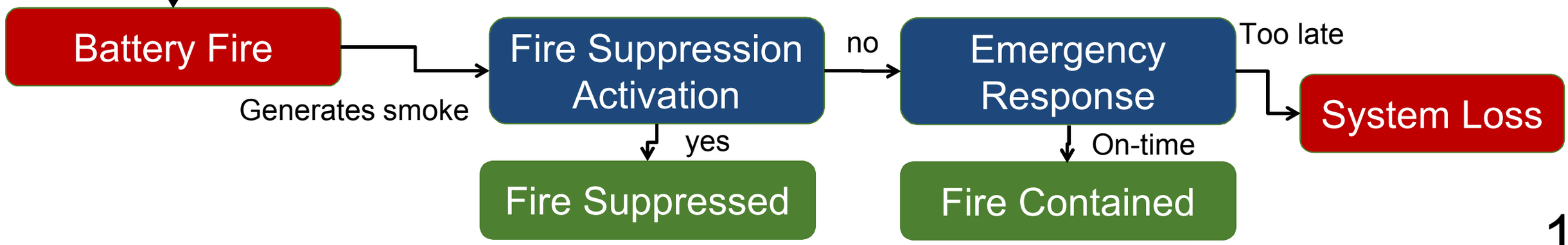
Analysis answers three questions:

1. **What** can go wrong?
2. How **likely** is that?
3. How **bad** would that be?

PRA Consists of a combination of Event trees and Fault trees



Example Event Tree: tracks deterministic events and outcomes



Systems Thinking

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

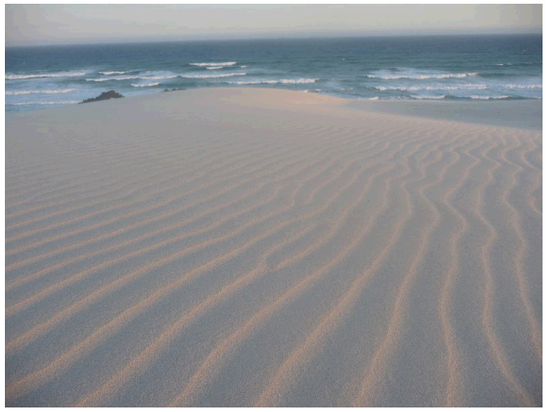
Carbon Analogy: Structure

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/shirazc/ (http://www.flickr.com/photos/shirazc/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)

Systems Thinking (Safety)

"Safety is an emergent property that arises when system components interact with each other within a larger environment."
(Leveson 2012)

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?

STAMP – New Accident Model

Sandia National Laboratories

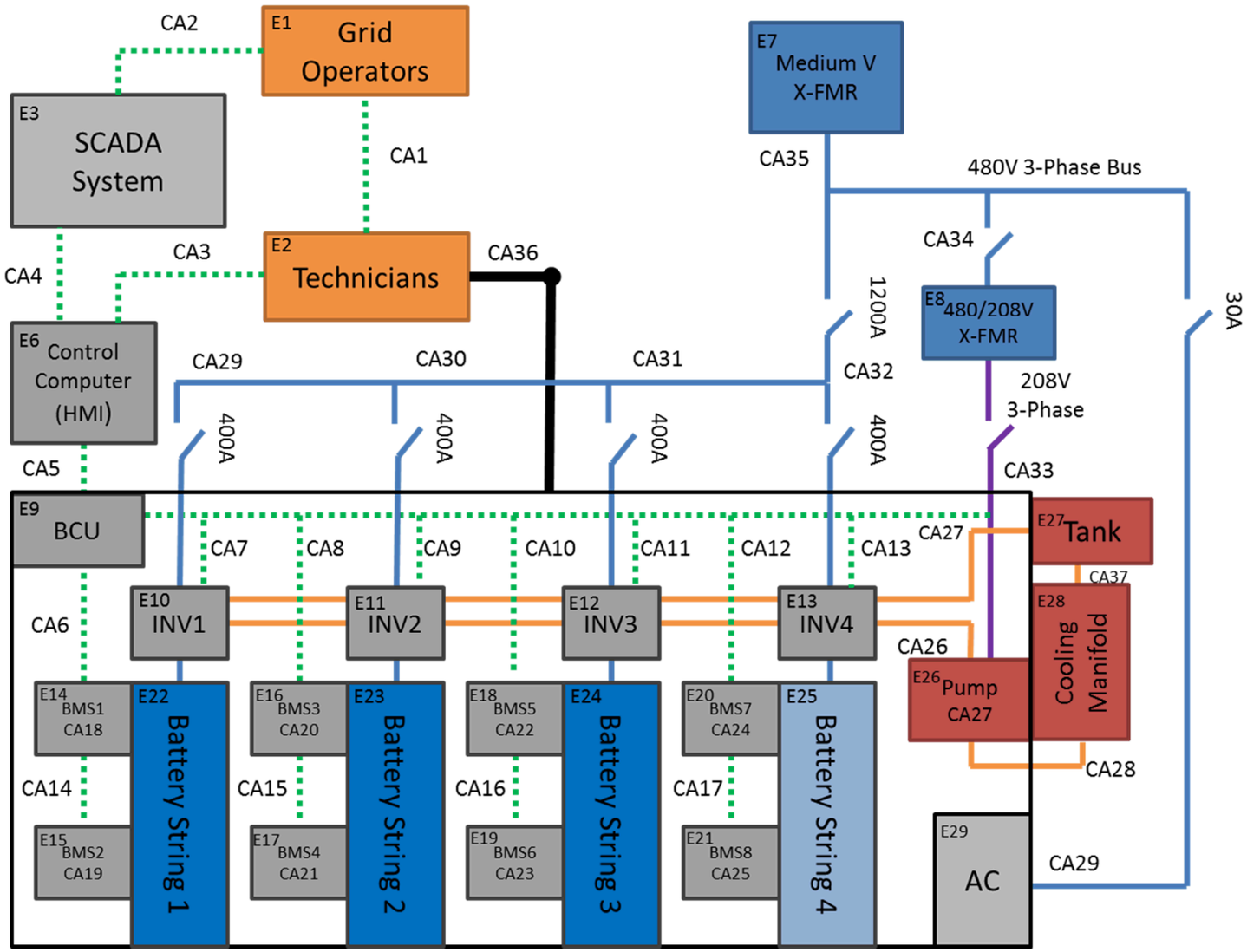
Systems-Theoretic Accident Model and Processes [Leveson, 2012]

Accidents occur when interactions violate **safety constraints**,

The system enforces these constraints using control.

Being evaluated for use by: [Leveson, 12, 13, 14]

- Boeing
- EPRI
- NRC
- VOLPE
- Etc.



Illustrative Example of a Safety Control Structure

STPA and CAST

Systems-Theoretic Process Analysis (STPA)

Goal: Identify how safety constraints can be violated in a design

Similar applications to:

FMEA/Fault-Tree

Casual Analysis based on STAMP (CAST)

Goal: Identify what safety constraints were violated during an accident

Similar applications to:

Root Cause Analysis

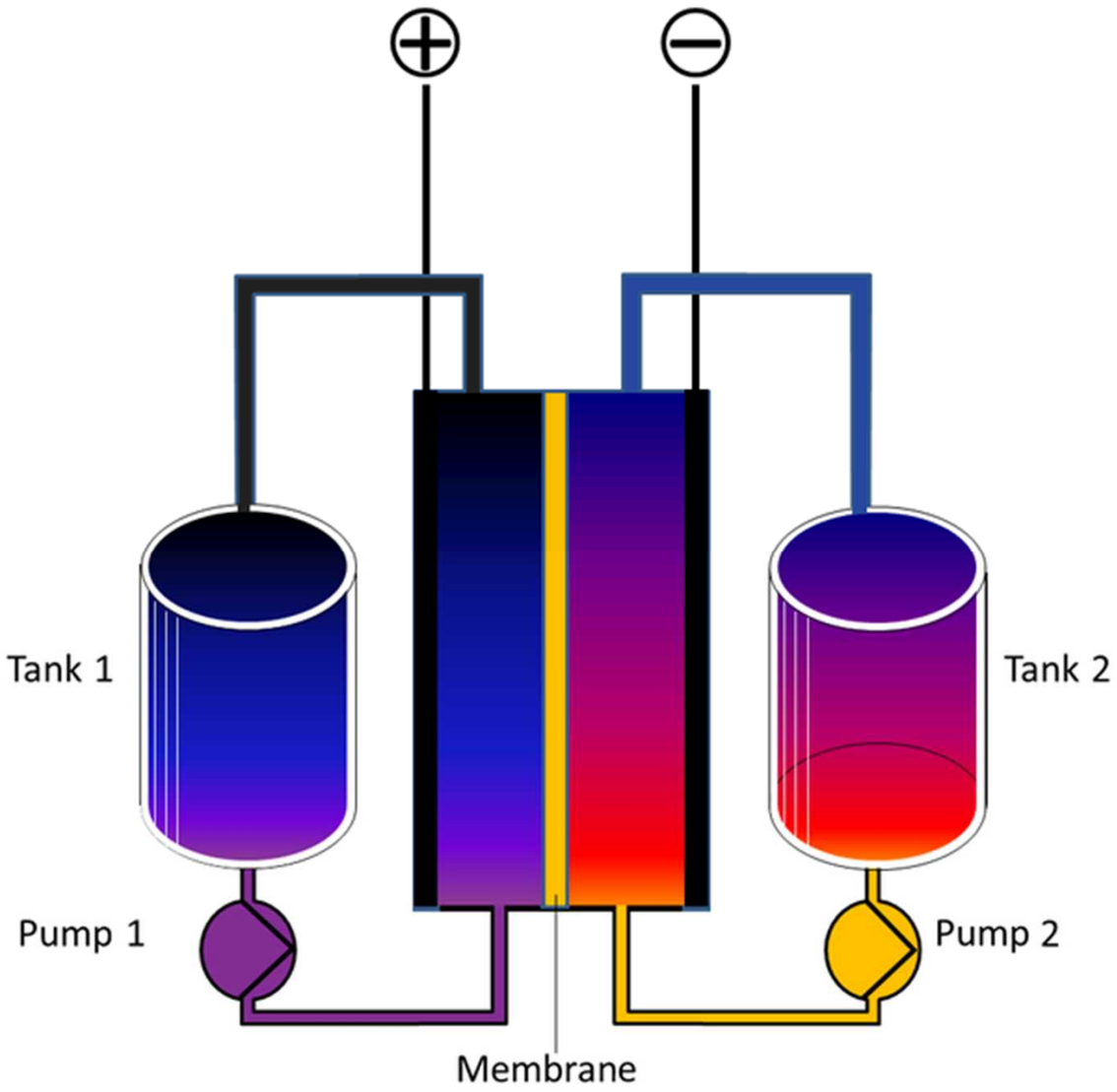
Both ask

How effectively does the system enforce its safety constraints?

How could it work better?

Example of CAST

Generic Flow Battery

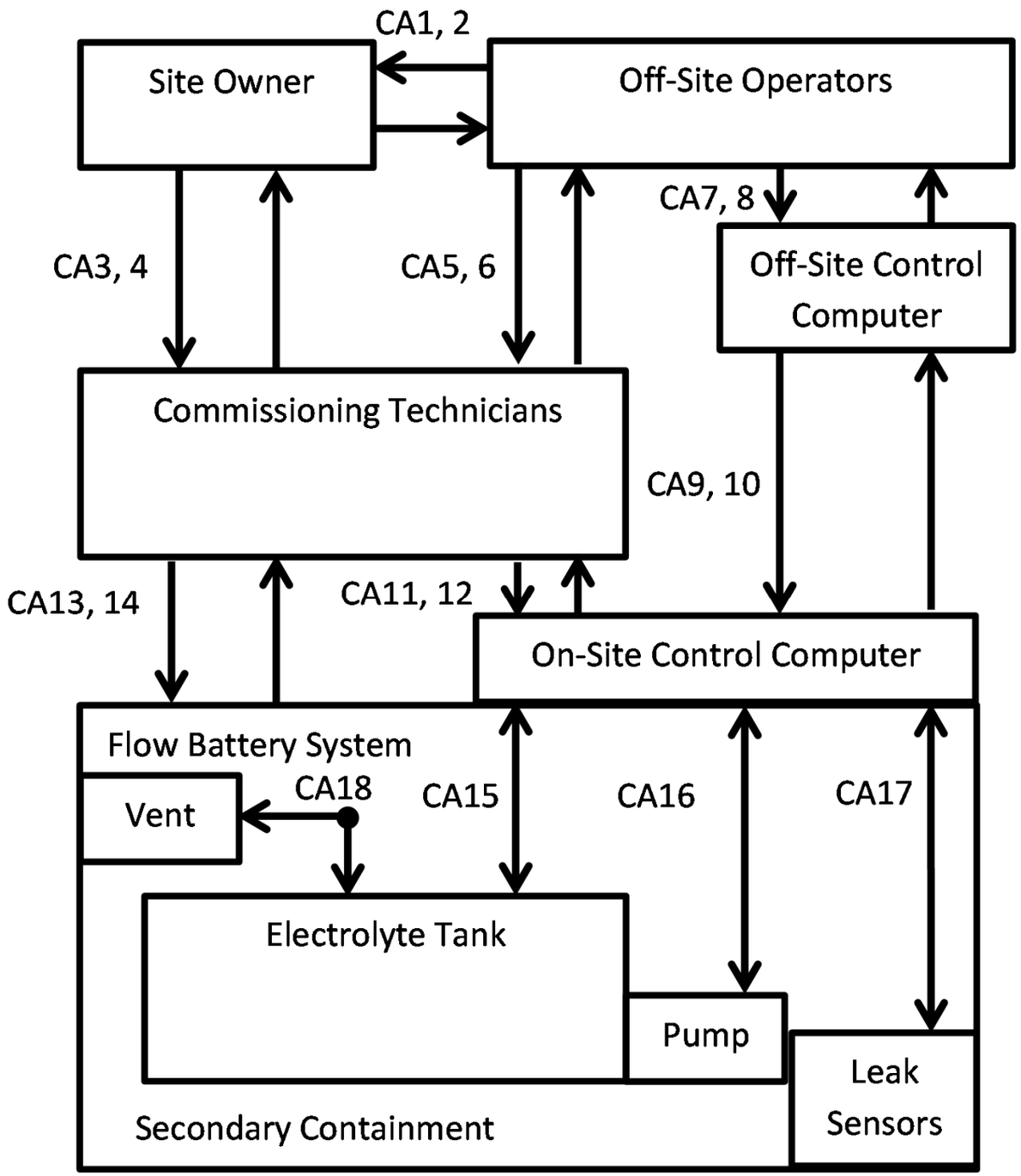


By Nick B, benboy00 [CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

Accident: Loss of effective electrolyte containment

- Several month delay for commissioning
- Leak sensors were removed to fill tank
- The vent had been blocked by nesting insects
- Electrolyte heated during use causing tank pressure to rise
- Tank was damaged by pressure rise and leaked
- Secondary containment filled and started to overflow

CAST of a Flow Battery Electrolyte Spill



Flow battery functional control diagram

CAST of a Flow Battery Electrolyte Spill

Unsafe Control Actions

- Delay of Commissioning
- Incident notification was delayed
- Emergency response procedures not effectively communicated
- Multiple controller issues
- The leak was not detected or transmitted by the system controller
- System was operated before commissioning the leak sensors
- System operation under overpressure
- **Vent Blocked**
- Secondary containment did not contain the electrolyte

Select Causal Factors

Name of Unsafe Control Action	Causal Factor 1	Causal Factor 2	Causal Factor 3	Causal Factor 4	Causal Factor 5
CA1					
Delay of commissioning	Contract/Agreement delays	Inconsistent permitting, inspection and commissioning requirements across industry	Access Control Interlock insolation had to be installed after inspection	Immature codes for ESS inspectors to reference	
CA12					
The leak signal was not sent by the On-Site computer	Leak sensors were non-operational	the communication link for the leak sensor was non-operational	Commissioning technicians ran the system before the leak sensors were in place	Inconsistent permitting, inspection and commissioning requirements across industry	Immature codes for ESS inspectors to reference
CA18					
Vent Blocked	Insect Nest	Commissioning delays	Vents not checked before operation	Inconsistent permitting, inspection and commissioning requirements across industry	Immature codes for ESS inspectors to reference

CAST of a Flow Battery Electrolyte Spill

- 3 Proposed corrective actions from initial incident report
- 9 Additional recommendations from applying CAST

Outcome of Root Cause Analysis

Proposed Actions
Develop Emergency Call List
Protection circuit verification to be performed before operation
Install Vent Tube Screen

Actions for Sandia/DOE

1. Develop consistent and complete Codes Standards and Regulations (CSR) for ESS
2. Develop general commissioning Requirements for ESS
3. Develop energy storage System Safety Protocols for flow batteries

Site Owner

4. Develop clear site use requirements

Actions for Off-Site Operators

5. Ensure communication with on-site personnel is consistent throughout commissioning

Energy Storage Vender

6. Update commissioning plan to include inspection and testing of all critical elements before operation
7. Design a feedback mechanism to detect tank overpressure
8. Conduct practice commissioning sessions for technicians
9. Design more effective secondary containment

Parting Knowledge

- Life-long learning starts now
- Under the right conditions, mistakes can be opportunities
- Safety is a moral imperative
- Your classes give you the skills to solve many problems
- Your education and experience give you the ability develop new skills to solve the problems you never even heard of

This work was funded by the DOE OE. Thanks to Dr. Gyuk for his support of work advancing the safety of energy storage.

I also want to acknowledge professor Nancy Leveson and her team at MIT for the development of STAMP, STPA, and CAST. More information can be found at:

http://sunnyday.mit.edu/

Questions?

David Rosewater PE

dmrose@sandia.gov

505 844-3722

References

-Nancy Leveson, 2012. Engineering a Safer World: System's Theory Applied to Safety. MIT Press, Cambridge, MA

-Peter M. Senge, 1990. The fifth discipline: The art & practice of the learning organization. NY: Doubleday., p. 78

-Nancy Leveson, (2012, 2013, 2014) "STAMP Workshop Presentations" MIT Partnership for a System's Approach to Safety, [Online], Available: http://psas.scripts.mit.edu/home/