Sandia National Laboratories

Exceptional service in the national interest

Applying STPA to a Battery Energy Storage System

Energy Storage System Safety and STPA

Battery energy storage systems have experienced a few high-profile accidents in recent history, reducing customer confidence and slowing market growth. As the density of batteries installed in energy storage systems increases in response to demands for greater performance and reduced footprint, the probabilistic design methodologies of the last century become less able to effectively identify and communicate hazards. Wide adoption of hazardous analysis techniques such as Systems-Theoretic Process Analysis (STPA), which include causal perspectives broader than simple probabilistic chains of events, could help improve the safety design culture of the stationary energy storage industry, hopefully preventing what happened on Oahu from happening again elsewhere.

Figure 1 Battery Fire at Kahuku Wind-Energy Storage Farm, Oahu Hawaii, August 1st 2012
(From www.hawaiinewsnow.com courtesy: Jay Armstrong)

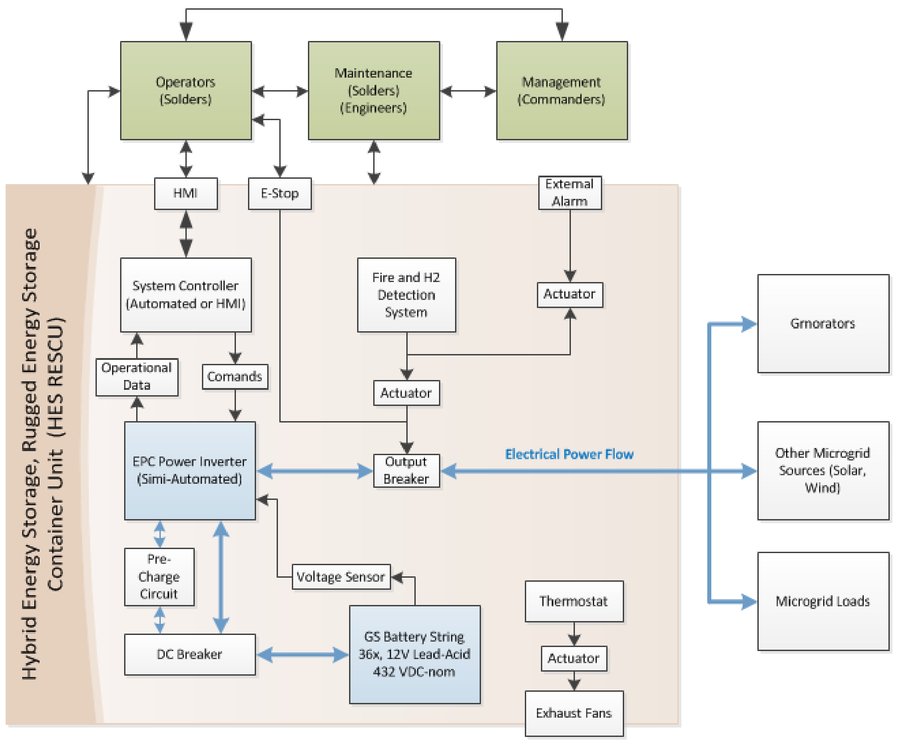

Figure 2 HES RESCU Control Structure

The HES RESCU

The Hybrid Energy System, Rugged Energy Storage Container Unit (HES RESCU) is a Lead-Acid battery energy storage system designed and built by GS Battery and EPC Power to optimize energy production and use in a military Forward Operating Base (FOB). This application of STPA serves as a test of how well the technique is able to identify and communicate the unique hazards of large scale energy storage systems.

Select Unsafe Control Actions (STPA Step 1)

Actor or Component	Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped to Soon or Applied Too Long Causes Hazard
System Controller	Conduct a Normal Charge	If the system is left for an extended period of time below 60% SOC sulfation can occur causing damage to the batteries.	Operation in this mode should not exceed any of the limits on the system components including current, voltage, and temperature.	Conducting a normal charge not often enough can cause damage to the batteries.	charging incorrectly (too long, not long enough, at too high a rate or not a high enough rate) can cause damage to the batteries
Fire and H2 detection system	Command External Alarm to Activate	If there is either a fire or a buildup of H2 and the alarm does not activate the operators would not know that action must be taken	Nuisance alarms will cause operators to loose confidence in or deactivate this device	This system should be started along with the system and should remain in operation as long as the system has power. The alarm should sound along with the output breaker opening	alarm should be able to be silenced and should be deactivated when the system is returned to a safe state
Exhaust Fans	Activate	The temperature of the batteries must be managed in order to ensure an operational life.	if the batteries are too cold then the exaust could cause further damage	Not Hazardous	if the batteries are too cold then the exhaust could cause further damage

Select Corrective Measures (Results from STPA Step 2)

- Additional sensors should be installed in the pre-charge circuit to detect when it is not functioning properly before it can damage itself, the inverter, or the batteries it is connected too
- The external alarm should differentiate fire from H2 build-up
- Add an operator warning for when the battery State of Charge (SOC) is below 60%
- Maintenance program should evaluate battery State of Health (SOH) on a regular basis to prevent damage during operation
- The thermostat should operate off of battery temperatures (max and min) rather than air temperature
- In very hot and very cold environments active heating and cooling should be installed.
- Independent battery voltage and current sensors should be installed to display battery conditions to operators
- Inverter should be enabled to limit charge and discharge rates based on battery temperature

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.
SAND No. 2014-2146P

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration