Sandia National Laboratories

SAND2020-9850C

Detection of False Data Injection Attacks in the State of Charge Estimation of Battery Energy Storage Systems

Rodrigo D. Trevizan[1], Victoria Obrien[2] and Vittal Rao[2]

1. Sandia National Laboratories, Albuquerque, NM 2. Texas Tech University, Lubbock, TX

Abstract: Battery Energy Storage Systems (BESS) integrate Information Technology and Operational Technology devices from multiple vendors and that are often connected to public networks. In face of these supply chain and cybersecurity threats, it is important to take a security-in-depth approach to defend ESS against cyberattacks. False data injection attacks (FDIA) have emerged as a source of stealth attacks on sensors and actuators, where the attacker attempts to cause damage or alter operations without being detected. In such scenario, the attacker designs an attack vector that minimizes the probability of detection by traditional estimation methods. In this work we evaluate possible FDIA in BESS and alternatives to detect them and mitigate their effects.

Cybersecurity of BESS

- BESS are composed by many software and hardware devices from various source
- Commercial BESS are often connected to public internet to receive software patches and updates, to communicate with servers for remote monitoring, and to receive advanced analytics services from manufacturers
- Network exposure and complex supply chain create a large surface for cyberattacks
- **Goal**: design algorithms capable of detecting false data injection attacks (FDIA) in state-of-charge (SoC) estimation

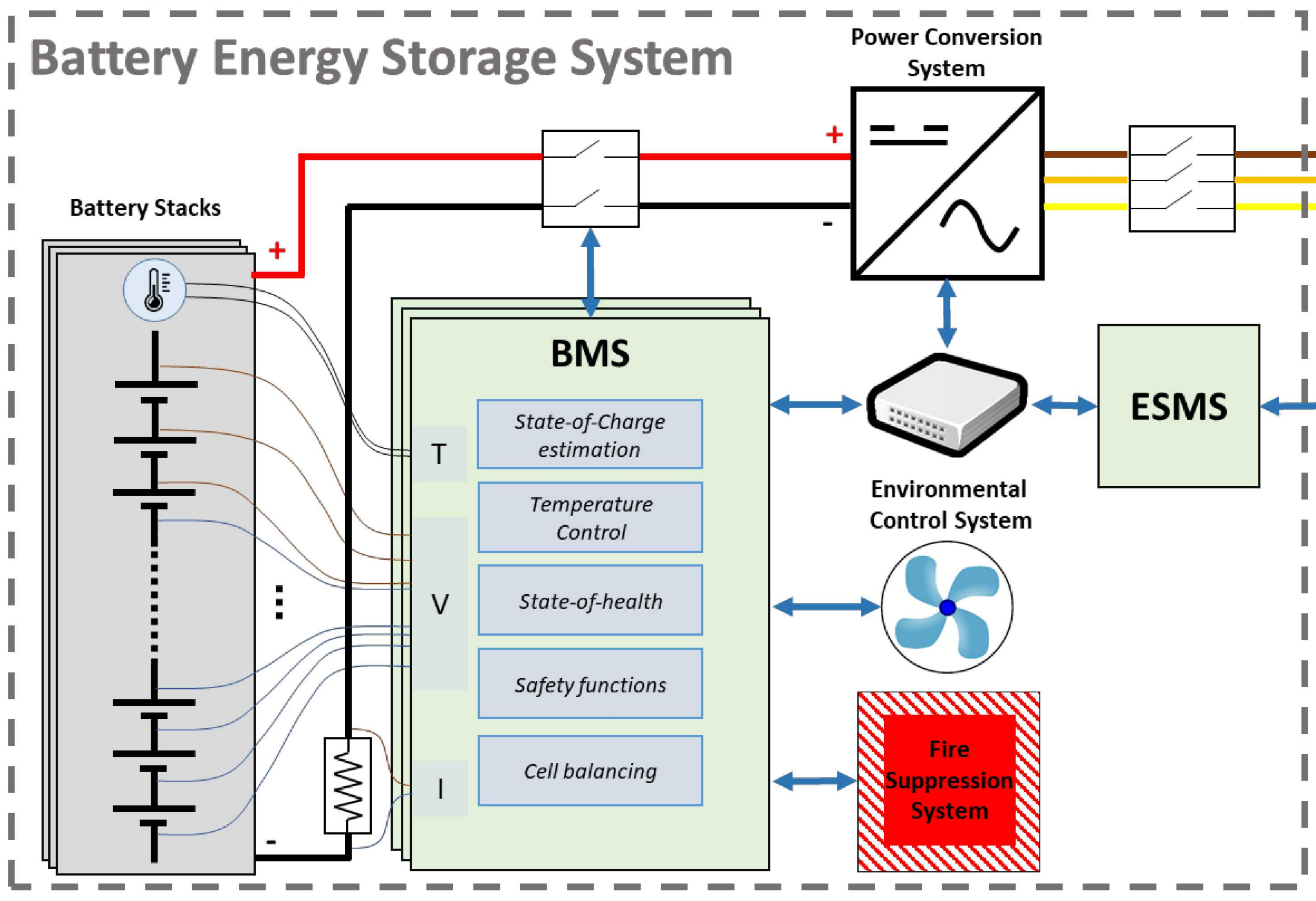

Fig. 1. Components and subsystems of a BESS.

Problem Formulation

- Accurate SoC estimation in BESS is fundamental for effective operation
- Since SoC cannot be directly measured, it is necessary to rely on estimated based on available measurements, usually by the battery management system (BMS)
- SoC can be estimated based on cell/stack voltage and stack current measurements
- One can postulate that a malicious actor can launch cyberattacks on organizations manufacturing, operating or maintaining the BESS to alter i
- **Attack model:** FDIA on sensor data in the BESS to modify its SoC

State of Charge Estimation

- A simplistic BESS model can be represented by the linear dynamics (1)[1,2]:

$$\begin{aligned}\dot{\mathbf{x}} &= \mathbf{Ax} + \mathbf{Bu}\\ \mathbf{y} &= \mathbf{Cx} + \mathbf{Du}\end{aligned} \qquad (1)$$

- Often, a recursive model-based state estimator implemented in a computer, such as a Discrete Kalman Filter[1,2], is used to estimate SoC.

- **x**: vector of states, **u**: system inputs
- **y**: vector of system measurements
- **A**: state transition matrix
- **B**: control input model
- **C**: observation model
- **D**: control input observation model
- $\mathbf{P}[k|k-1]$: covariance of state prediction

State-of-Charge Estimation Model

- Charge reservoir model with 1st order equivalent circuit given by (1) – (5):

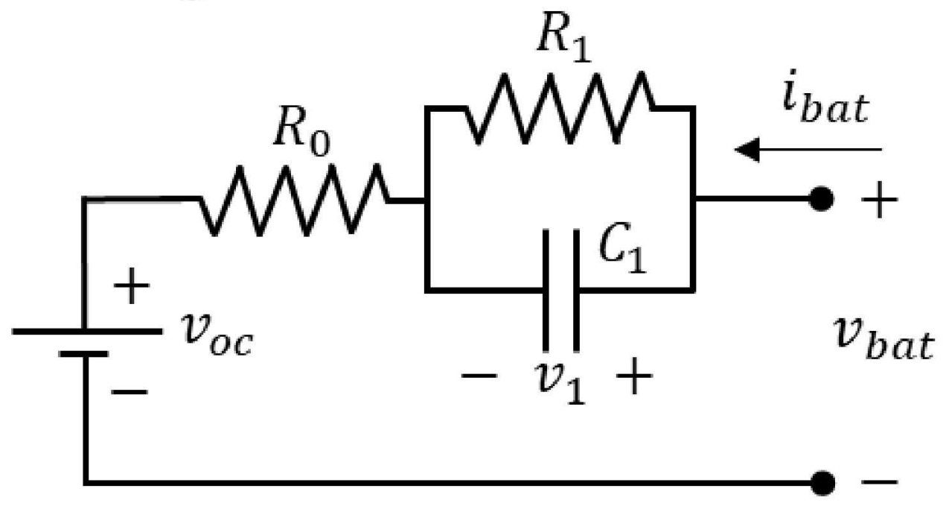

Fig. 2. 1st order equivalent circuit.

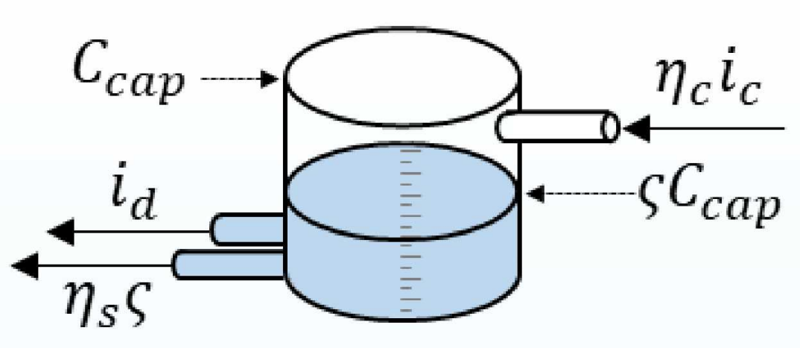

Fig. 3. Charge reservoir model.

$$\frac{\partial v_1}{\partial t} = -\frac{1}{R_1 C_1} v_1 + \frac{1}{C_1}(i_c + i_d) \qquad (1)$$

$$v_{bat} = v_{oc} + R_0 i_{bat} + v_1 \qquad (2)$$

$$i_{bat} = i_c + i_d \qquad (3)$$

$$\dot{\varsigma} = \frac{1}{C_{cap}}(\eta_c i_c + i_d) - \eta_s \varsigma \qquad (4)$$

$$v_{oc} = \gamma\varsigma + v_0 \qquad (5)$$

- ς: SoC
- v_1: voltage of capacitor C_1
- v_{bat}: battery terminal voltage

- Linearizing these equations, we obtain the state-space representation:

$$\mathbf{A} = \begin{bmatrix} -\frac{1}{R_1 C_1} & 0 \\ 0 & -\eta_s \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \frac{1}{C_1} & \frac{1}{C_1} \\ \frac{\eta_c}{C_{cap}} & \frac{1}{C_{cap}} \end{bmatrix}, \quad \begin{aligned} &\mathbf{C} = [1 \quad \gamma], \mathbf{D} = [R_0 \quad R_0] \\ &\mathbf{y} = [\Delta v_{bat}], \mathbf{x} = \begin{bmatrix} v_1 \\ \varsigma \end{bmatrix}, u = \begin{bmatrix} i_c \\ i_d \end{bmatrix} \\ &\Delta v_{bat} = \gamma\varsigma + R_0 i_{bat} + v_1 \end{aligned} \qquad (6)$$

False Data Injection Attacks

- A FDIA that is not detected by residual-based bad data detection methods of static linear state estimators can be obtained if the malicious actor has knowledge of the system's parameters and measurements[3]
- With that information, it is possible to determine which and by how much measurements have to be modified such that the result of the state estimation determined by the attacker is obtained
- Such attack vector, $\Delta\mathbf{y_a}$, can be used to modify the estimated state of a system from $\hat{\mathbf{x}}$ to $\hat{\mathbf{x}}_\mathbf{a}$by injecting an attack vector in the measurements:

$$\mathbf{y_a} = \mathbf{y} + \Delta\mathbf{y_a} \qquad (7) \qquad\qquad \Delta\mathbf{y_a} = \mathbf{C}(\hat{\mathbf{x}}_\mathbf{a} - \hat{\mathbf{x}}) \qquad (8)$$

Detection of FDIA

- To detect (8), the FDI detector (10) based on innovation (9) is designed

$$\mathbf{z}[k|k-1] = \mathbf{y}[k] - \hat{\mathbf{y}}[k|k-1] \qquad (9)$$

$$g[k|k-1] = \mathbf{z}[k|k-1]^T \mathbf{P_z}[k|k-1]^{-1} \mathbf{z}[k|k-1] \qquad (10)$$

$$\mathbf{P_z}[k|k-1] = \mathbf{CP}[k|k-1]\mathbf{C}^\mathrm{T} + \mathbf{R} \qquad (11)$$

Results

- To test the effectiveness of this detector, a model of a battery based on data from Ref. 2 was developed in Simulink, along with a discrete linear Kalman Filter and a static SoC estimator.
- An attacker manipulates i_{bat} and v_{bat} measurements to increase SoC by 10% at t=60s , which are not detected by the static estimator

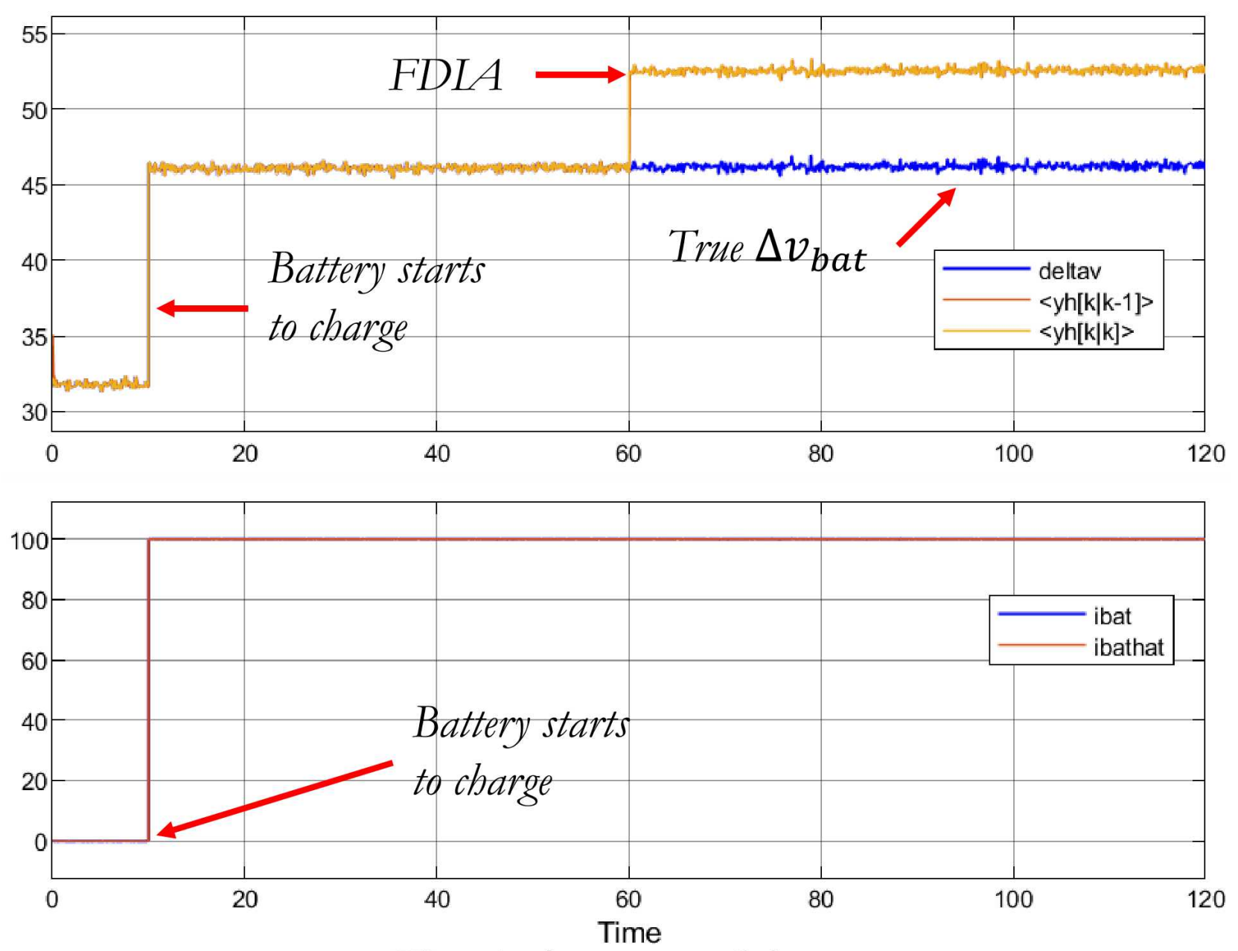

Fig. 4. Δv_{bat} and i_{bat}.

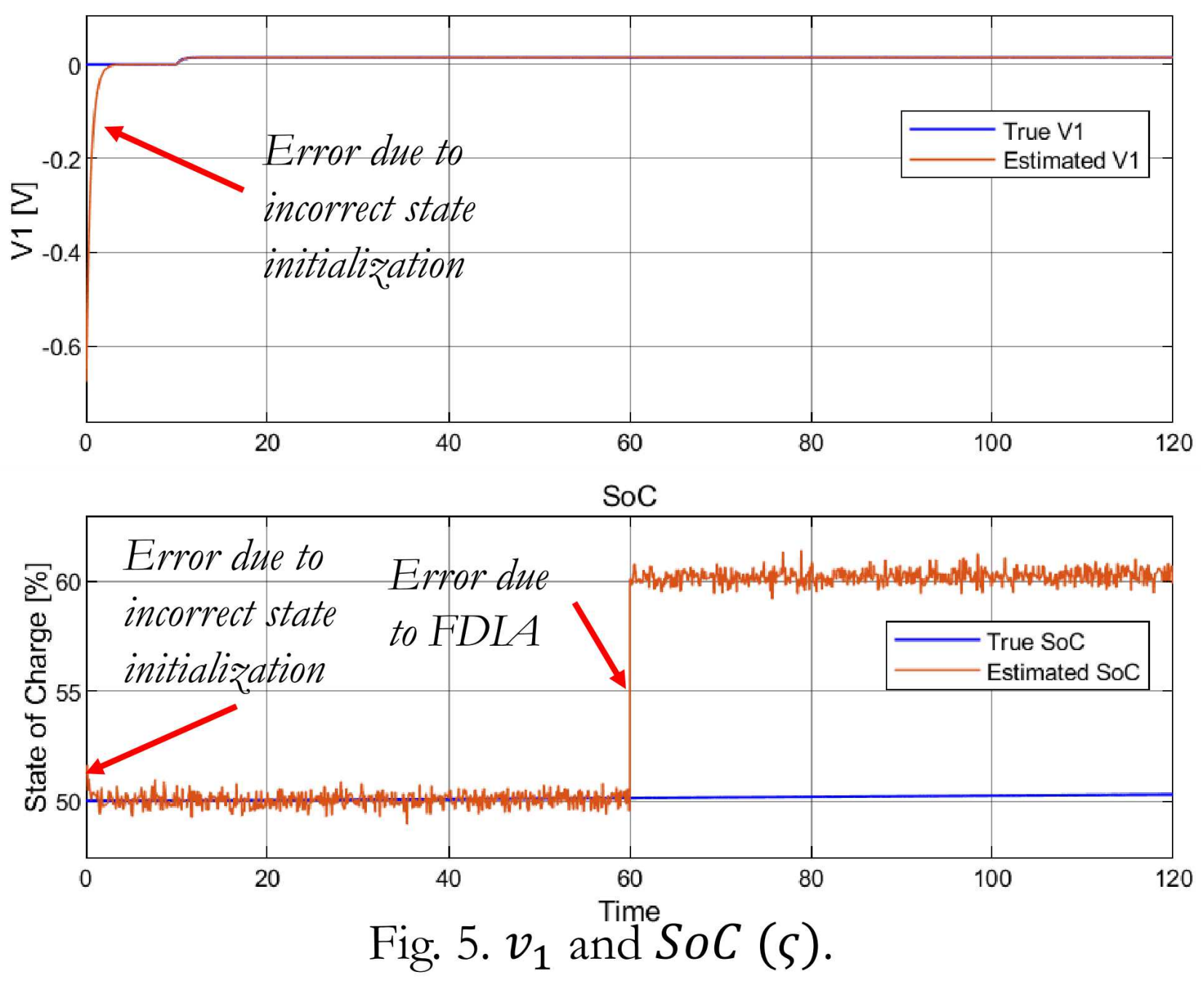

Fig. 5. v_1 and SoC (ς).

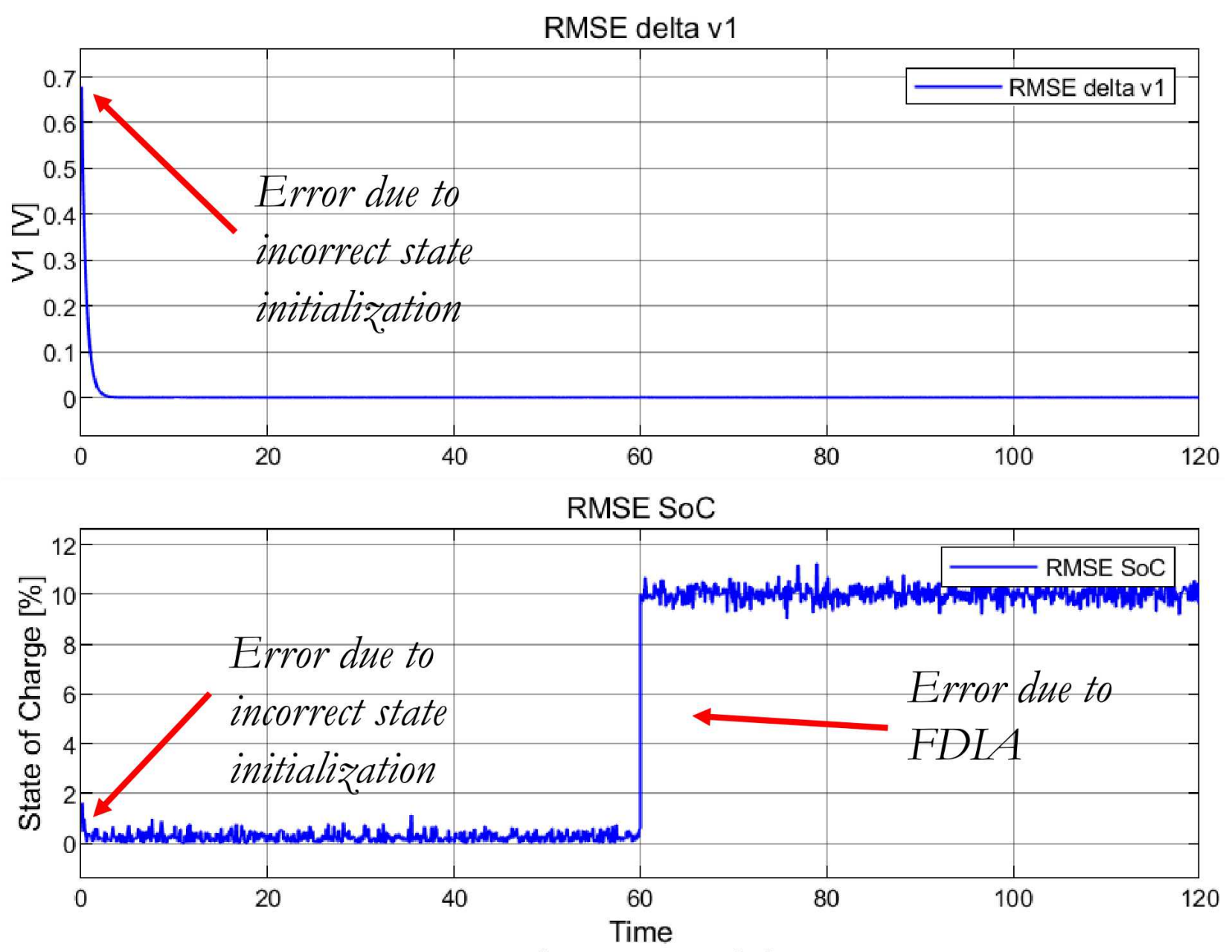

Fig. 6. Δv_{bat} and i_{bat}.

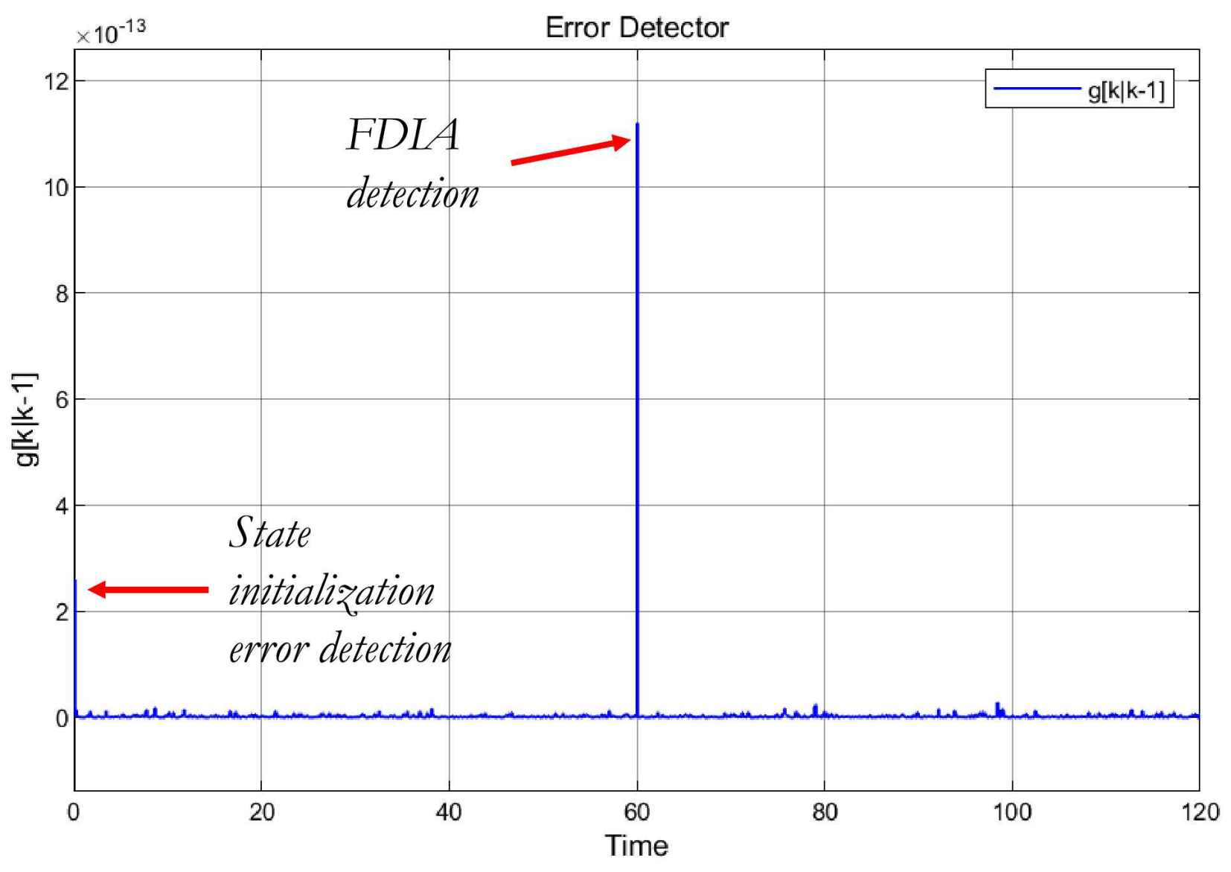

Fig. 7. Detector results.

Conclusion

- Stealthy FDIA designed for static estimators can affect dynamic SoC estimation algorithms
- Adding an innovation-based detector to a SoC estimator can allow detecting step-type FDIA to states that cannot be detected by static estimators
- Future work:
  - Design detectors for more sophisticated attacks and more complex battery models

References

1. G. L. Plett, "Sigma-point Kalman filtering for battery management systems of LiPB-based HEV battery packs: Part 1: Introduction and state estimation,:"in J. Power Sources, v. 161, no. 2, pp. 1356-1368, 2006
2. D. Rosewater, S. Ferreira, D. Schoenwald, J. Hawkins and S. Santoso, "Battery Energy Storage State-of-Charge Forecasting: Models, Optimization, and Accuracy," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2453-2462, May 2019, doi: 10.1109/TSG.2018.2798165.
3. Y. Liu, P. Ning, and M.K. Reiter. "False data injection attacks against state estimation in electric power grids," in ACM Transactions on Information and System Security (TISSEC) 14, no. 1, pp. 1-33, 2011.

Acknowledgement: Funding was provided by the US DOE Energy Storage Program managed by **Dr. Imre Gyuk** of the DOE Office of Electricity Delivery and Energy Reliability.

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. ____________