Sandia National Laboratories

Towards Deploying Anomaly Detection Algorithms in Battery Management Systems

Victoria A. O'Brien and Rodrigo D. Trevizan
Sandia National Laboratories, Albuquerque, NM

Background

- Grid batteries require a battery management system (BMS) for a variety of functions (Fig. 1.)
- Sensor measurements are susceptible to anomalies that could interfere with state estimation (Fig. 2)

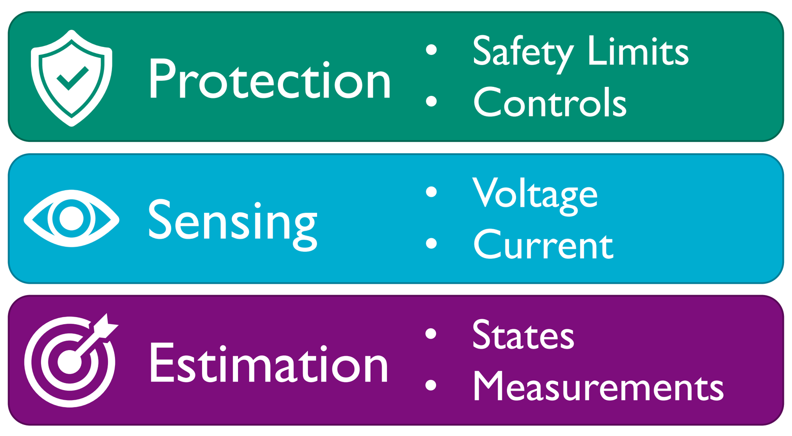

Fig. 1. Selected functions of the BMS

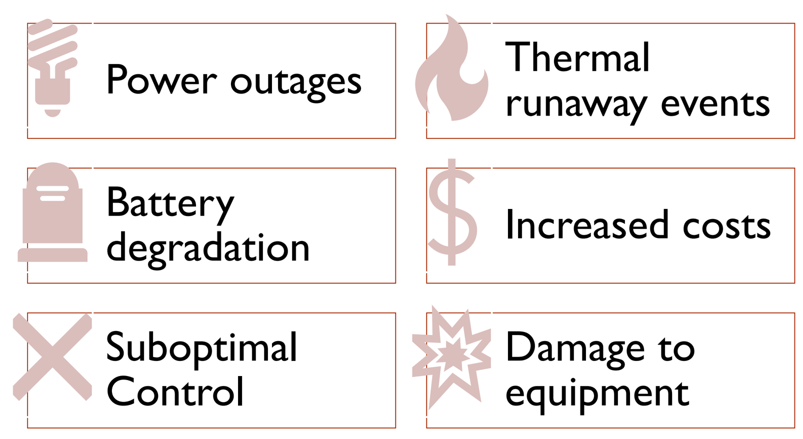

Fig. 2. Consequences of poor state estimation

Additive Bias Anomalies

- Could be caused by sensor errors, cyberattacks, excessive noise, poor calibration, faults, failures, etc.

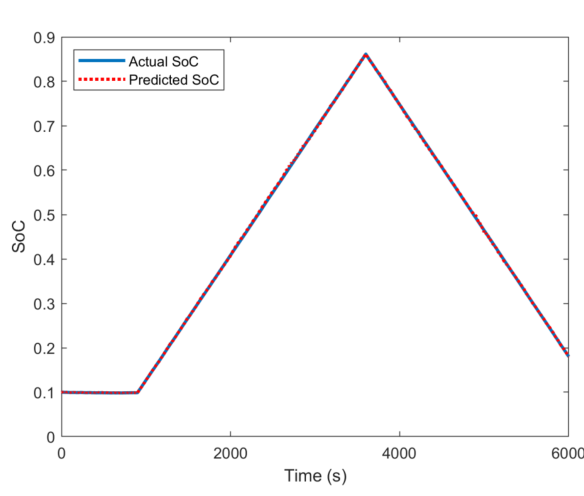

Fig. 3. Healthy SoC estimation

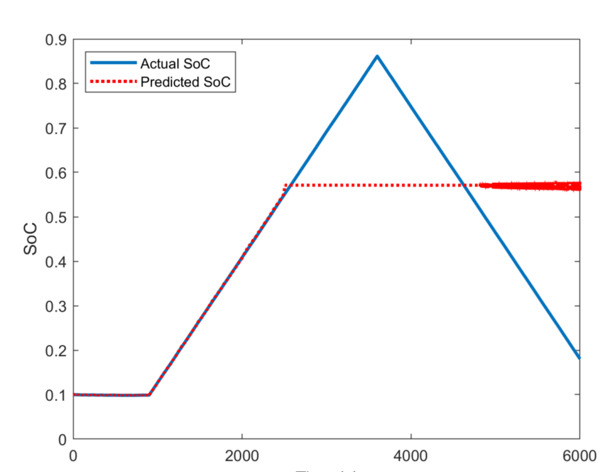

Fig. 4. SoC following -100 mV bias

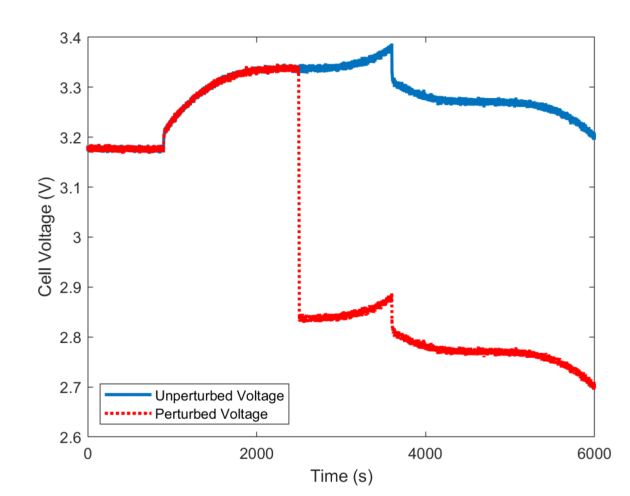

Fig. 5. Voltage following -100 mV bias

Proposed Approach

Goal: to evaluate model-based anomaly detection methods, to determine which method would be suitable for future deployment in grid-scale battery systems with modeling and estimation capabilities.

Model-Based Anomaly Detection

Step 1: Battery Modeling
Use battery models to represent system dynamics

Step 2: Nonlinear Estimation
Estimate the states and measurements

Step 3: Test Statistic
Generate the test statistics that will be used in the anomaly detection methods

Step 4: Anomaly Monitoring
Run the test statistic through an anomaly detector

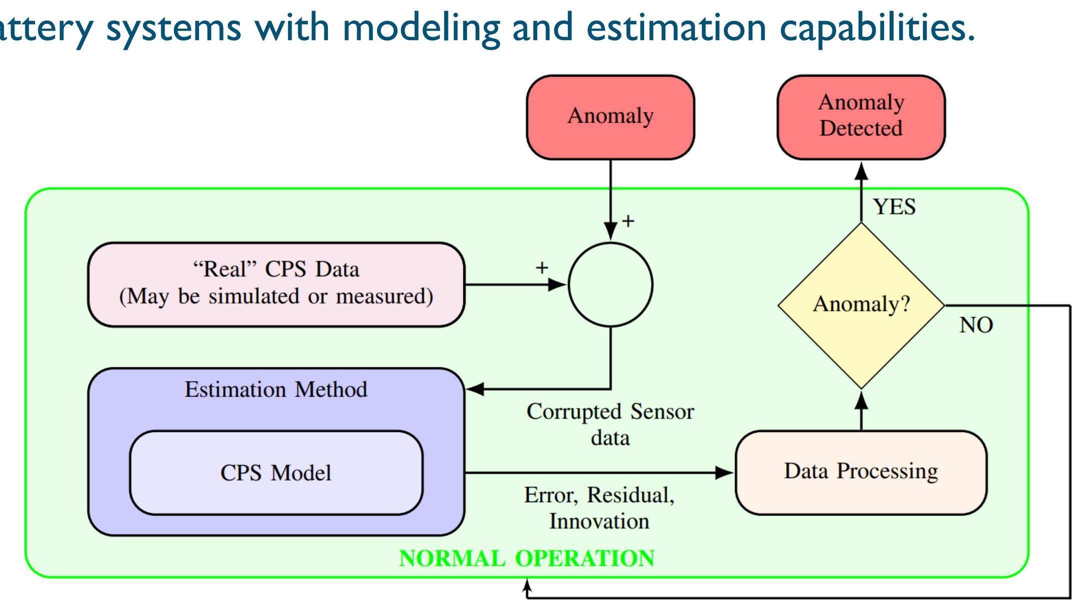

Fig. 6. Framework of a model-based anomaly detector

Battery Modeling and Estimation

- An equivalent circuit model (ECM) and charge reservoir model (CRM) are used to model the dynamics
- An unscented Kalman filter was used to estimate the states, measurements, and test statistics

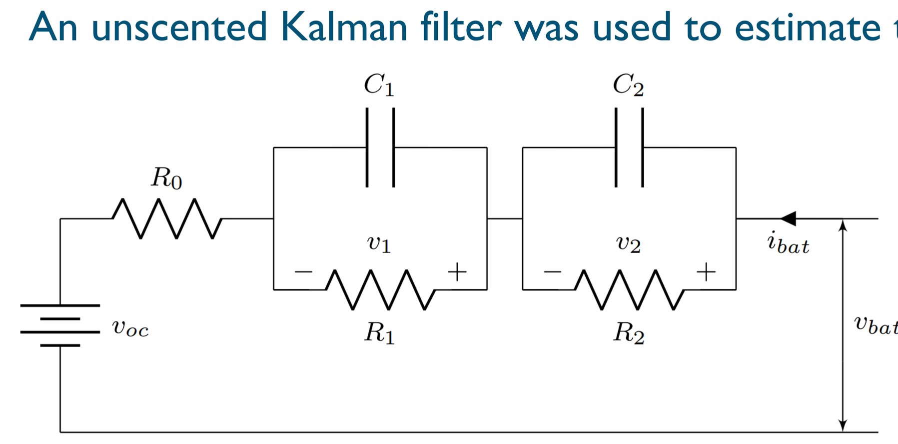

Fig. 7. ECM diagram

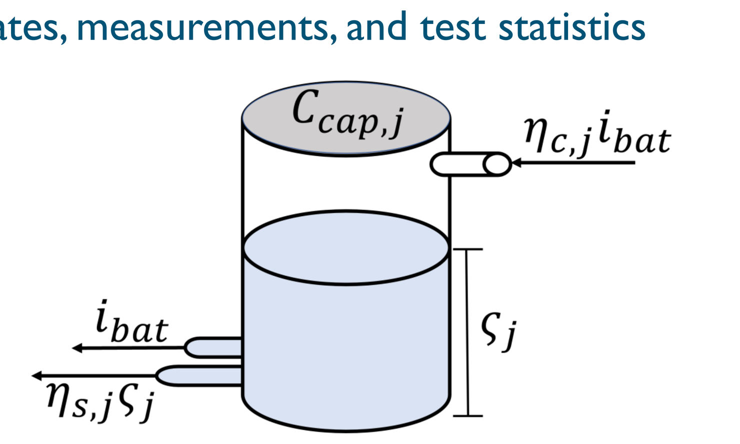

Fig. 8. CRM diagram

Anomaly Detection Overview

Chi-squared test, cumulative sum (CUSUM) algorithm, summation detector (SUM) [1], Shewhart chart ($\bar{X}$)

Table I. A Comparison of Model-Based Anomaly Detection Methods

	Chi-Squared	Cumulative Sum	Summation	$\bar{X}$ Chart
Test Statistics	1	2	1	1
Thresholds	1	2	1	2
Distribution	Chi-Squared	Normal	Chi-Squared	Normal
Has Memory?	No	Yes	Yes	No
Bias Classification?	No	Yes	No	No
Online & Offline	Yes	Yes	Yes	Yes
Tunable?	Yes	Yes	Yes	Yes
Complexity	Low	Low	Low	Low
Detection Time	Fast	Fast	Fast	Fast

[1] D. Ye and T.Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," IEEE Transactions on Cybernetics, vol. 50, no. 6, pp. 2338– 2345, June 2020.

Selected Anomaly Detection Methods

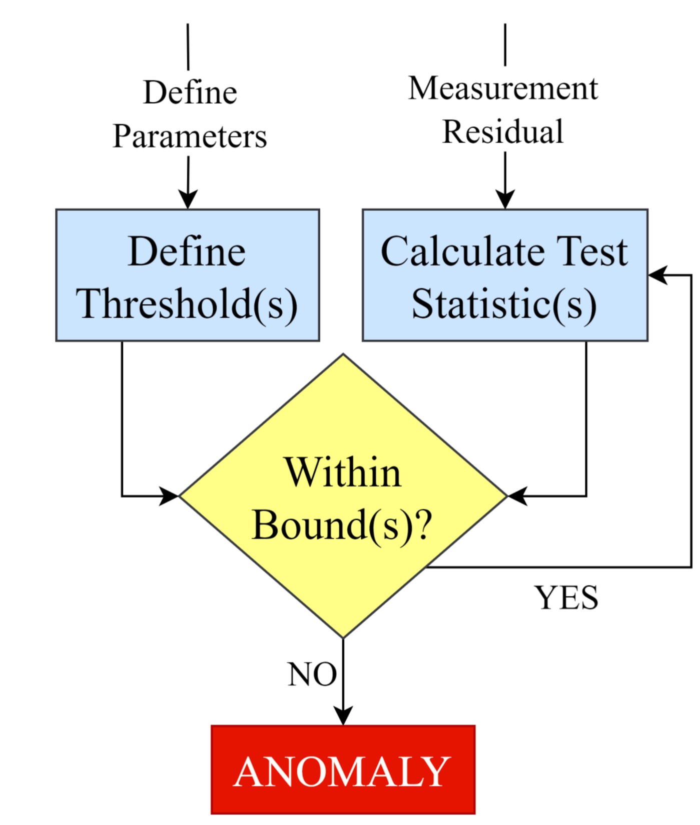

Fig. 9. Generalized detector flowchart

Table II. Anomaly Detection Equations

Chi-Squared Test	
Threshold	$F^{-1}(p\|v)$
Test Statistic	$z^T[k\|k-1]S^{-1}[k]z[k\|k-1]$
CUSUM Algorithm	
Thresholds	$\pm h\sigma_{\bar{z}}$
Test Statistics	$\max(0, \bar{z}_i - \mu - \gamma\sigma_{\bar{z}} + SH_{i-1})$ $\min(0, \bar{z}_i - \mu + \gamma\sigma_{\bar{z}} + SL_{i-1})$
SUM Algorithm [1]	
Threshold	$F^{-1}(p\|v)$
Test Statistic	$\frac{1}{k+1}\Sigma z[k\|k-1]S^{-1}[k]\Sigma z^T[k\|k-1]$
$\bar{X}$ Chart	
Thresholds	$\bar{\bar{X}} \pm A_2\bar{R}$
Test Statistic	$\bar{X} = \bar{z}_i$

Results

- More than 1000 simulations were run to evaluate the selected anomaly detection methods.
- The CUSUM algorithm was the most effective due to its high accuracy and classification capability.
- Depicted anomaly scenarios:
  - No anomaly, +50 mV anomaly at 2500 s, -300 mV anomaly at 5500, +2.5 V anomaly at 3000 s, -2 V anomaly at 4000 s

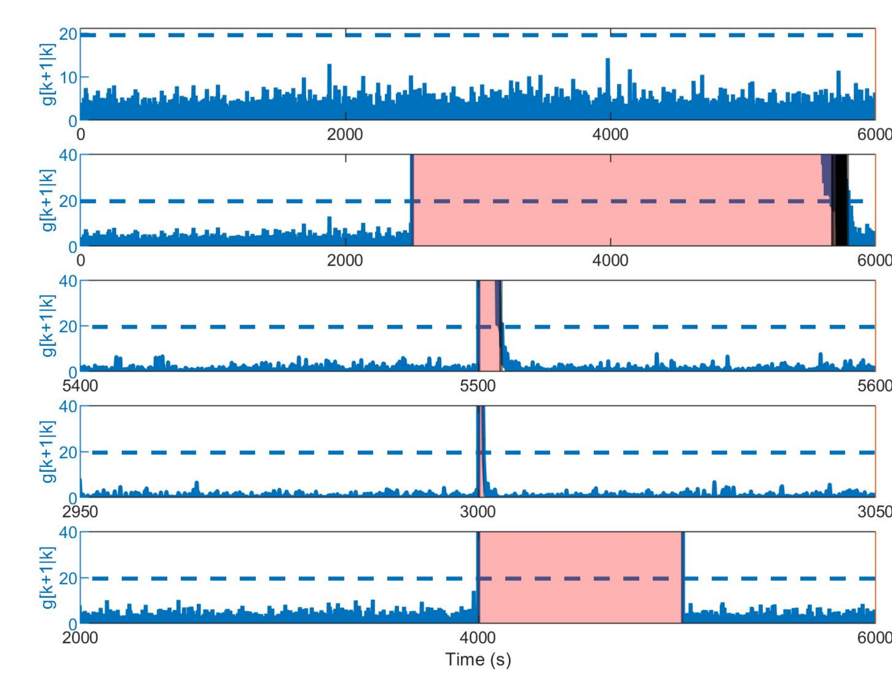

Fig. 10. Chi-Squared Detector

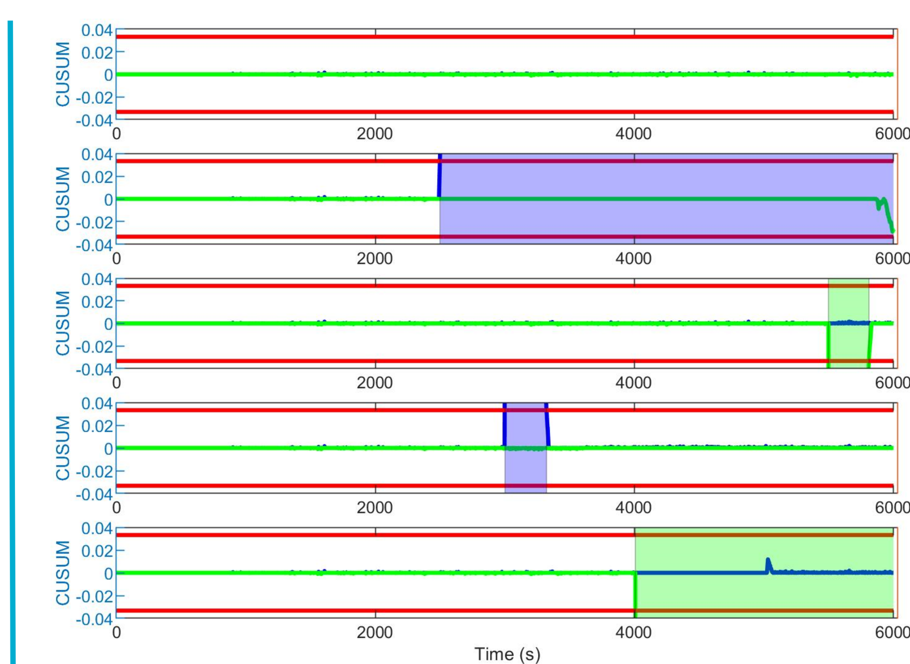

Fig. 11. CUSUM Detector

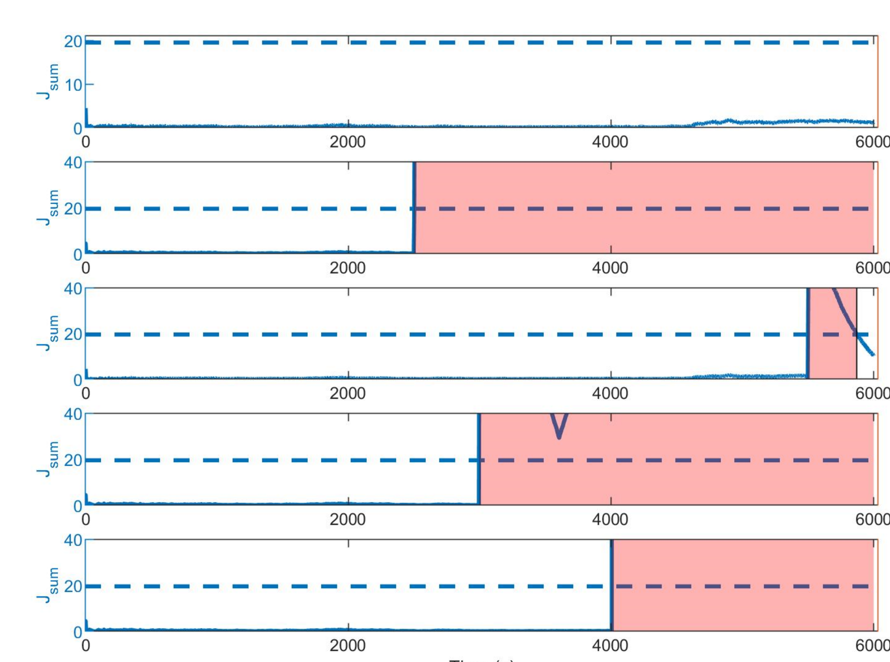

Fig. 12. SUM Detector

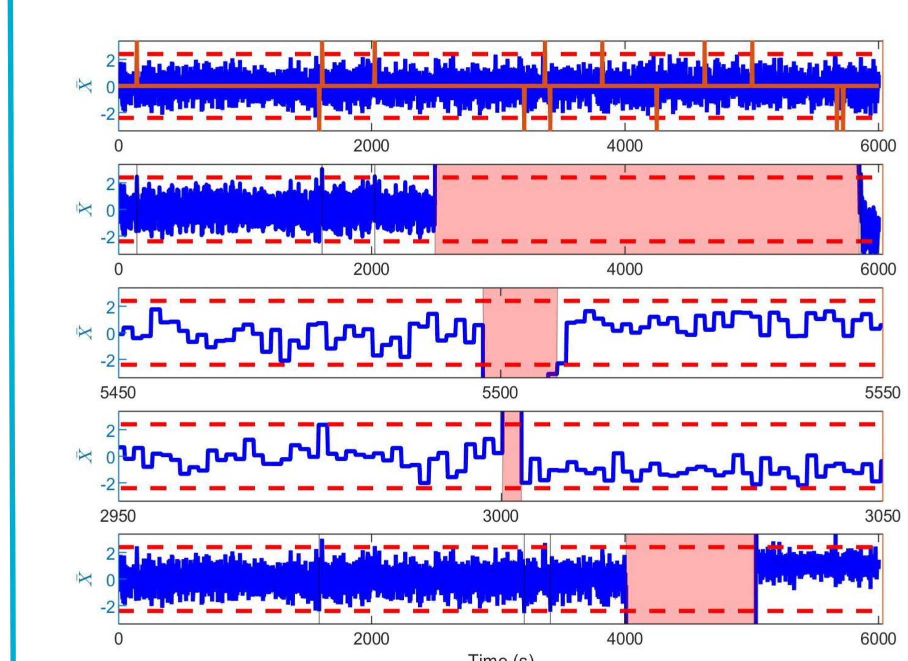

Fig. 13. $\bar{X}$ Detector

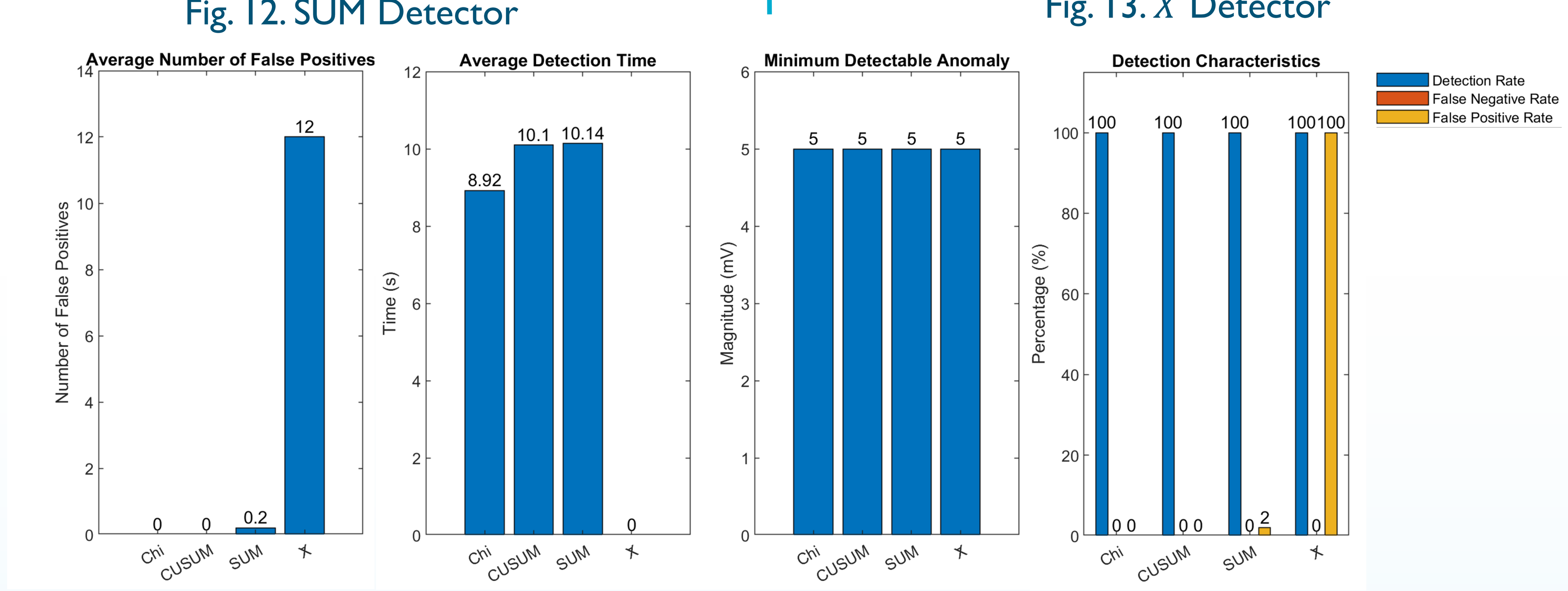

Fig. 14. Batch Simulation Results

Conclusions and Future Work

- Chi-Squared, CUSUM, and SUM had similar performance, the $\bar{X}$ chart had a high FP rate (100%).
- The CUSUM Algorithm is the best overall detector as it was able to classify the bias of the anomaly.
- CUSUM is recommended but the chi-squared test is suitable to lower the computational burden.
- Run real-time simulations using real-time testing applications, such as Speedgoat
- Apply discussed methodology to deployed battery data

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.
SAND No. SAND2024-09324C

Sandia National Laboratories

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