SCADA Resilience via Autonomous Cyber-Physical Agents

Joseph Andrew Giampapa
PI, Senior Member of Technical Research Staff
Software Engineering Institute

Gabriela Hug-Glanzmann
Soummya Kar
Co-PIs, Assistant Professors
Electrical and Computer Engineering

Carnegie Mellon University
Pittsburgh, PA 15213

Tuesday, 4 February 2014

Disclaimer

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000954

Advisors from Industry

Kevin Ding
CenterPoint Energy
Houston, TX

Valentine Emiseh
CenterPoint Energy
Houston, TX

Dong Wei
Siemens Corporation
Princeton, NJ

Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

Cyber-Threat: False Data Injection (FDI) Attack

- Single-most critical EMS function is ***state estimation***
  - Process is ***central*** to a grid control center
  - Receives noisy remote sensor data
  - Identifies and discards ***bad data***
  - Determines ***state variables*** of the grid for power flow calculations
  - Based on this data, power grid operations are determined

- False Data Injection
  - Falsifies data that is input to state estimation
  - Has two potential impacts on operator's perception of grid state:
    - Loss of ***observability*** of power grid state
    - Perceived ***observability***, but
      - ➢ Incorrect and unsafe adjustments can be made
      - ➢ Based on misperceptions of system state due to FDI data

Outline

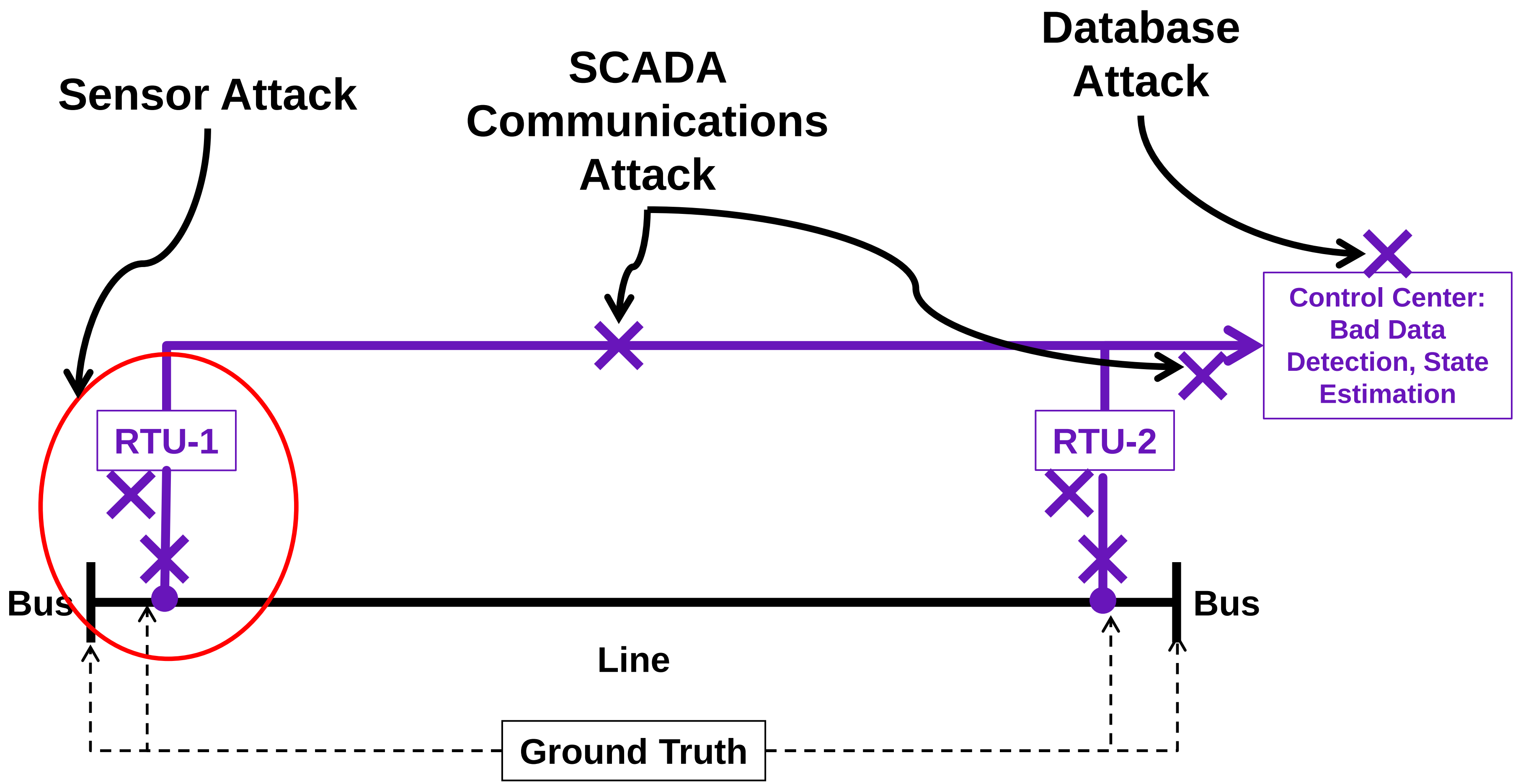
- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

Three Types of FDI Attacks

1. Sensor Attack
2. SCADA Communications Attack
3. Attack on Control Center Centralized Database

- Each type of attack is detectable and/or identifiable in isolation
  - Combinations of attacks are not yet considered

Schematic of Attacks



Sensor Attack

- With complete sensor agent coverage
  - We can *detect* and *identify* an attacked sensor.
  - Complete: one agent per sensor, one sensor per bus
  - As long as the set of non-attacked measurements constitute an observable set of measurements.
- Caveat: most grids do not deploy complete sensor coverage.
- For a specific grid, observability analysis will need to be performed before guarantees can be made.

SCADA Communications Attack

- We can *detect* the presence of an attack
  - It can be *localized* if the communications topology is radial
    - All sensors communicate directly with the control center
  - And if the sensors from which the readings are made are from an observable set of measurements
- In the event of non-radial communications topology:
  - Localization of attack will depend and need to be analyzed per segment
  - Assurance claims can still be made that inform area of compromise.

Database Attack

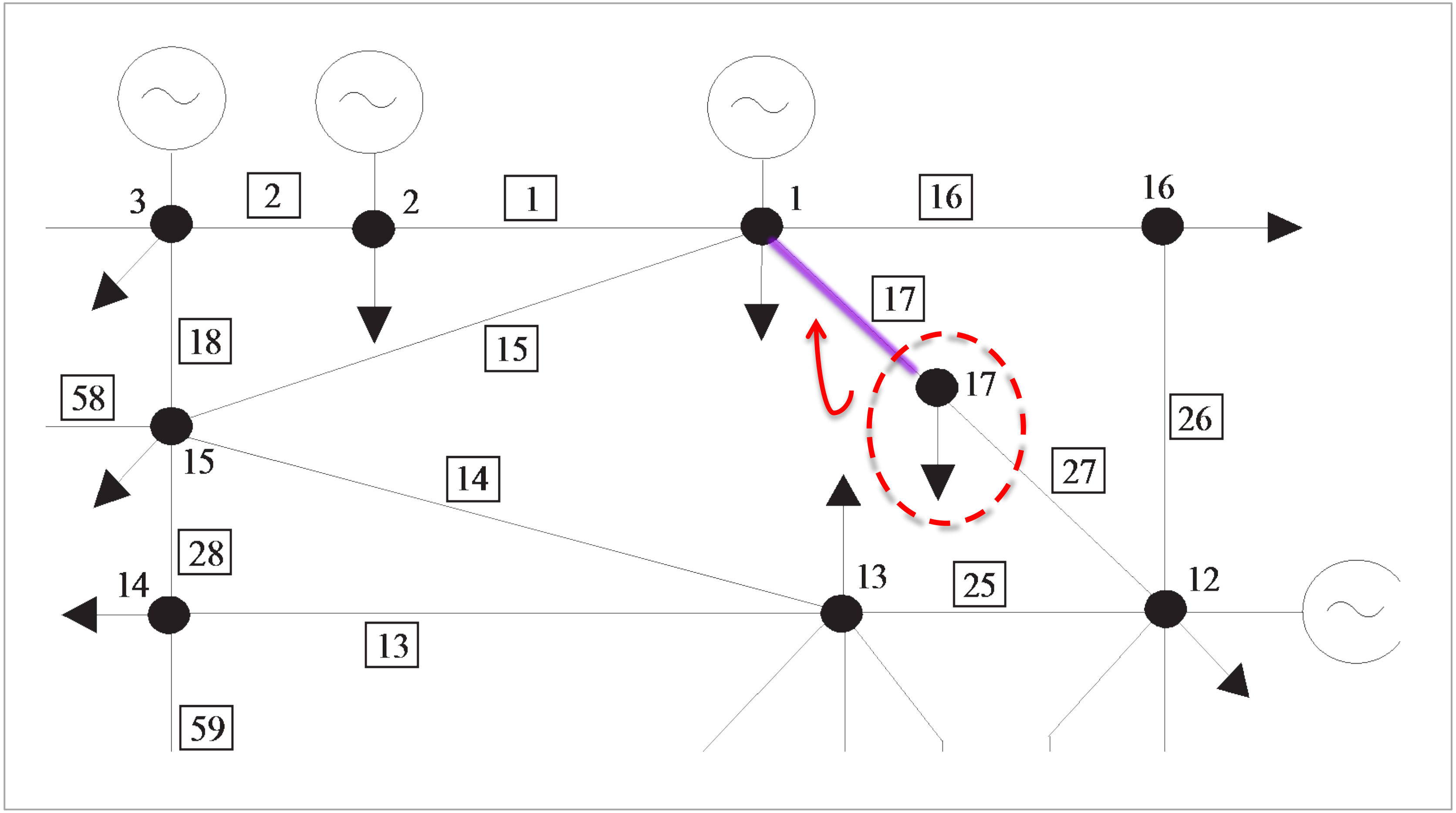
- An FDI attack can be *detected* and *localized* to DB
  - Via distributed state estimation performed by the agents
  - Assuming that all communications are secure, and that we have an
  - Observable set of measurements from the sensors

Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

Illustrative example

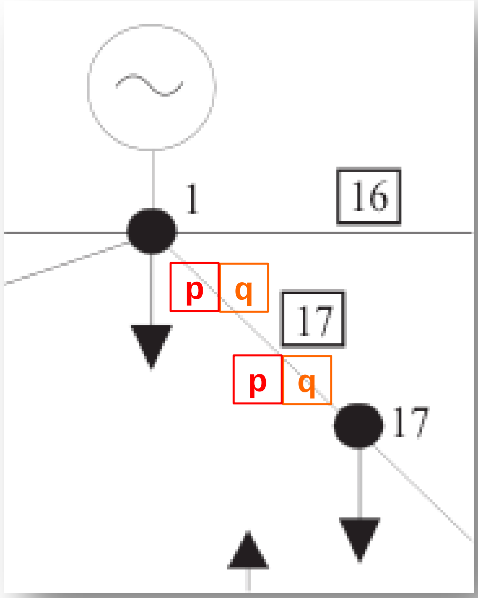
Consider an attack on line 17 to induce a load shed situation targeting bus 17 …



Illustrative example: FDI

Impact on the Line 17:

Line 17					
Type	Line Number	From Bus	To Bus	**Detection likely?**	**Mismatch (Std Dev)**
Pline	17	1	17	**No**	**18.990**
Pline	17	17	1	**No**	**18.690**
Qline	17	1	17	**No**	**3.469**
Qline	17	17	1	**No**	**4.840**



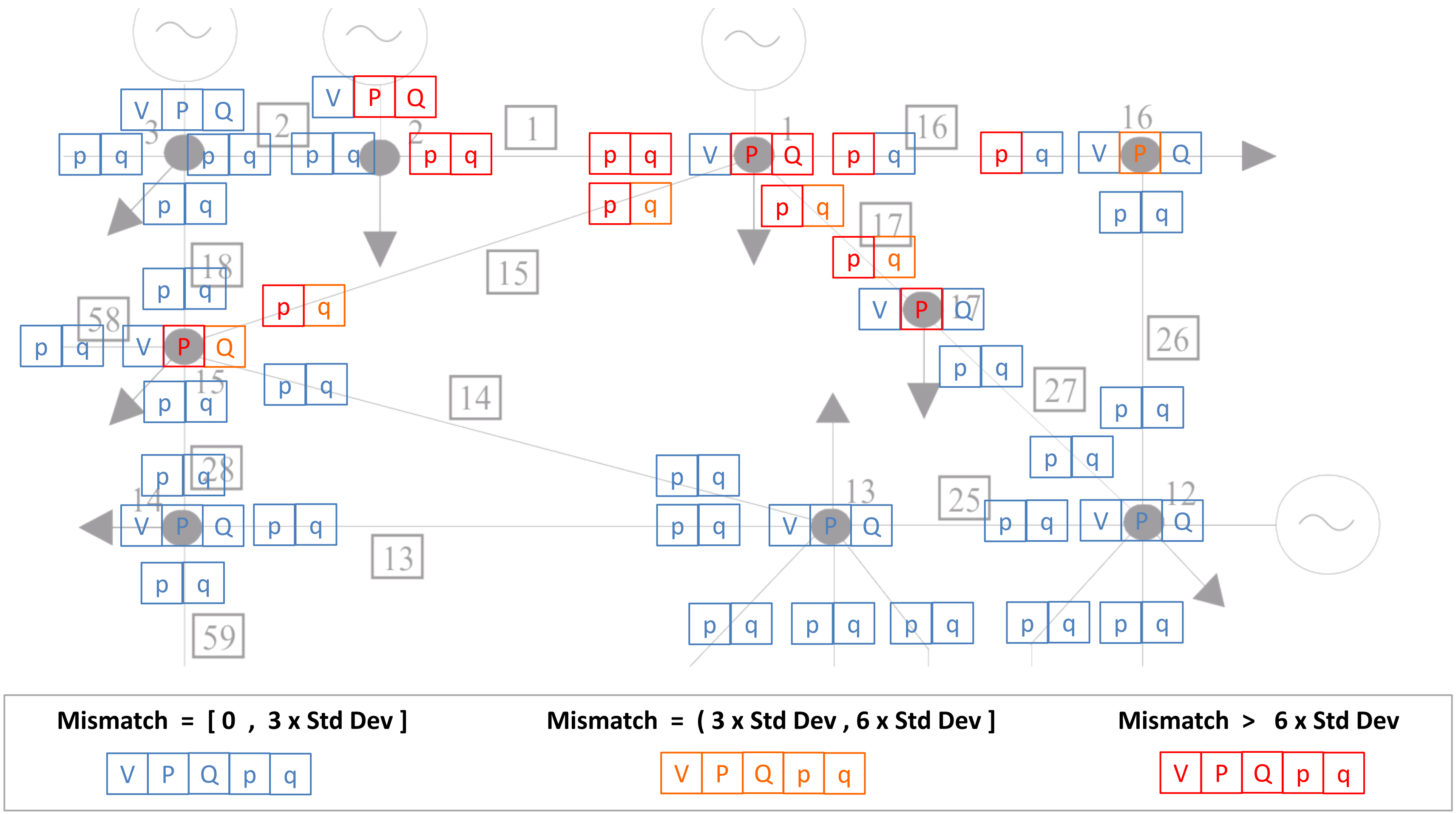
Legend:

V	Voltage magnitude measurement
P	Active power injection measurement
Q	Reactive power injection measurement
p	Active power flow measurement
q	Reactive power flow measurement
V P Q p q (blue)	Undetected ; Mismatch = [0 , 3 x Std Dev]
V P Q p q (orange)	Undetected ; Mismatch = (3 x Std Dev , 6 x Std Dev]
V P Q p q (red)	Undetected ; Mismatch > 6 x Std Dev
V P Q p q (black)	Detected

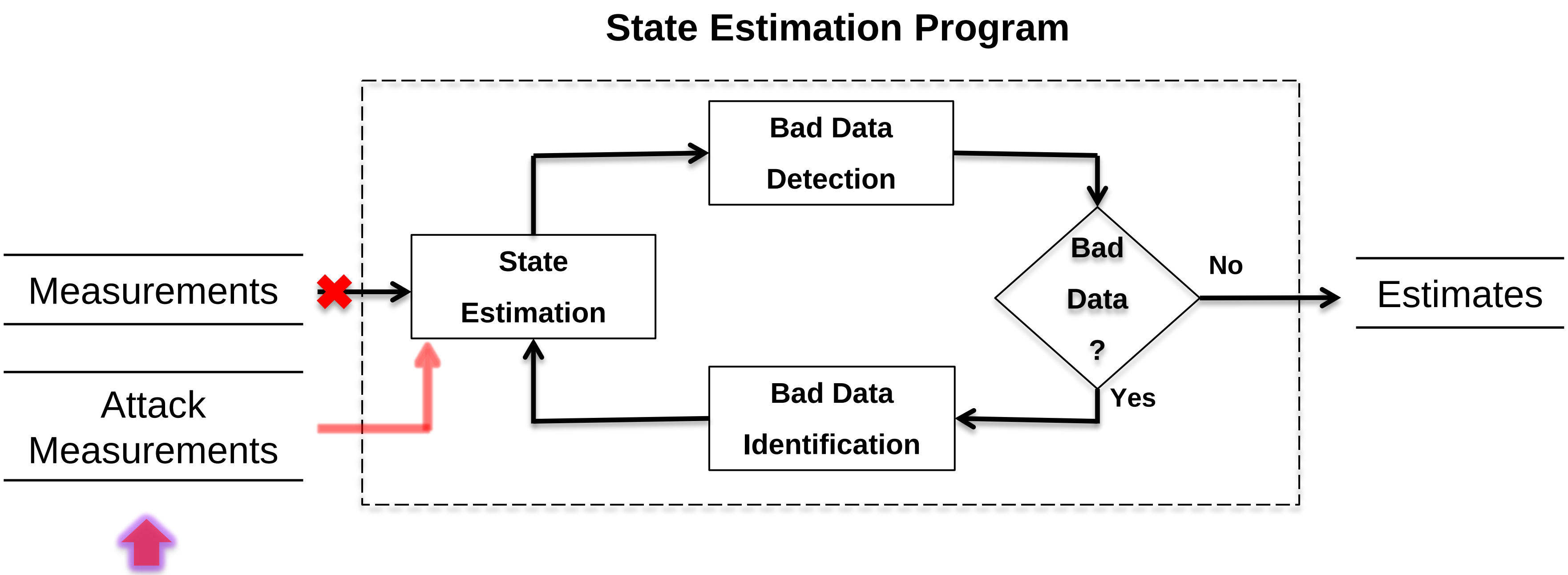
Illustrative example: FDI

Observations:

The extent of the impact diminishes with distance from the point of attack, e.g. line 17.



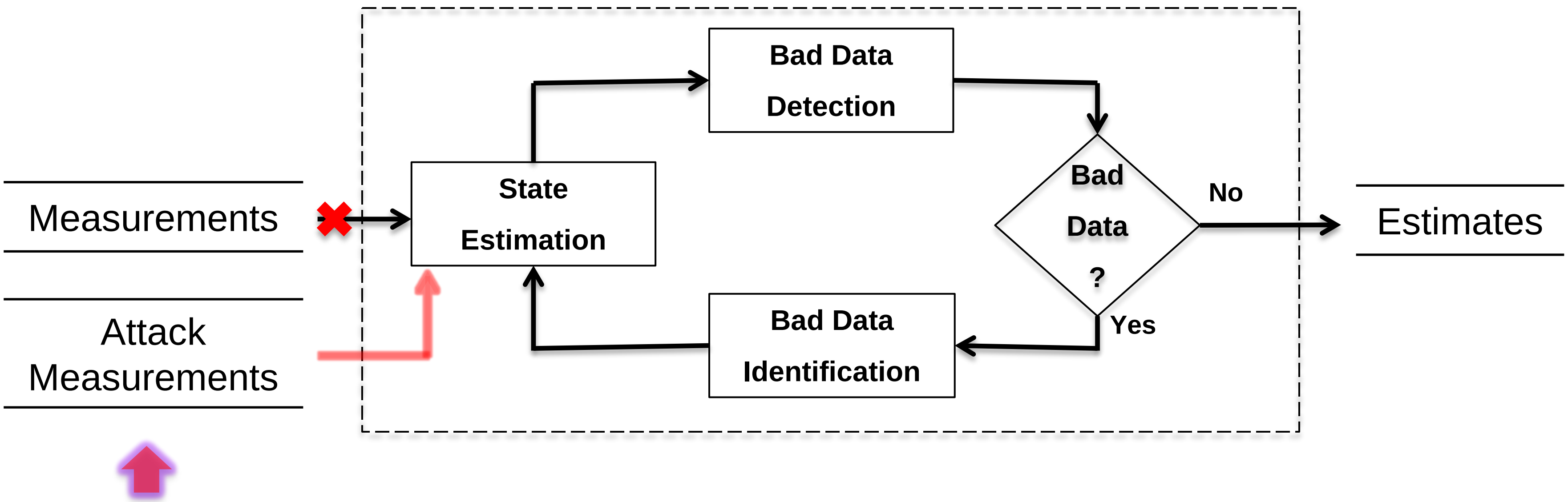
Illustrative example: FDI



Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	**0.453**
Pline	17	17	1	**-0.448**
Qline	17	1	17	**0.072**
Qline	17	17	1	**-0.081**

Illustrative example: FDI

State Estimation Program



Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	**0.453**
Pline	17	17	1	**-0.448**
Qline	17	1	17	**0.072**
Qline	17	17	1	**-0.081**

Measurement Model:

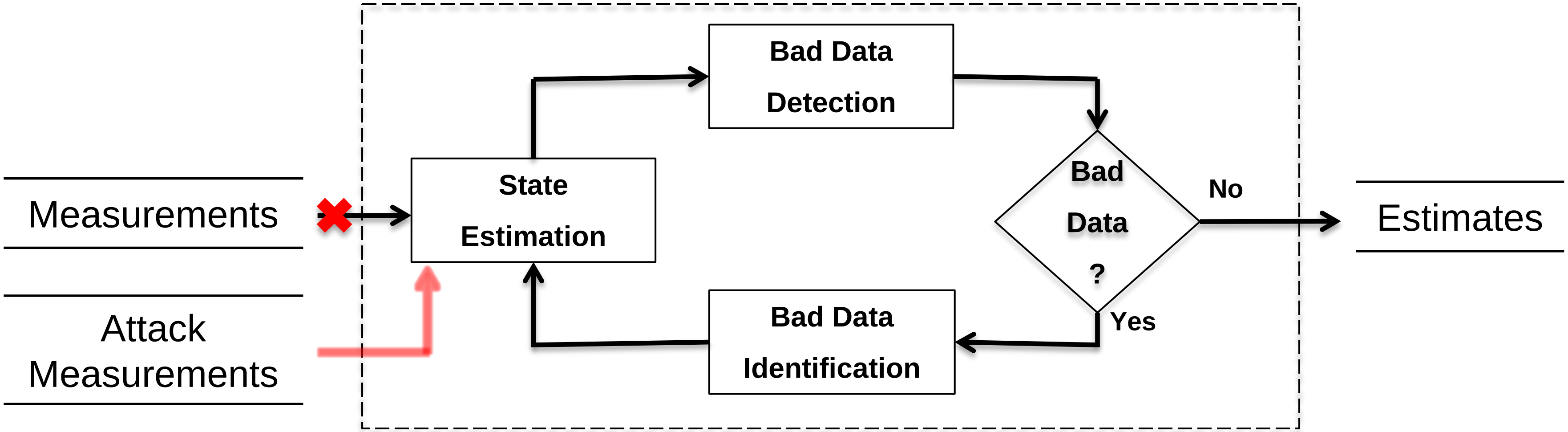
Measurement = Ground Truth + Random Error + **FDI**

where

Ground Truth: Actual physics of grid
Random error: Gaussian noise ~ N(0 , Std Dev)
Std Dev: Sensor precision
FDI: Highly structured error

Illustrative example: FDI

State Estimation Program



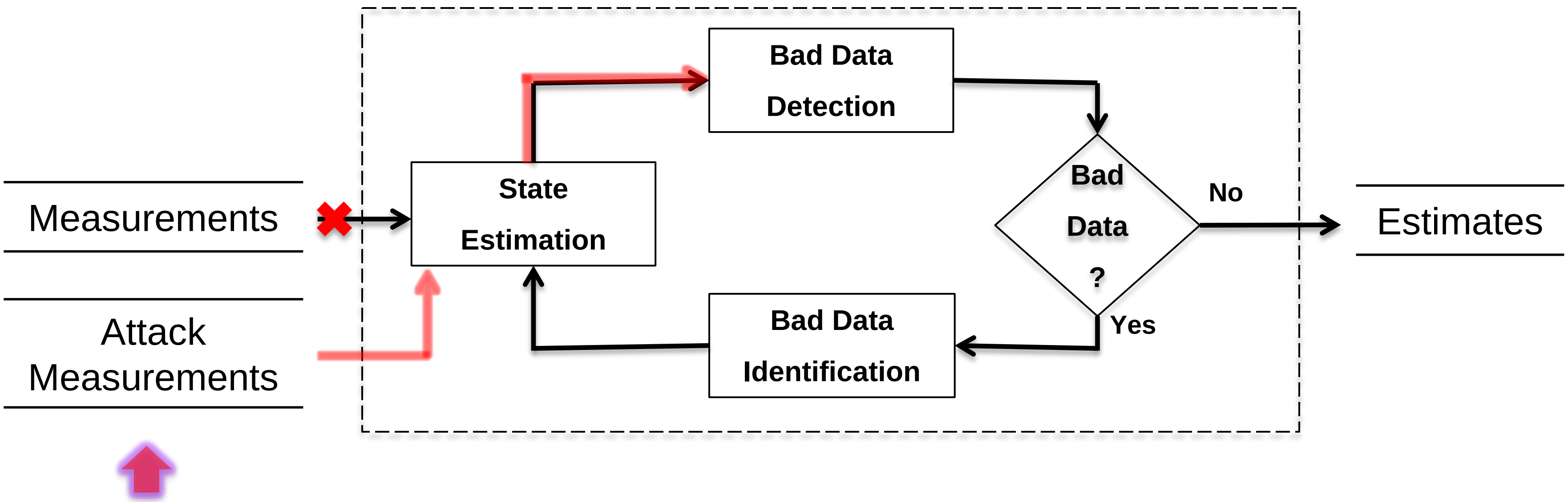
Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	**0.453**
Pline	17	17	1	**-0.448**
Qline	17	1	17	**0.072**
Qline	17	17	1	**-0.081**

Measurement Model:

Ground Truth (p.u.)	FDI (p.u.)	Random Error (p.u.)	Std Dev (p.u.)
0.301	1.448E-01	7.111E-03	8.000E-03
-0.299	-1.501E-01	5.538E-04	8.000E-03
0.100	-3.176E-02	4.011E-03	8.000E-03
-0.120	3.440E-02	4.323E-03	8.000E-03

FDIs are large relative to Std Devs. Unlike Gross Errors, FDIs are strategically designed using the attacker’s knowledge of the grid.

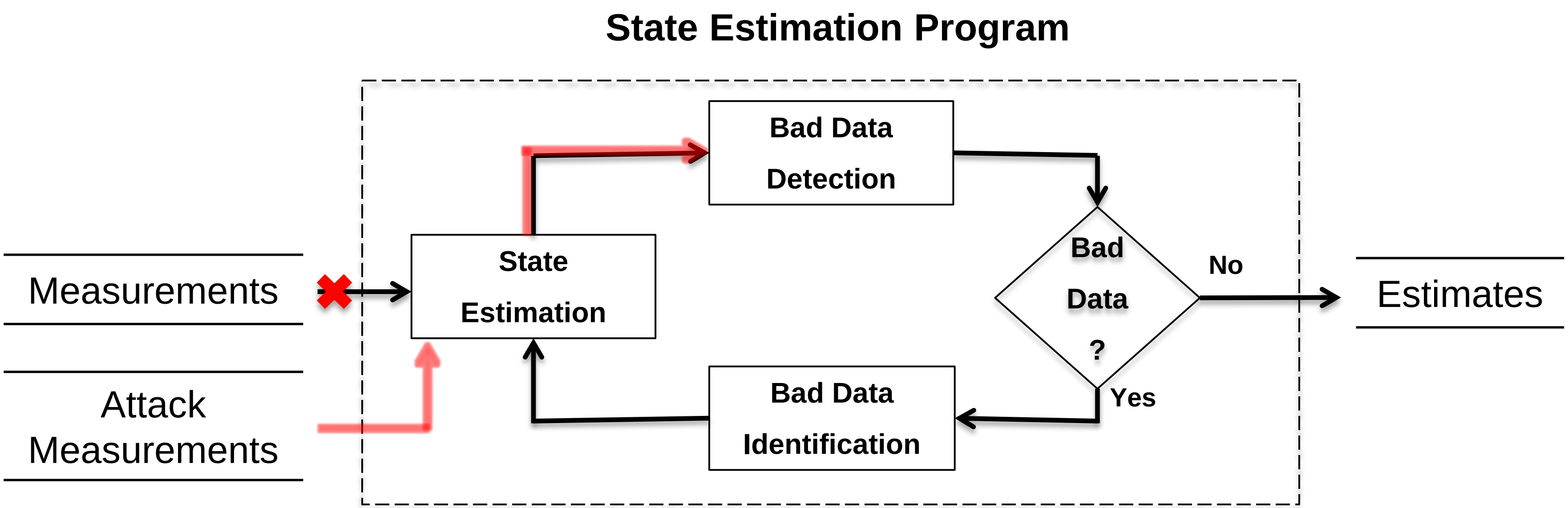
Illustrative example: FDI



Line 17				
Type	**Line Number**	**From Bus**	**To Bus**	**Measurements (p.u.)**
Pline	17	1	17	**0.453**
Pline	17	17	1	**-0.448**
Qline	17	1	17	**0.072**
Qline	17	17	1	**-0.081**

Estimation Results:

Illustrative example: FDI



Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	0.453
Pline	17	17	1	-0.448
Qline	17	1	17	0.072
Qline	17	17	1	-0.081

V.S.

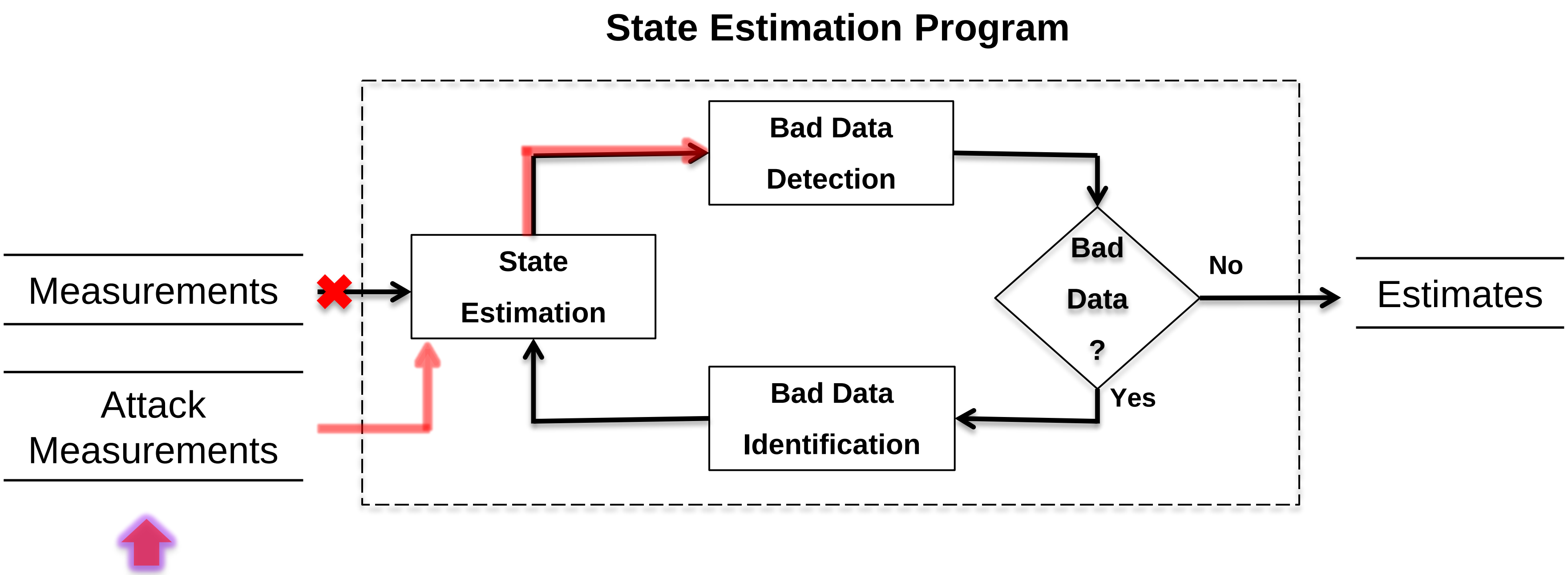
Estimation Results:

Estimates (p.u.)	Residuals (p.u.)	Weighted Residuals (p.u.)
0.453	1.080E-07	1.350E-05
-0.448	1.370E-07	1.713E-05
0.072	3.774E-07	4.718E-05
-0.081	7.335E-07	9.169E-05

Ground Truth (p.u.)
0.301
-0.299
0.100
-0.120

Estimates and measurements agree perfectly, but there are huge discrepancies when compared Ground Truth.

Illustrative example: FDI



Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	0.453
Pline	17	17	1	-0.448
Qline	17	1	17	0.072
Qline	17	17	1	-0.081

Estimation Results:

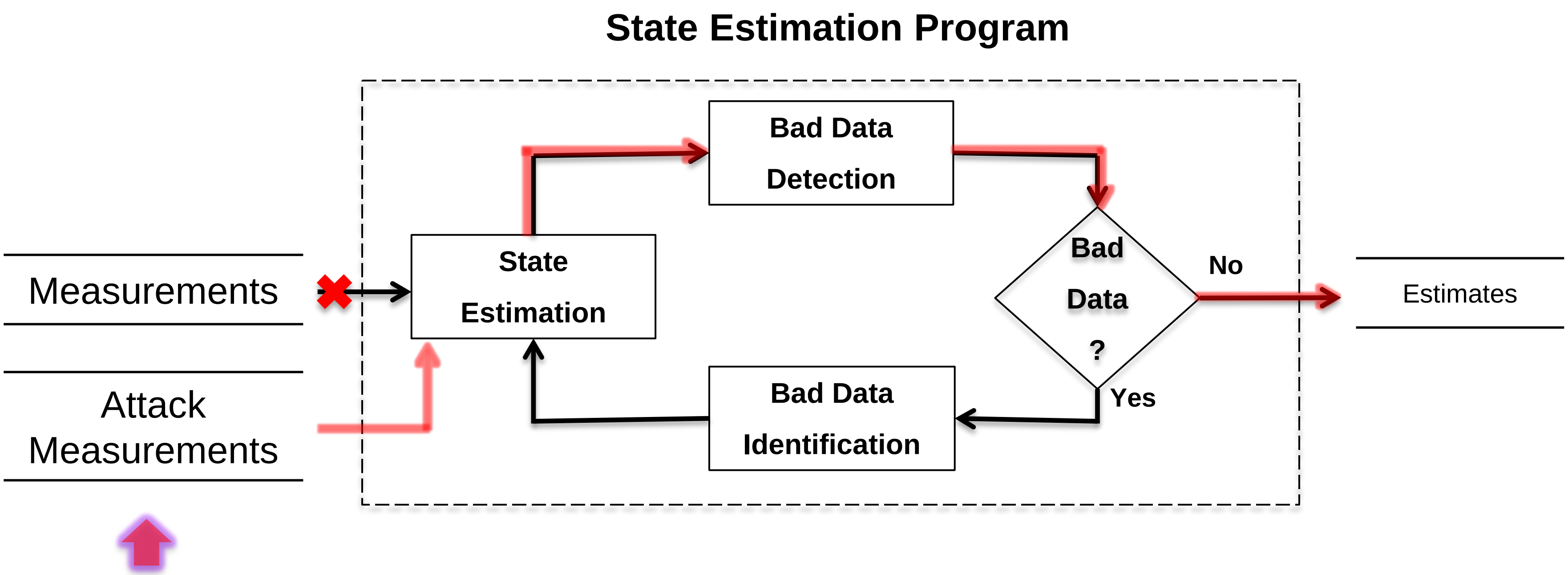
Estimates (p.u.)	Residuals (p.u.)	Weighted Residuals (p.u.)
0.453	1.080E-07	1.350E-05
-0.448	1.370E-07	1.713E-05
0.072	3.774E-07	4.718E-05
-0.081	7.335E-07	9.169E-05

Random Error:

Std Dev (p.u.)
8.000E-03
8.000E-03
8.000E-03
8.000E-03

Residuals practically insignificant compared to Std Devs.

Illustrative example: FDI



Line 17				
Type	Line Number	From Bus	To Bus	Measurements (p.u.)
Pline	17	1	17	0.453
Pline	17	17	1	-0.448
Qline	17	1	17	0.072
Qline	17	17	1	-0.081

Estimation Results:

Estimates (p.u.)	Residuals (p.u.)	Weighted Residuals (p.u.)
0.453	1.080E-07	**1.350E-05**
-0.448	1.370E-07	**1.713E-05**
0.072	3.774E-07	**4.718E-05**
-0.081	7.335E-07	**9.169E-05**

Random Error:

Weighted Residuals (p.u.)
7.801E-01
1.762E-01
5.206E-01
5.059E-01

Weighted residuals are practically insignificant compared to the Random Error case.
No bad data detected => DANGER !!!

Illustrative example: FDI

Summary of results:

- If bad data detection is tuned to data with assumed random error distribution, then
  - FDI data will likely not be detected if it is highly structured
  - Because the weighted residual of the FDI data is much less than that of the random error.
- The negative consequences of the FDI attack:
  - Data that would normally be rejected (cf. Mismatch (Std Dev)) is accepted as good.
  - Control center operator will be making decisions based on wrong perception of operating state.
- Two types of mismatches, below, illustrate this:
  1. Mismatch = Estimated_{FDI} – Ground Truth [p.u.]
  2. Mismatch = Estimated_{FDI} – Ground Truth [Std Dev]

Line 17											
Type	Line Number	From Bus	To Bus	Weighted Residual_{FDI} (p.u.)	Weighted Residual_{Random} (p.u.)	**Detection likely?**	Estimated_{FDI} (p.u.)	Ground Truth (p.u.)	Std Dev (p.u.)	Mismatch (p.u.)	**Mismatch (Std Dev)**
Pline	17	1	17	1.350E-05	7.801E-01	**No**	0.453	0.301	8.000E-03	0.152	**18.990**
Pline	17	17	1	1.713E-05	1.762E-01	**No**	-0.448	-0.299	8.000E-03	0.150	**18.690**
Qline	17	1	17	4.718E-05	5.206E-01	**No**	0.072	0.100	8.000E-03	0.028	**3.469**
Qline	17	17	1	9.169E-05	5.059E-01	**No**	-0.081	-0.120	8.000E-03	0.039	**4.840**

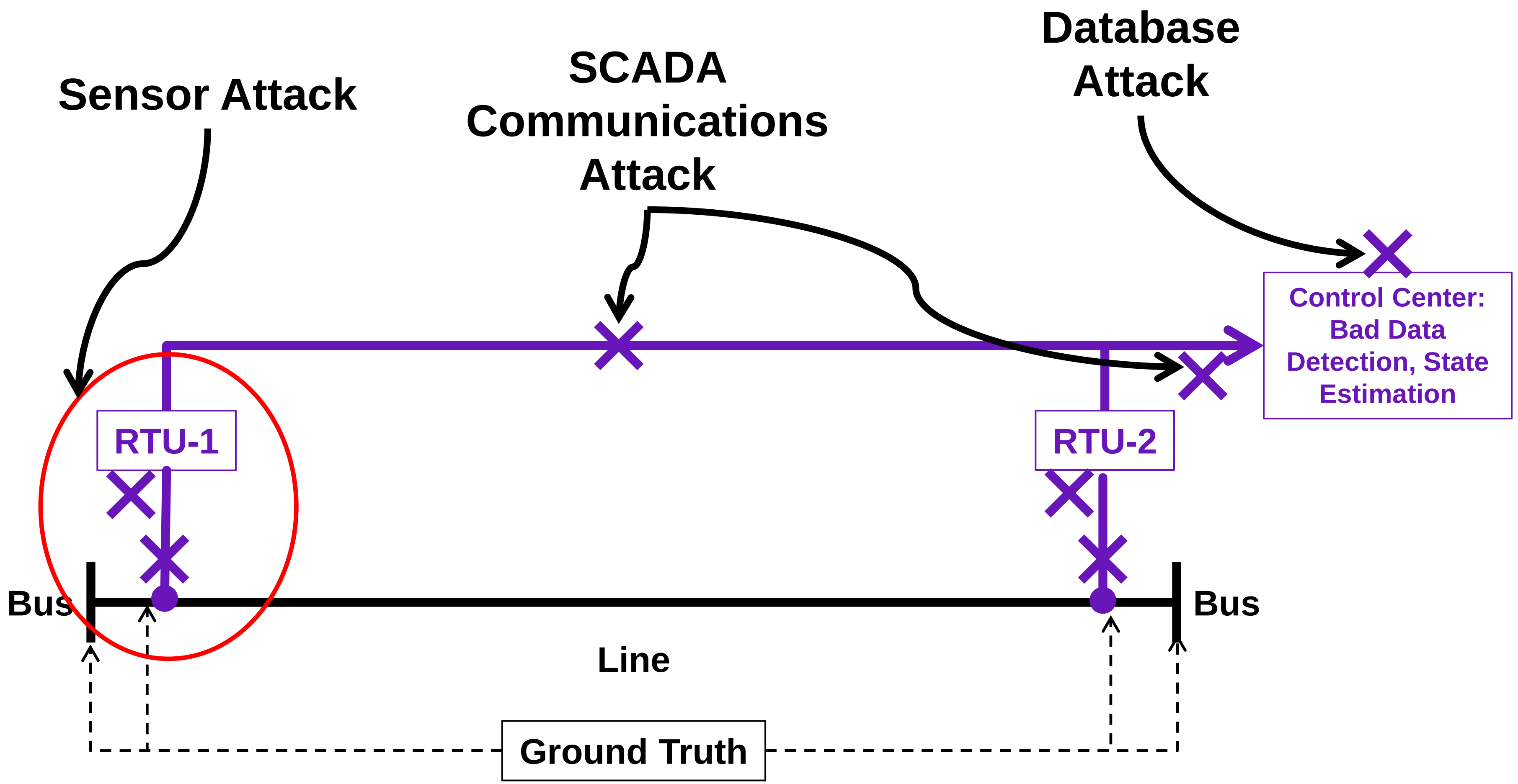
Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

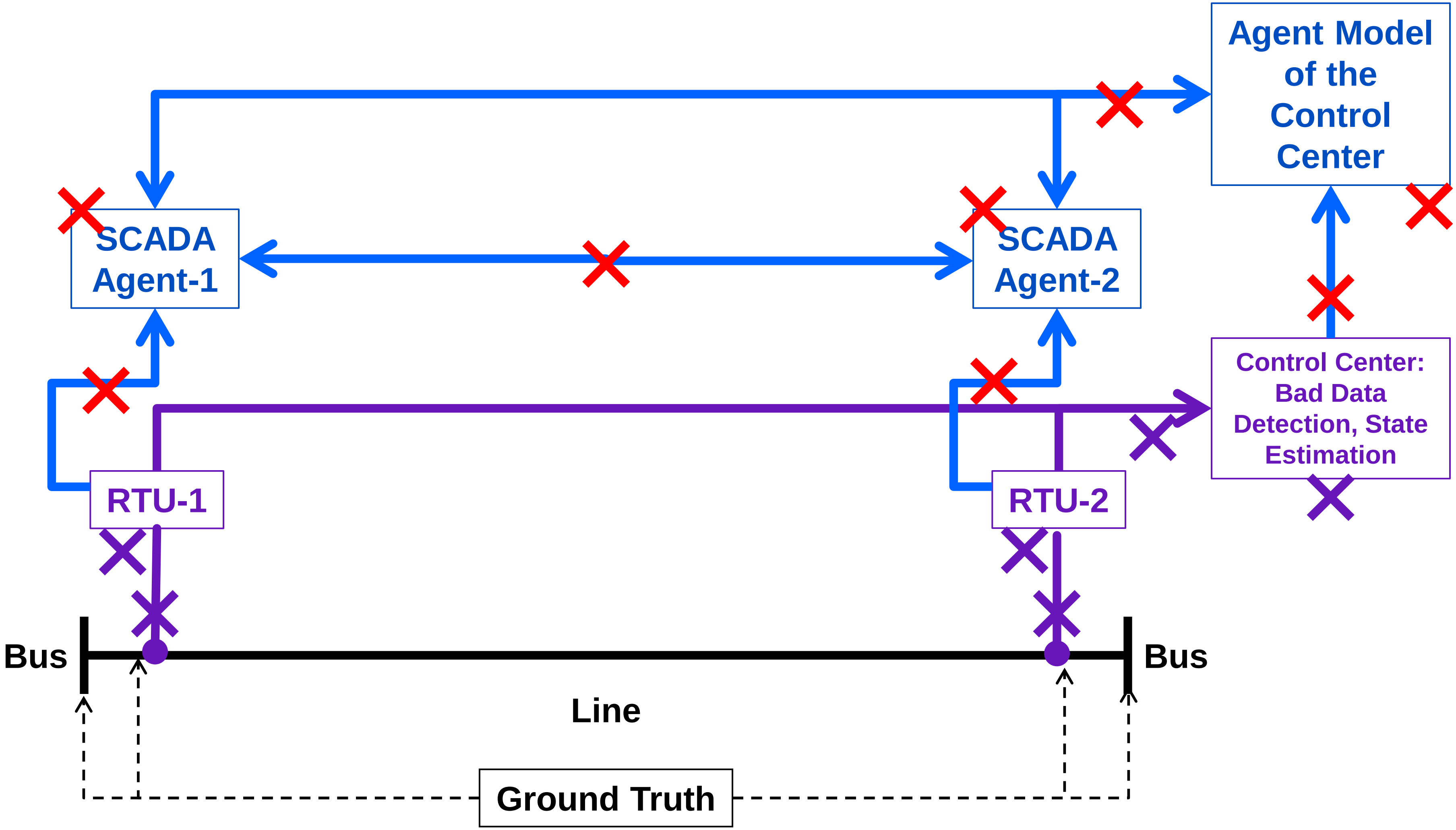
Architectual Rationale

- Do not modify centralized state estimation functions with security enhancements
  - It is an optimized process for current operations
  - Early and widespread adoption is desired
    - Interoperability with legacy systems
    - Low-interference with current operations
    - Minimize startup and implementation costs
- Overlay distributed state estimation (DSE) verification for security
  - If DSE can be conducted autonomously by software agents
  - FDI attacks on centralized state estimation can be detected by distributed agents
  - Power system is a closed system
    - There is always knowledge elsewhere that can be leveraged

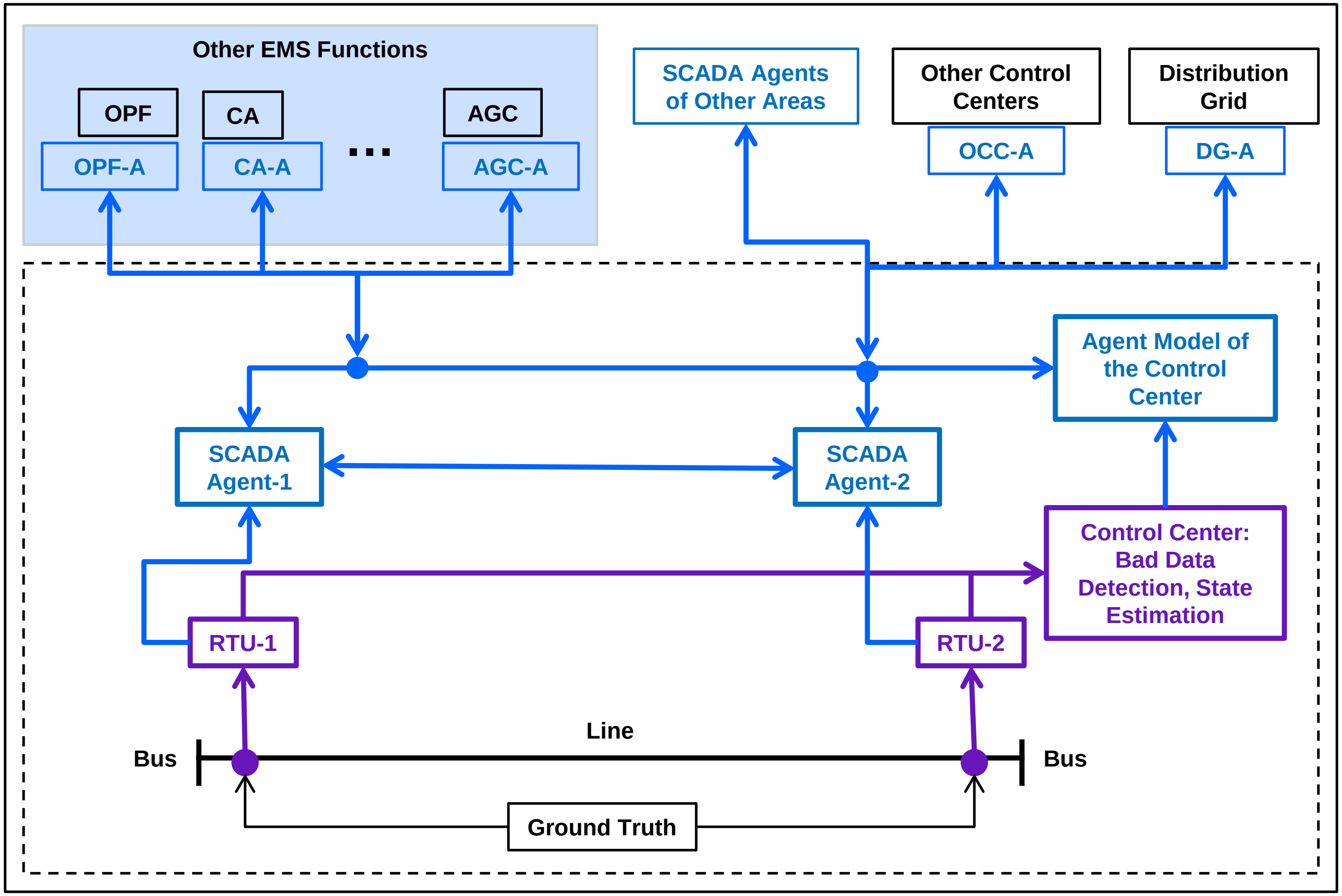
Schematic of Attacks



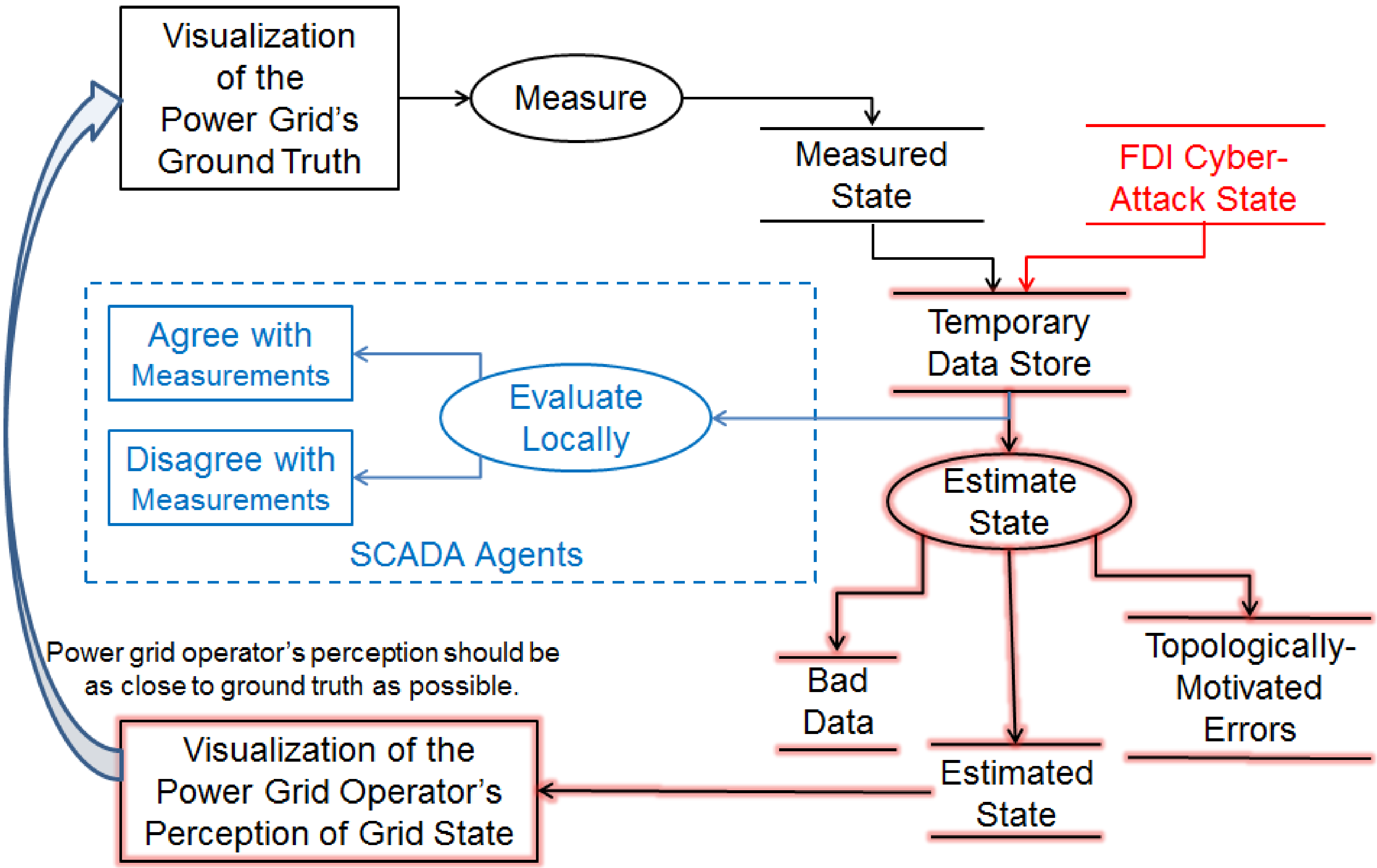
Detection Even if Agents Are Compromised



SCADA Agent Architecture



Test Bed & Data Flow



Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

References

1. G. Hug-Glanzmann and J.A. Giampapa, "Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks," in IEEE Transactions on Smart Grid, Vol. 3, No. 3, pp. 1362–1370, September 2012, DOI: 10.1109/TSG. 2012.2195338.

   http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6275516&isnumber=6275510

2. A. Tajer, S. Kar, H.V. Poor, and S. Cui, "Distributed Joint Cyber Attack Detection and State Recovery in Smart Grids," in *Proceedings of Cyber and Physical Security and Privacy* (IEEE SmartGridComm), © 2011 IEEE, pp. 202–207.

   http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06102319

3. Y. Liu, P. Ning, and M.K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, IL, November 2009.

4. National Communications System (NCS), Technical Information Bulletin 04-1, "Supervisory Control and Data Acquisition (SCADA) Systems", *NCS TIB 04-1*, October 2004, pp. 76.

   http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

Outline

- False Data Injection (FDI) Attack
- Three Types of FDI Attack
- Illustrative Example
- Autonomous Cyber-Physical Agent Architecture
- References
- Discussion

Contact Information

Joseph Andrew Giampapa

Senior Member of the Research Technical Staff

Research, Technology, and Systems Solutions (RTSS) Program

Telephone: +1 412-268-6379

Email: garof@sei.cmu.edu

Web

www.sei.cmu.edu

www.sei.cmu.edu/staff/garof

U.S. Mail

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA