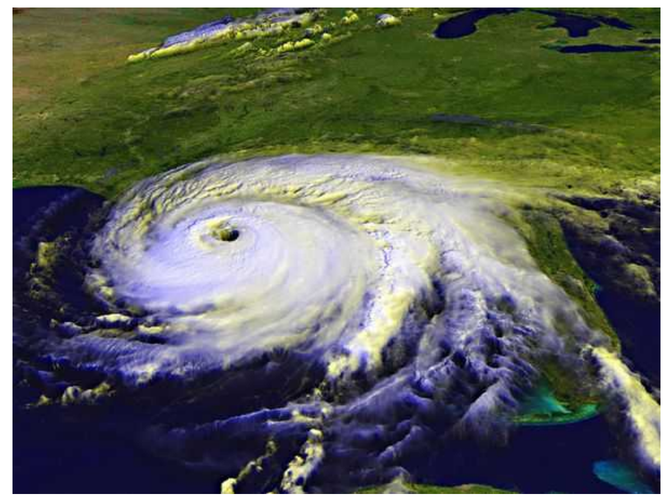
SAND2014-19648C

Exceptional service in the national interest

Sandia National Laboratories

energy.sandia.gov



Engineering Systems Theory Applied to Stationary Energy Storage Safety

11/13/2014 David Rosewater PE

Energy Storage Test Engineer

U.S. DEPARTMENT OF ENERGY NNSA 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 to Safety Engineering (PRA)
- Systems Thinking and STAMP
- Systems Theoretic Processes Analysis (STPA) and Causal Analysis based on STAMP (CAST)
  - Example and Implications
- Parting Knowledge

Probability Risk Assessment (PRA)

Accidents happen because the **stochastic** components of a system fail.

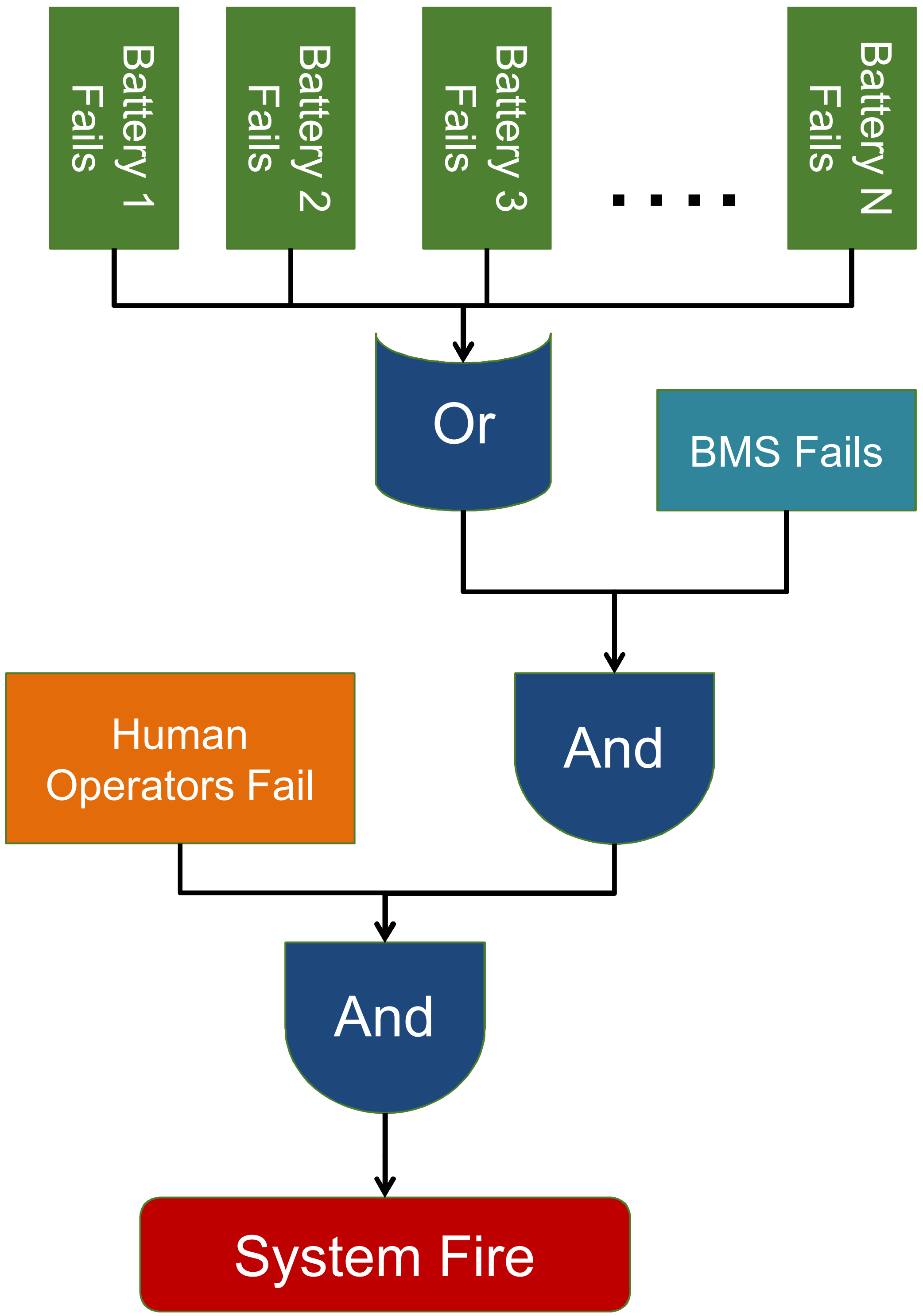
Analysis answers three questions:

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

PRA Techniques

- *Event trees*
- *Fault trees*
- HAZOP
- FMEA and FMECA
- Monte Carlo Simulation

Example Fault Tree: If…



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

- <u>Hard to apply on serial number 001 in the design phase</u>
- 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

Systems Thinking

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

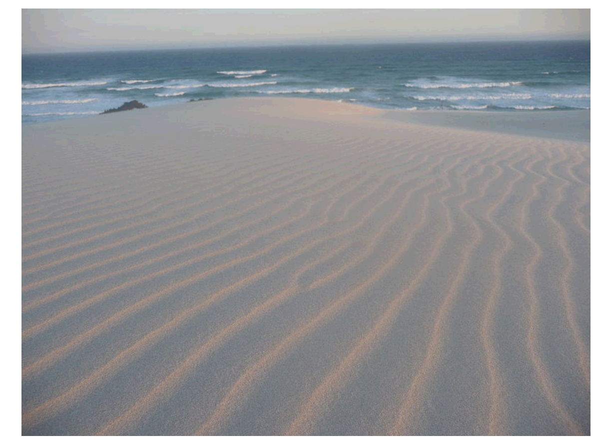
Carbon Analogy: Structure

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 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?

STAMP – New Accident Model

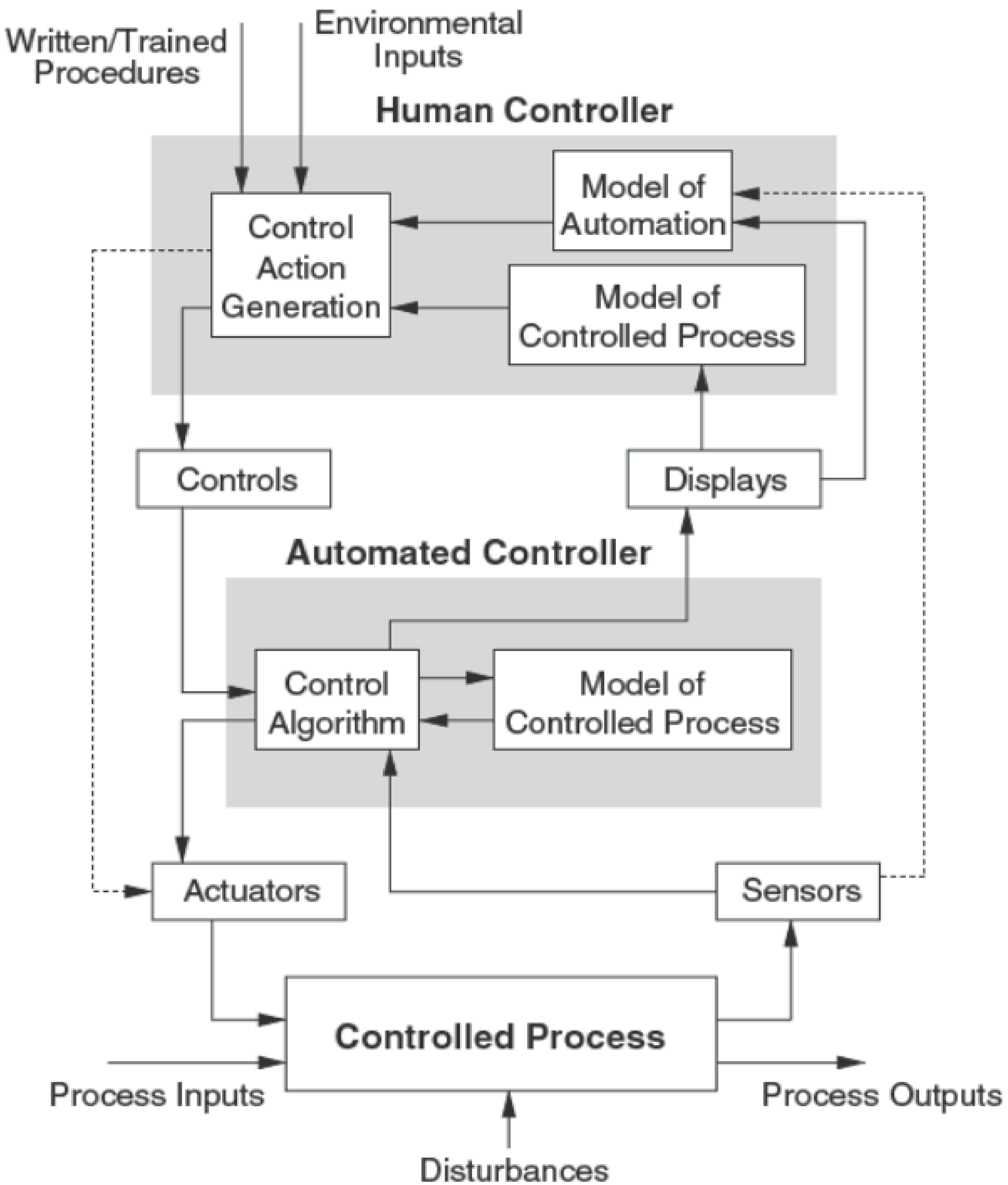
Systems-Theoretic Accident Model and Processes [Leveson, 2013]

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

The system enforces these constraints using control.

Being evaluated for use by:

- Boeing
- EPRI
- NRC
- VOLPE
- Etc.



Example Safety Control Structure (Leveson, 2013)

STPA and CAST

Systems-Theoretic Process Analysis (STPA)

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

Similar to: FMEA/Fault-Tree

Casual Analysis based on STAMP (CAST)

Goal: Identify what safety constraints were violated during an accident

Similar to: Root Cause Analysis

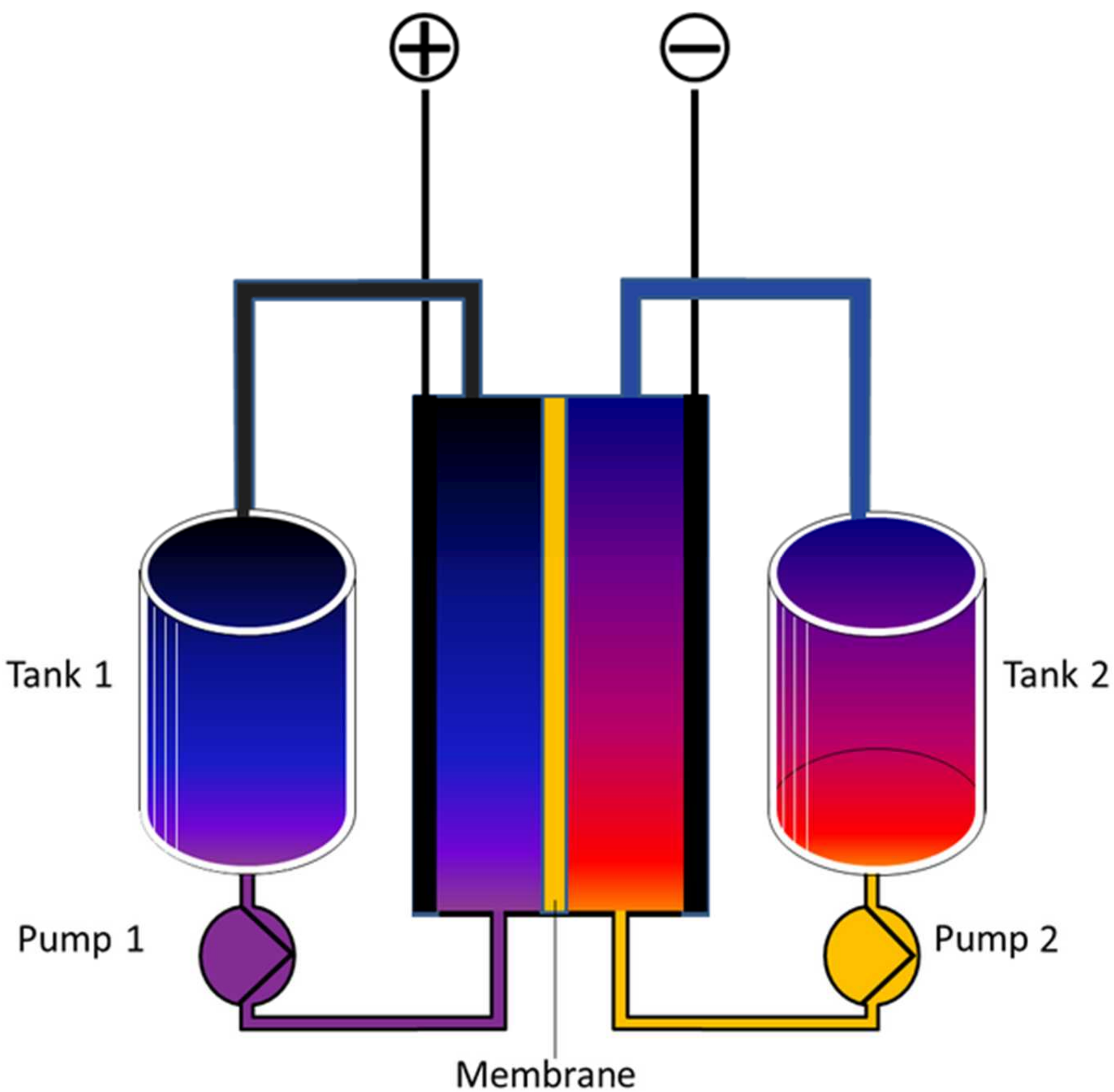
Both ask

How effectively does the system enforce its safety constraints?

How could it work better?

Example of CAST

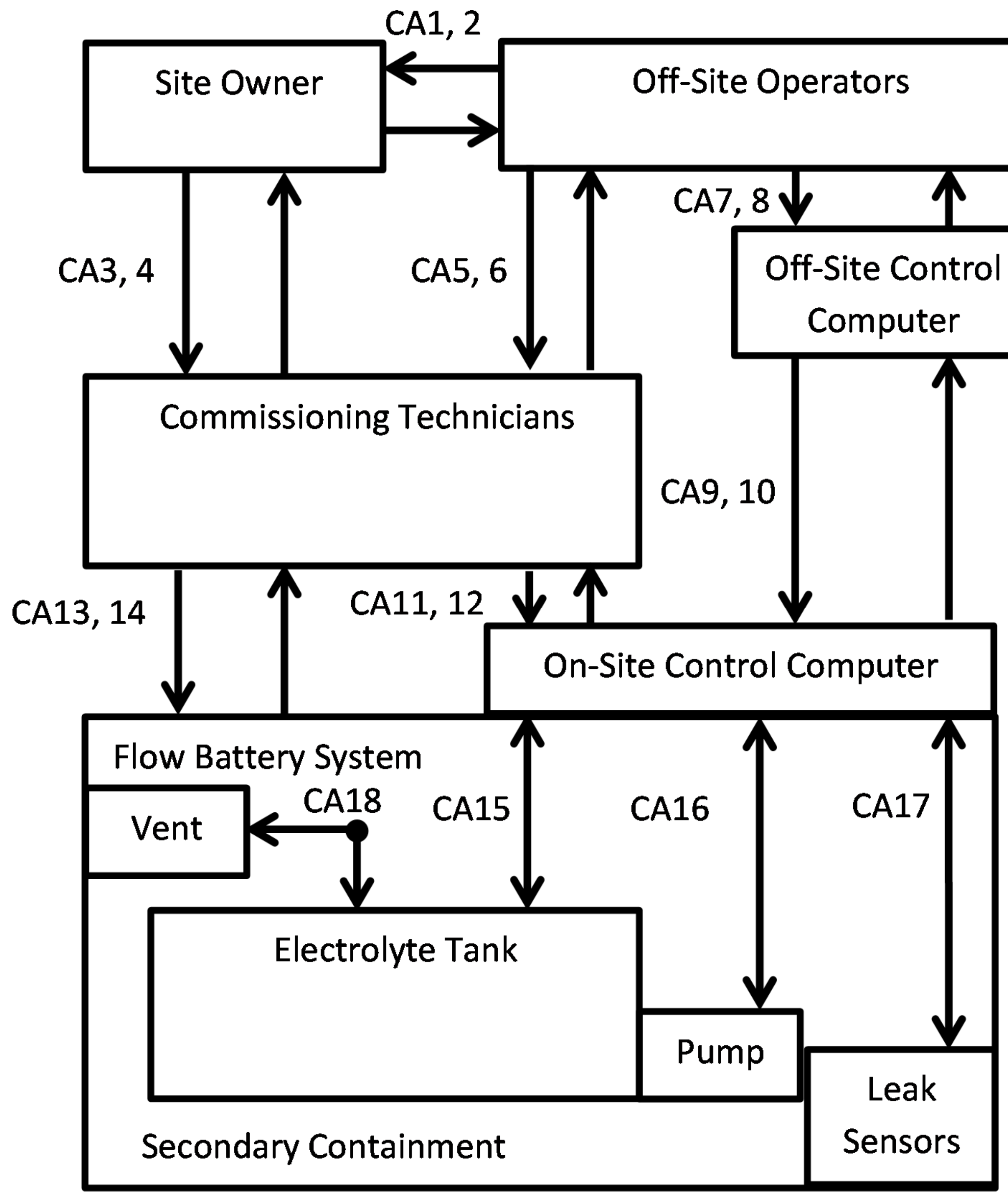
Generic Flow Battery



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	Contract/ agreement 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

- A new perspective viewing safety as an emergent or structural system property has advantages over viewing safety as measured by individual components
- The "cause" of accidents sometimes comes from the structure of a system rather than it's components
- STPA and CAST could be a very useful tools in managing the safety of highly complex systems

Thank You to the DOE OE and especially Dr. Gyuk for his dedication and support to the ES industry and Sandia's ES Program.

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, 2013. Engineering a Safer World: System's Theory Applied to Safety. MIT Press, Cambridge, MA

-Zio, E Reliability engineering: Old problems and new challenges, Reliability Engineering and System Safety 94, 2008, 125-141

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