Cybersecurity of Battery Energy Storage Systems

Victoria O'Brien

2024 DOE Office of Electricity Energy Storage Program Annual Meeting and Peer Review

August 5, 2024

Session ID: 405

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2024-09881C

Policy for Battery Energy Storage System Cybersecurity

Cybersecurity standards exist for adjacent systems, including bulk electric systems, power systems, distributed energy resources, and general cybersecurity principles, but **a research gap exists for specific policy for battery energy storage systems.**

- NIST Cybersecurity Framework 2.0
- NERC-CIP-011-2 Information Protection
- NERC-CIP-010-2 Configuration change management vulnerability assessments
- NERC-CIP-007-6 Security System Management
- IEEE 1547.3 – 2023 Cybersecurity of Distributed Energy Resources
- NIST Guides
- NIST 800-82 Guide to Operational Technology (OT) Security
- Sandia Energy Storage Handbook 2020 Chapter 18
- Common Sense Guide to Mitigating Insider Threats
- NIST Cybersecurity Framework 2.0
- IEEE 1547.3 – 2018 annex D.4 Cybersecurity is out of scope

Selected cybersecurity standards and best practices

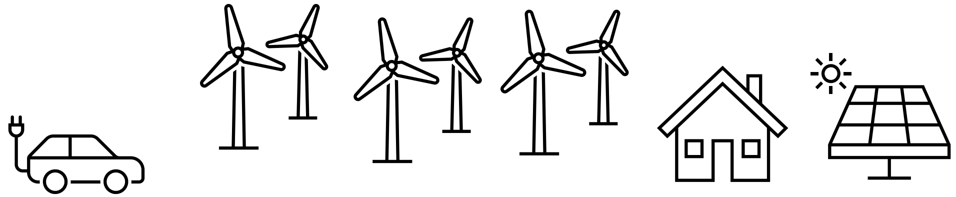
Cybersecurity Fundamentals Inspiring this Research

Unknown Probability of an Attack	Zero-Trust Approach	Defense-in-Depth Approach
• Hard to predict what vulnerabilities may be exploited • New vulnerabilities can be discovered • Different studies have differing results regarding the likelihood of cyberattacks	• Do not assume a system or device is attack free • Do not assume it is impossible to compromise a system • Authentication, Authorization, and Validation can help with this	• Add as many layers of protection to the system as reasonable / possible • If one layer is compromised, backup layers exist stop threats • Some layers may include: policy, physical, network, application, device

Fundamentals for battery energy storage system cybersecurity

Energy Storage Background

- Increased need for energy storage systems

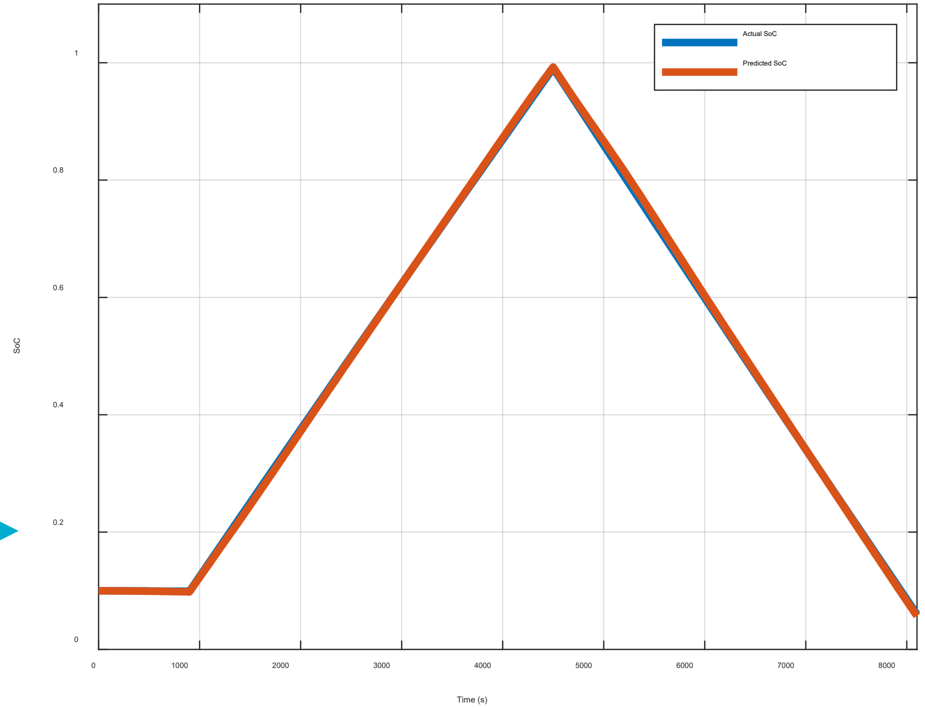


Pumped-Hydro | Battery ESS | Flywheels

- Batteries are controlled by battery management systems (BMSs)

Functions of the BMS

Protection	Sensing	Parameter Estimation
Ensure Safety Limit	Voltage	Internal Parameters
Control Operations	Current	State of Charge (SoC)
Cell Balancing	Temperature	State of Health (SoH)

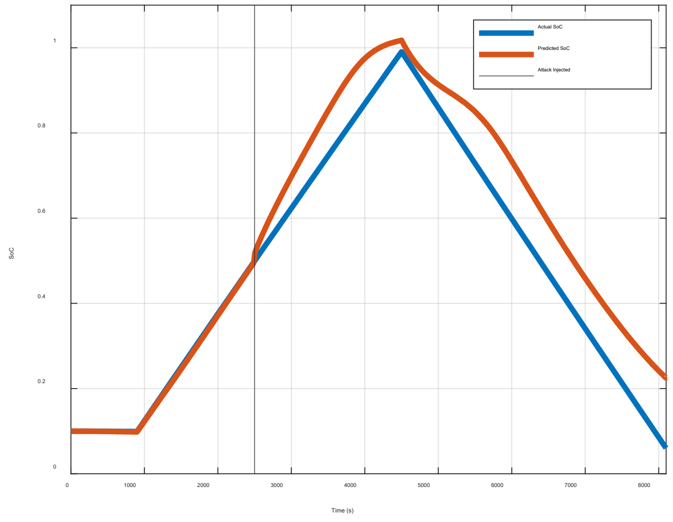


Predicted and actual SoC

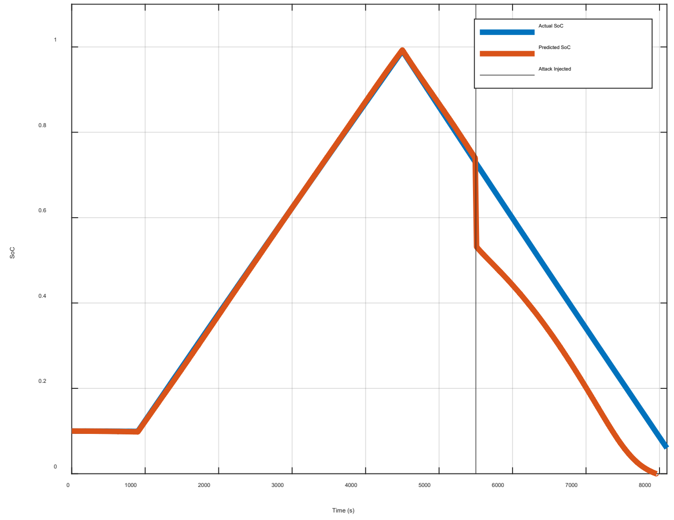
False Data Injection Attacks (FDIAs)

- Detection and mitigation of FDIAs is crucial to the safe and reliable operation of the system
- Targets sensors and aims to change measurement before used in estimation
- Possible consequences:

Power outages	Thermal runaway events
Battery degradation	Increased costs
Injury	Damage to equipment



SoC when a -100 mV FDIA was injected to a voltage sensor at 2500 s

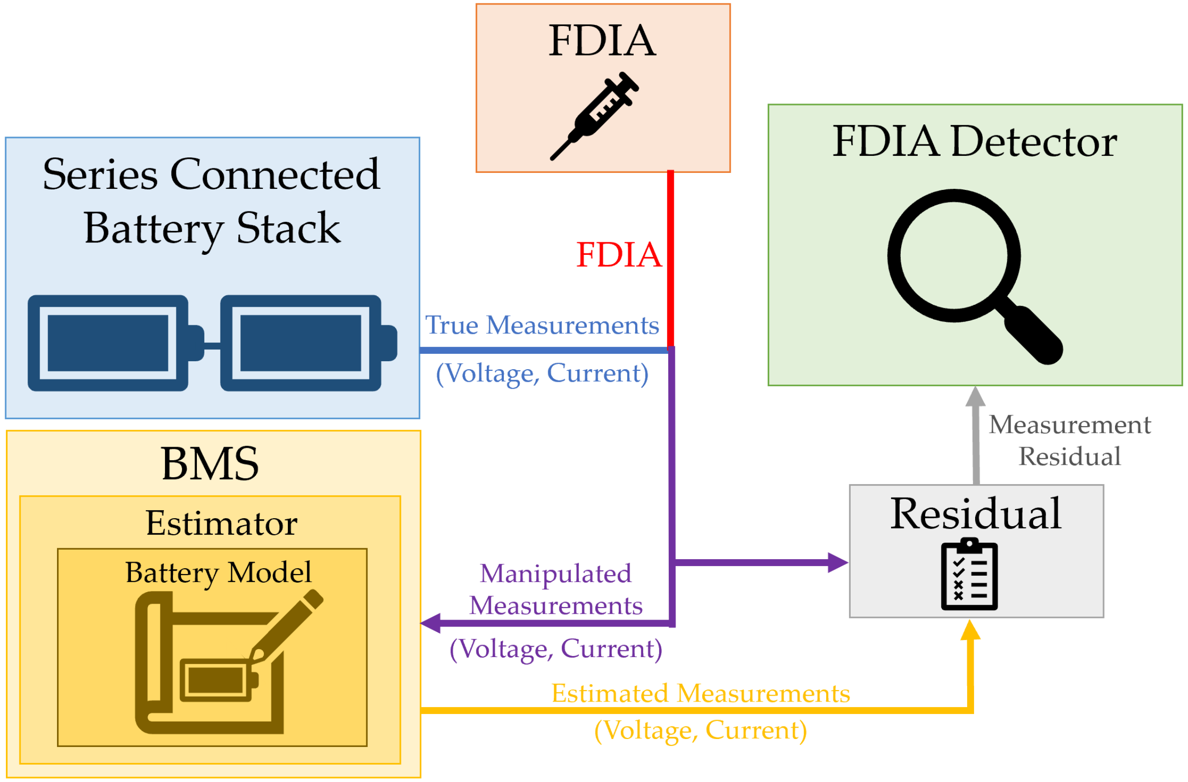


SoC when a +100 mV FDIA was injected to a voltage sensor at 5500 s

Approach

Goal: to repurpose anomaly detection methods and detect FDIAs targeting the sensors of battery stacks, to **increase** the **resiliency** and **reliability** of grid-connected battery systems.

- **Step 1:** Use battery models to represent dynamics of system
- **Step 2:** Use nonlinear estimator to estimate system states and measurements
- **Step 3:** Generate a priori measurement residual
- **Step 4:** Run a priori data through CUSUM algorithm for FDIA detection



General process of SoC estimation and FDIA detection

Approach

Approach: detect FDIAs in the sensors of battery stacks using a three-pronged method of battery modeling, state estimation, and statistics-based detection mechanisms

Utilize battery model to represent dynamics → Use estimator to estimate system states and measurements → Generate residuals between actual and estimated measurements → FDIA detection mechanism → FDIA is detected

Summary of proposed approach

Models

- Equivalent circuit model (ECM)
- Ambient temperature dependent ECM
- Charge reservoir model
- Single particle model

Estimators

- Kalman Filter (KF)
- Extended KF
- Unscented KF
- Input noise aware EKF

Detection

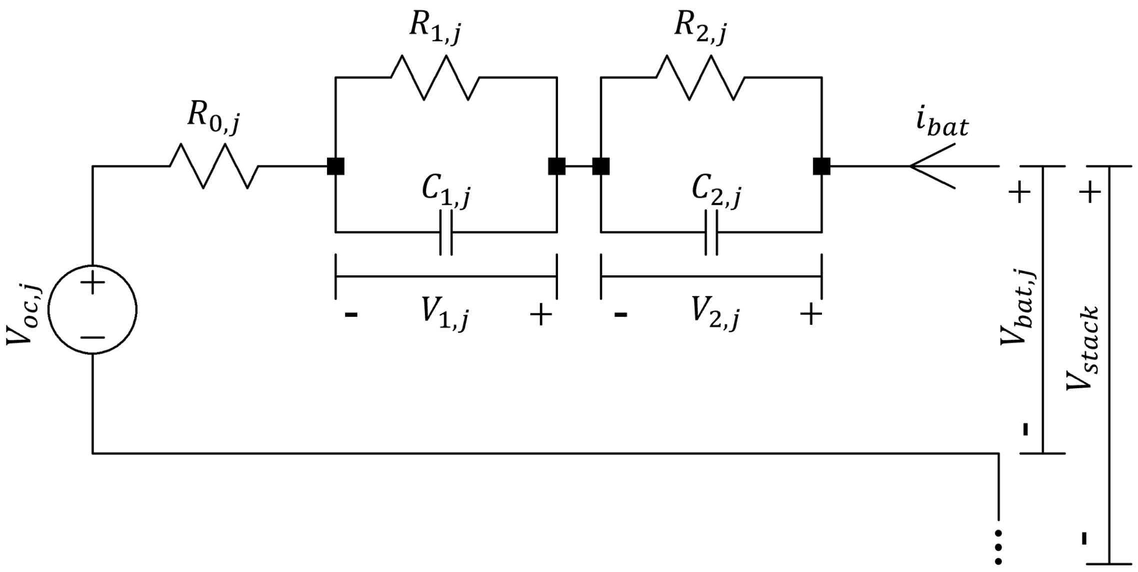
- Chi-squared test
- Normalized innovation error identifier
- Cumulative sum (CUSUM) algorithm

Studied Methods

Selected Battery Models

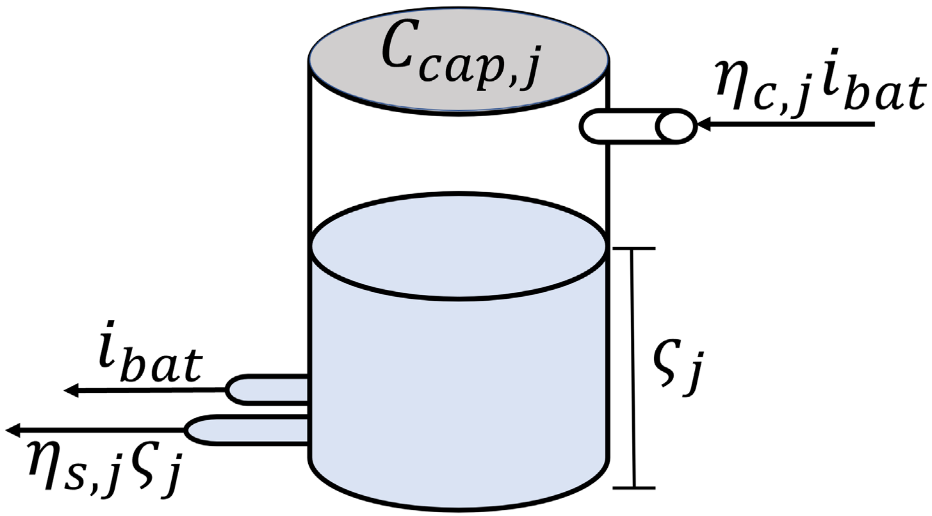
Equivalent Circuit Model

- Models the response of battery voltage (output) to the stack current (input)
- Good balance of accuracy and complexity
- Does not account for degradation



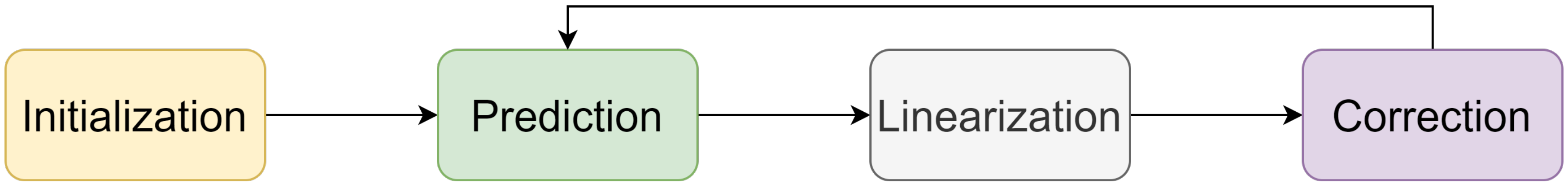
Charge Reservoir Model

- Models charging and discharging as filling and draining of a cylindrical tank, respectively
- Required to supplement ECM, as it does not include SoC estimation



Extended Kalman Filter (EKF)

- Used to estimate SoC and measurements
- Estimated measurements are compared to actual measurements to calculate the a priori measurement residual (used in detector)
- Compatible with nonlinear systems
- Theoretically less accurate than the unscented Kalman filter, but less computationally complex – we had similar results regardless of estimator

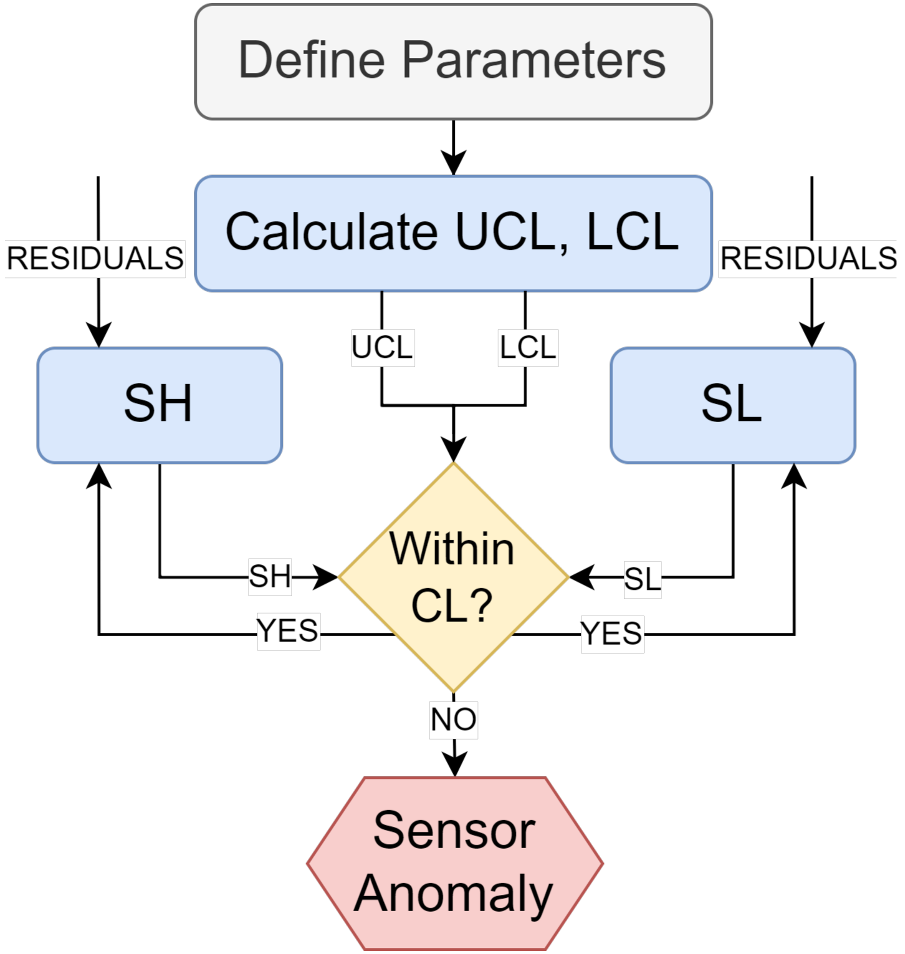


Simplified EKF Flowchart

Cumulative Sum (CUSUM) Algorithm

- Recursive sum applied for FDIA detection
- Uses a priori measurement residual calculated by the estimator and model
- In some cases, was able to identify the targeted sensor and classify the bias of the attack as positive or negative

General CUSUM Rules
Detection
If SH > UCL or SL < LCL → FDIA Detected
Identification
If SH or SL of Sensor X diverges → FDIA injected in Sensor X
Classification
SH > UCL → Positively biased, SL < LCL → Negatively biased

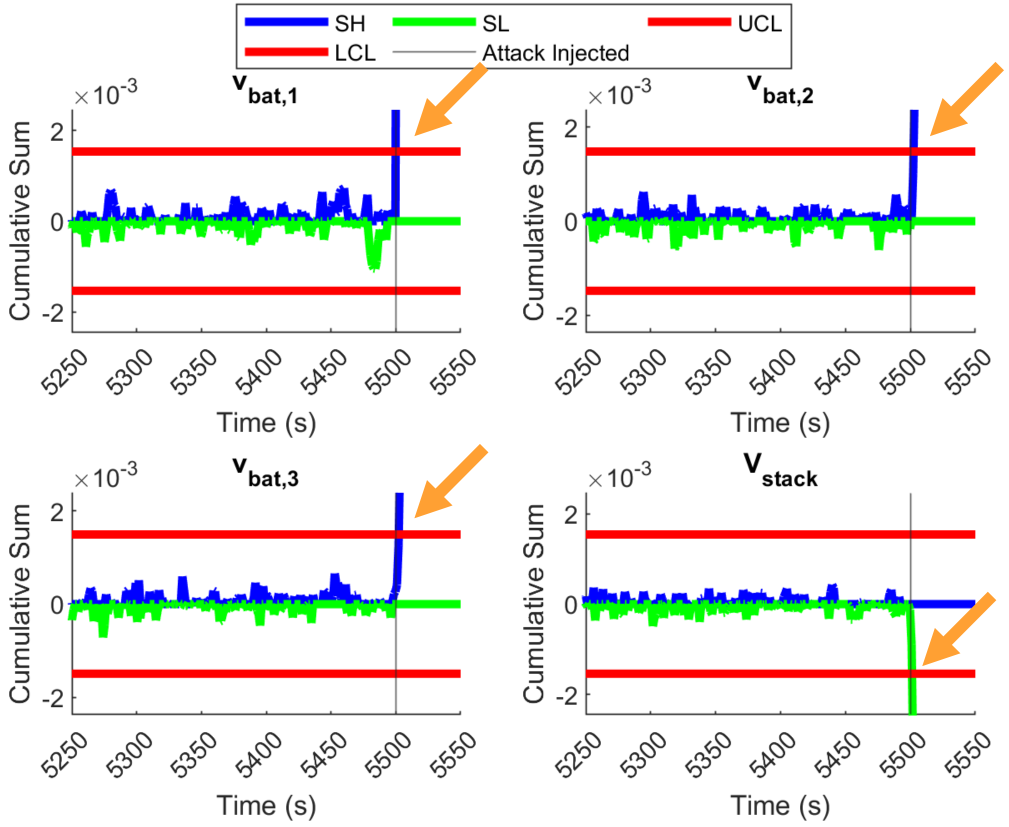


Simplified CUSUM Flowchart

Simulation Example and Results

Simulation Setup	
Battery Models	ECM + CRM
Estimator	EKF
Detector	CUSUM
Simulation time	8100 s
Simulations run	3200
Vulnerable Cells / Sensors	3 / 4
Attack range / resolution	$\pm 20\ mV$ / $153\ \mu V$
Input Current	$\pm$ 4.0435 A

Batch Results	
False Positive Rate	0%
Detection Rate	99.90%



Output CUSUM charts when a +20 mV attack was injected in the $v_{bat,1}$ sensor at 5500 s.

Conclusion and Additional Results

- The proposed approach combined three existing methods (battery modeling, estimation, and statistical error detection) and was successful in detecting FDIAs in all tested scenarios

Case Study	A	B	C	D	E	F
Cells	1	1	3	3	3	3
Model(s)	ECM + CRM	ECM + CRM	ECM + CRM	ATDECM + CRM	SPM	ECM + CRM
Estimator(s)	KF	EKF	EKF	EKF / UKF	UKF	INAEKF
Detector(s)	CUSUM	CUSUM / chi	CUSUM	CUSUM	CUSUM / chi	CUSUM / chi
False Positive	0%	0% / 100%	0%	0% / 0%	0% / 100%	0% / 100%
Detection	91.55%	92.95% / 100%	99.90%	99.5% / 99.6%	99.83% / 100%	99.16% / 100%
Identification	n/a	n/a	n/a	95.81% / 95.75%	97% / 6.17%	98.43% / 87.46%
Classification	91.55%	n/a	n/a	95.81% / 95.75%	97% / 2.53%	n/a

Key Takeaways:

1) CUSUM was highly accurate in detection, identification, and classification (where applicable)
2) CUSUM had a false positive rate of 0%
3) CUSUM outperformed other detectors studied and was compatible with all tested models / estimators

Future Work

- Run real time simulations using Speedgoat
- Apply discussed methodology to real battery data
- Evaluate computational burden of algorithms and determine viability of implementing methods in deployed BMSs
- Realize “worst-case scenarios” of FDIAs using uncertainty propagation

Acknowledgements

This material is based upon work supported by the U.S. Department of Energy, Office of Electricity (OE), Energy Storage Division.

Special thanks to Rodrigo Trevizan and Vittal Rao.

Victoria O'Brien: vaobrie@sandia.gov

Rodrigo Trevizan: rdtrevi@sandia.gov

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY