ASU Arizona State University

Reliability Enhancements for Real-Time Operations of Electric Power Systems

Xingpeng Li

Nov. 1st, 2017

Committee Members:
Dr. Kory Hedman (chair)
Dr. Gerald Heydt
Dr. Vijay Vittal
Dr. Jiangchao Qin

Agenda

- Introduction
- Real-time contingency analysis with corrective transmission switching (Part-I)
- Real-time security-constrained economic dispatch with corrective transmission switching (Part-II)
- False data injection cyber-attack detection (Part-III)
- Conclusions
- Future work

Introduction

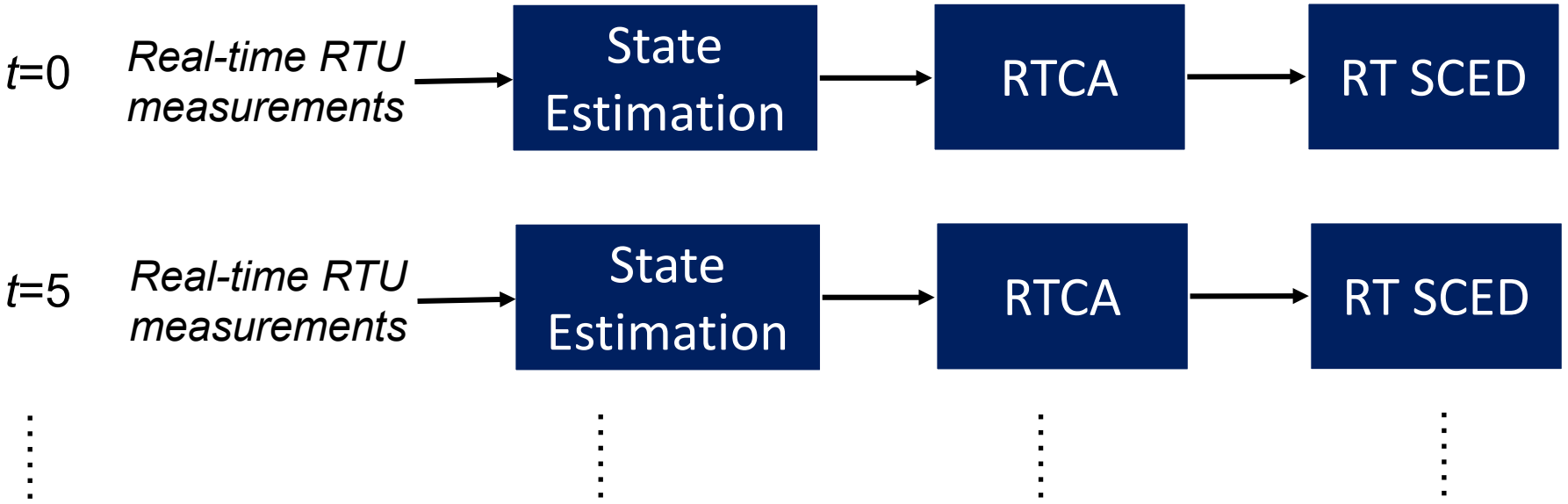
Introduction

Energy management system (EMS)

- Computer-aided tool
  - Help operators monitor and control the system
- Key functions
  - System monitoring (**state estimation**)
  - Real-time contingency analysis (**RTCA**)
  - Real-time security-constrained economic dispatch (**RT SCED**)

Introduction

Current industry practices of power system **real-time** operations



This process repeats continuously in real time.

RTU denotes Remote Terminal Unit.

Introduction

Flexibility in transmission networks

- **Not modeled** in **existing** RTCA and RT SCED applications.
- Transmission network is **traditionally** treated as a **static** network in real-time operations.
- Operators can **reconfigure** the network in real-time.
- Transmission switching
  - Enables RTCA and RT SCED to take advantage of the flexibility in transmission networks.

Introduction

Corrective transmission switching (**CTS**)

- disconnects a line out of service, shortly after a contingency, as a **corrective** action.
- Implement **at most 1** corrective switching action.
- Identifying multiple CTS solutions per contingency can provide operators with **choices.**
- Applications
  - Part-I: RTCA with CTS
  - Part-II: RT SCED with CTS

Introduction

False data injection (**FDI**) and its detection

- State estimation
  - a very important EMS function - determines system status.
  - provides a base case for other EMS functions (e.g., RTCA and RT SCED).
  - is subject to FDI cyber-attacks.
- FDI detection (**FDID**)
  - key to efficiently identifying FDI attacks
  - enhance reliability of state estimation

Part-III: Enhancing state estimation with FDID

Real-Time Contingency Analysis with Corrective Transmission Switching

(Part-I: RTCA with CTS)

RTCA: Overview

Real-time contingency analysis

- A “what if” scenario simulator.
- *N*-1 check.
- Handle potential post-contingency violations
  - **Corrective transmission switching.**

Transmission Switching: Overview

- Algorithms to generate candidate switching list:
  - Heuristic algorithms
    - Regular data mining (**RDM**).
    - Enhanced data mining (**EDM**).
    - Closest branches to contingency element (**CBCE**).
    - Closest branches to violation element (**CBVE**).
  - Complete enumeration (**CE**)
    - Guarantee optimal solution
    - Long computational time - **impractical**.
    - Justify the effectiveness of the proposed heuristics.

RTCA with CTS

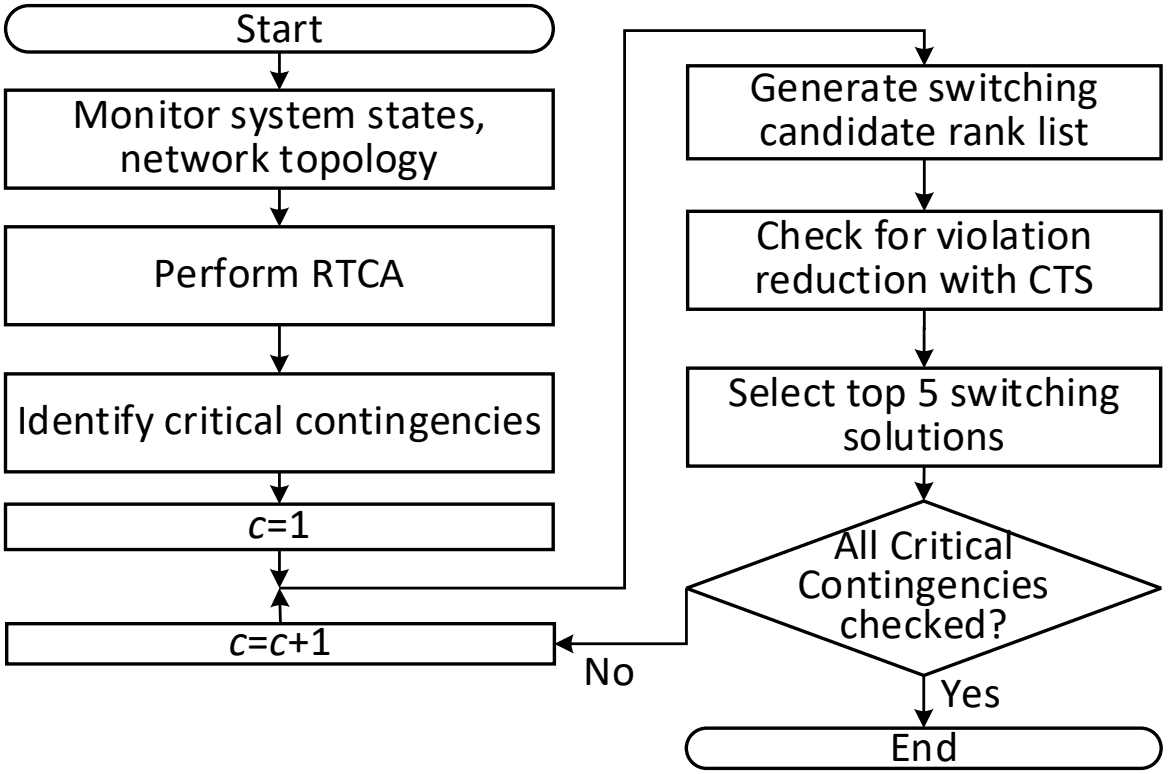


Fig. 1. Procedure of RTCA with CTS

Metric for CTS

Metric 1: *Average of violation reduction in percent*

- is used to investigate how much violation reduction can be achieved with CTS.

at an ***aggregate*** level

$$P_{TS} = \frac{1}{N_c} \sum_{c=1}^{N_c} (f_{c0} - f_{c1}) / f_{c0} \times 100\%$$

where,

f_{c0} denotes the total amount of violations under contingency c without CTS;

f_{c1} denotes the total amount of violations under contingency c with CTS;

N_c is the total number of critical contingencies simulated.

Metric for CTS

Metric 2: *Pareto Improvement*

- Reduction of total violations.
- No additional individual violation:
  - Not result in any new violation.
  - Not worsen any existing contingency violation

at an ***individual/elemental*** level

Results

Case studies

Summary of three practical systems

System	# of hours	Pload (MW)	Qload (MVAr)	# of Buses	# of Gens	# of Branches
TVA	72	~24,000	~4,000	~1,800	~350	~2,300
ERCOT	3	~56,900	~7,600	~6,400	~700	~7,800
PJM	167	~139,000	~22,400	~15,500	~2,800	~20,500

- The ERCOT cases and the PJM cases are actual system operation data.
- For the TVA system, we had to create the cases based on the data they provided.

Case studies

Cumulative results of RTCA on three practical systems

System	# of hours	# of contingencies simulated	# of critical contingencies
TVA	72	126,449	4,272
ERCOT	3	13,044	40
PJM	167	1,437,749	8,064
"*Sum*"	242	1,577,242	12,376

> 1.5 *million* contingencies were simulated

< 1% of the total contingencies simulated

Case studies

Cumulative results of CTS on three practical systems

System	# of critical contingencies	# of contingencies with violation fully removed by CTS	# of contingencies with violation reduced by CTS	# of contingencies with no violation reduced by CTS
TVA	4,272	427	3,535	310
ERCOT	40	6	27	7
PJM	8,064	2,684	4,554	826
"*Sum*"	12,376 **(100%)**	3,117 **(25.2%)**	8,116 **(65.6%)**	1,143 **(9.2%)**

The number of contingencies for which the associated violation can be fully eliminated by CTS: **> 25%.**

Case studies

Cumulative results of CTS on three practical systems

System	# of critical contingencies	# of contingencies with violation fully removed by CTS	# of contingencies with violation reduced by CTS	# of contingencies with no violation reduced by CTS
TVA	4,272	427	3,535	310
ERCOT	40	6	27	7
PJM	8,064	2,684	4,554	826
"*Sum*"	12,376 **(100%)**	3,117 **(25.2%)**	8,116 **(65.6%)**	1,143 **(9.2%)**

The number of contingencies where there is **NO beneficial** CTS solution: **< 10%**.

TVA

Results of CTS on the TVA system

Methods	Solution time (s)					Average violation reduction	
	max	min	median	average	std	Flow	Voltage
RDM	225.9	11.0	103.6	**108.3**	79.5	**39.77%**	**51.07%**
EDM	18.0	1.4	9.1	**9.6**	6.5	**38.73%**	**50.22%**
CE	9636.5	208.5	2003.5	**2458.2**	2316.9	***39.77%***	***51.22%***

Both RDM and EDM use 5% as the tolerance for defining whether a switching action is beneficial.

Note that the candidate CTS list for each contingency is the same for RDM while it is customized for EDM.

The proposed data mining methods (RDM and EDM) can achieve **very similar results** with complete enumeration. However, they are **much faster**.

ERCOT

Results from various CTS methods on the ERCOT system

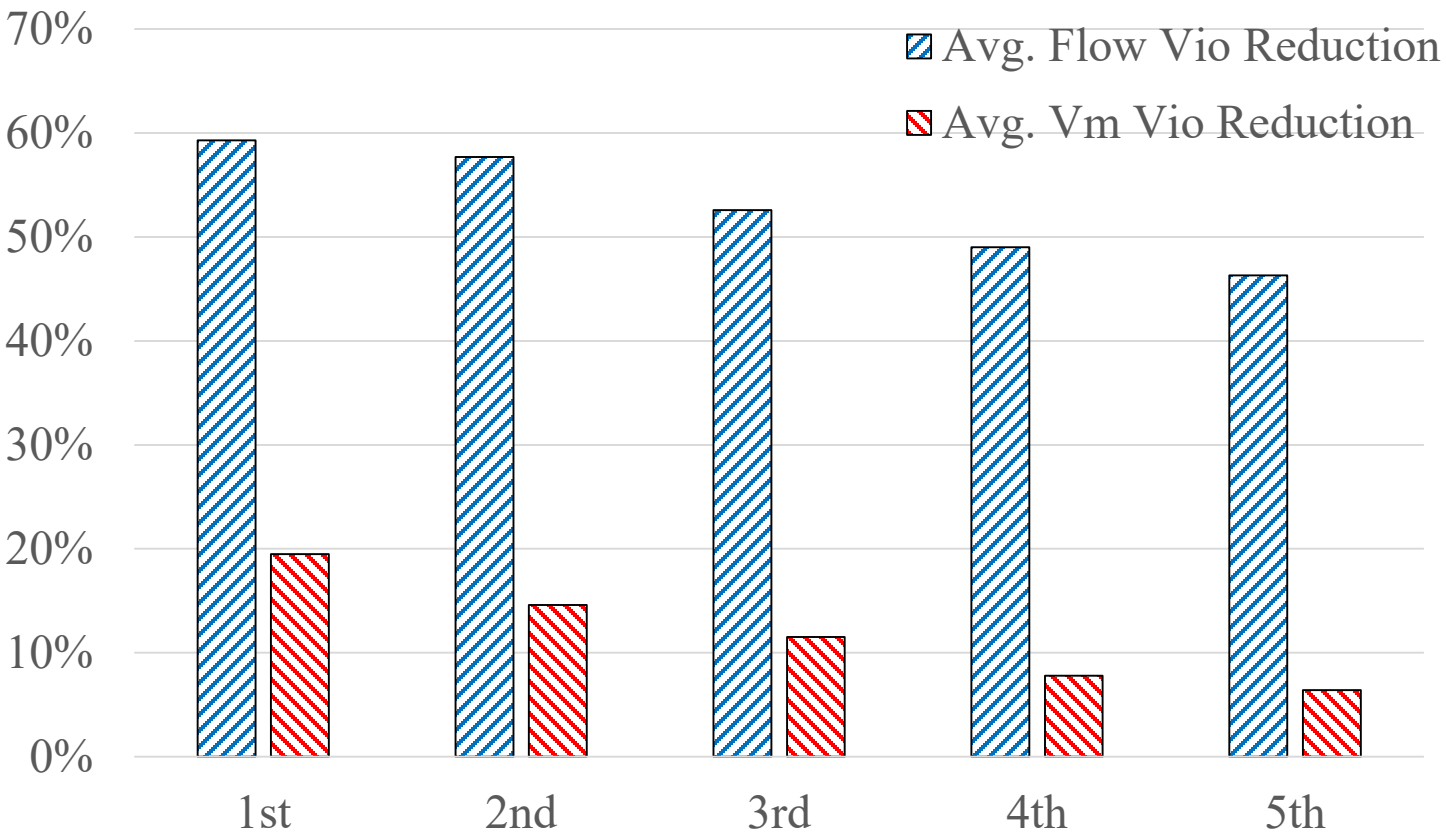
CTS methods	Solution time (s)	Avg. flow Vio Reduction		Avg. Vm Vio Reduction	
		w/o Pareto Improvement	w/ Pareto Improvement	w/o Pareto Improvement	w/ Pareto Improvement
Closest branch to the *contingency* (CBCE)	245	40.8%	37.7%	12.1%	12.1%
Closest branch to the *violations* (CBVE)	244	53.1%	49.3%	12.3%	12.3%
Complete *enumeration* (CE)	11,505	53.3%	49.3%	14.3%	14.3%

11505/244 = 47

Heuristic methods can achieve almost the same results with complete enumeration, but 47x faster !!!

Note: solution time (in seconds) does not include the time for simulating RTCA;
it is the solution time on average overall 3 scenarios/cases.

PJM

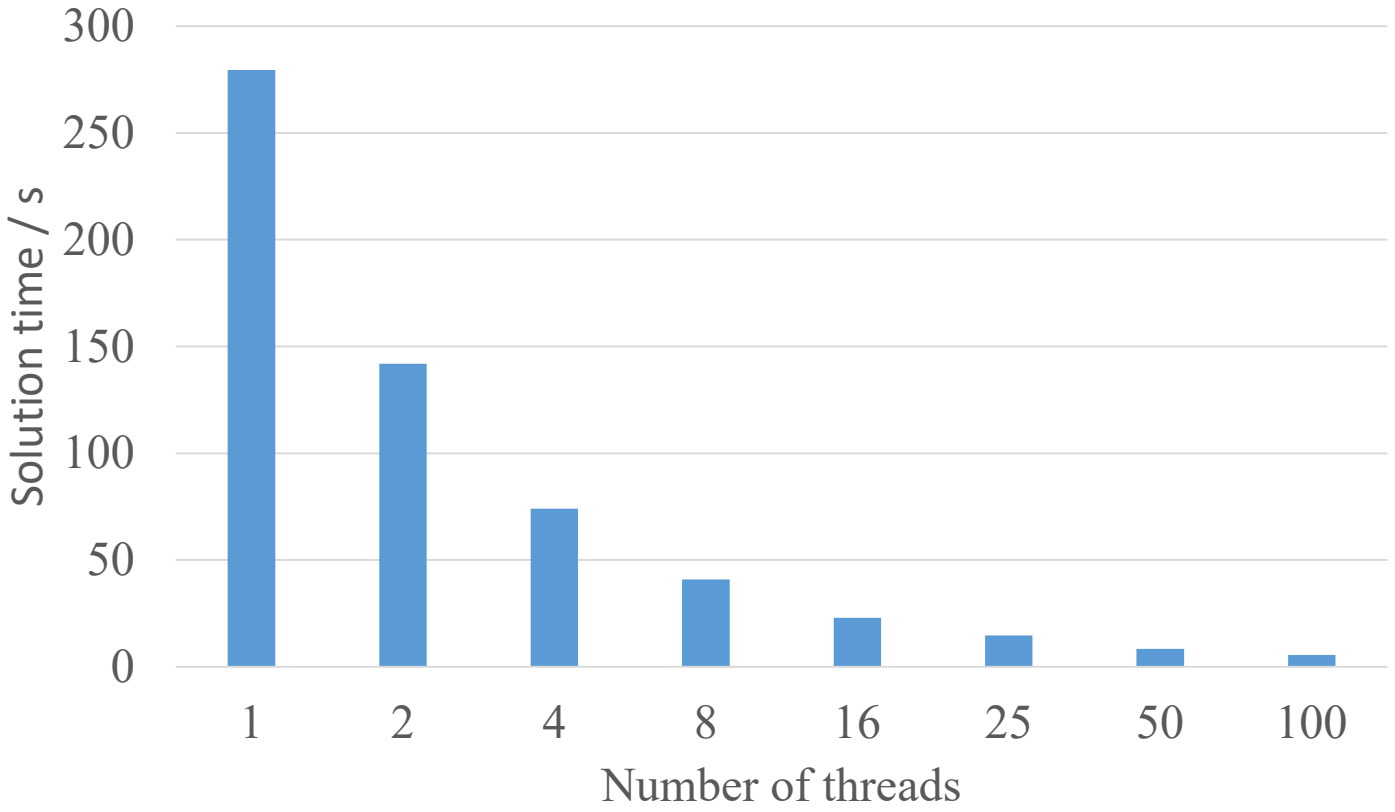


Average violation reduction with the 5 best switching actions on the PJM system

CTS method is 100 closest branches to the violation element (CBVE).

Parallel Computing

Average CTS solution time per scenario with different threads on the ERCOT system



Platform for these results is the “cab”, one of the clusters at Lawrence Livermore National Laboratory (LLNL).

Conclusions (RTCA with CTS)

- Heuristic algorithms are proposed to provide **fast** CTS solutions for reducing post-contingency violation.
- The heuristic methods can achieve very similar results of complete enumeration with **much less solution time**.
- A switching action that reduces violation for a contingency in one scenario can also provide benefits for the same contingency under a **different scenario.**
- Parallel computing can **further reduce** the solution time.
- Demonstrated significant benefits (violation reduction) with CTS for three large-scale models (data provided by **TVA**, **ERCOT**, and **PJM**).

Real-Time Security-Constrained Economic Dispatch with Corrective Transmission Switching

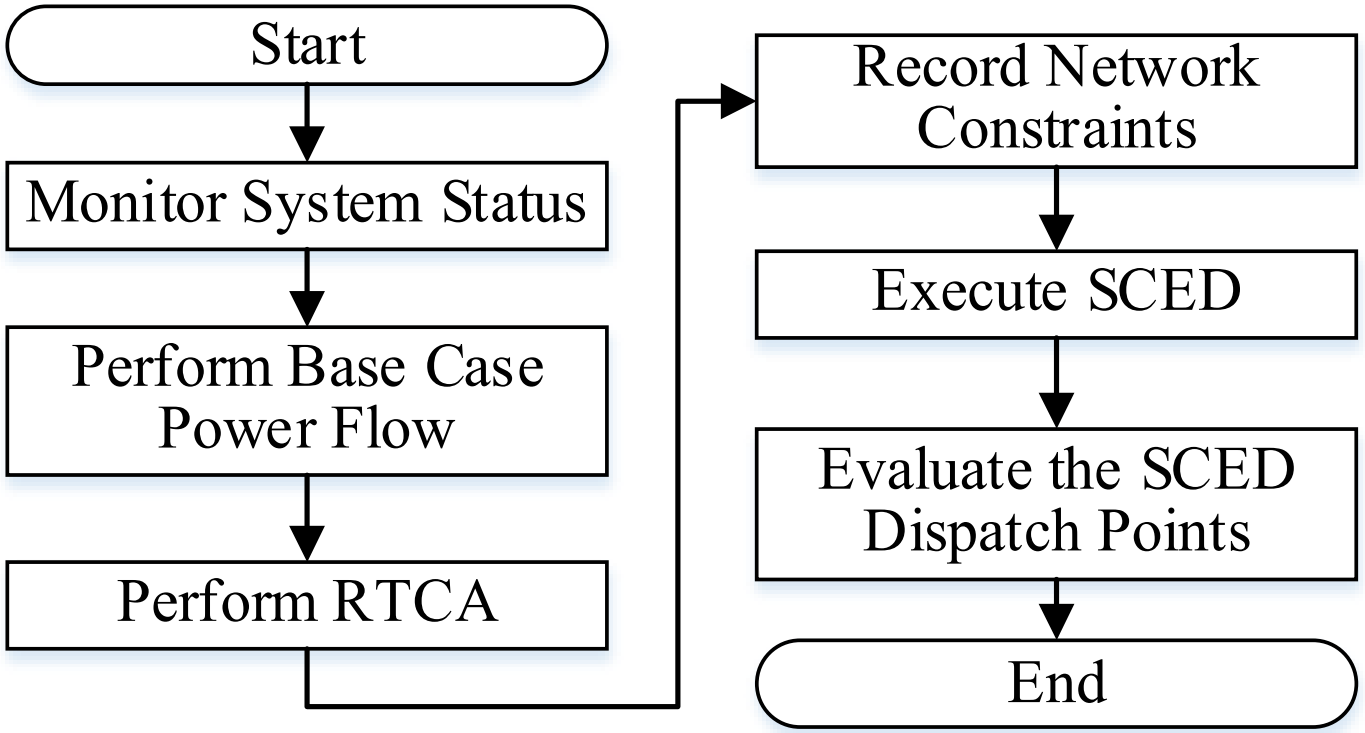
(Part-II: RT SCED with CTS)

RT SCED: overview

RT SCED:

- DC model based **optimization** process.
- aims to provide the **least cost** generation.
- meet all the operation and reliability constraints.
- runs **repeatedly** with **updated** inputs.
  - e.g., every 5 minutes for PJM

Energy management system (EMS)



Existing procedure of EMS (**Procedure-A**)

Model

Model inconsistency:

- RTCA uses full AC power flow model.
- RT SCED uses simplified DC power flow model.

Model conversion (connect RTCA and RT SCED):

- What RT SCED needs from RTCA?
  - Base-case network constraints
  - Contingency-case network constraints
- Assuming reactive power does not change in a short timeframe.

SCED with CTS

Benefits of CTS in RTCA

- CTS can reduce post-contingency violations.
- CTS can relieve network congestion under contingency.

Benefits of CTS in RT SCED?

- Considering the flexibility in transmission network would increase the feasible set of SCED, which may reduce the total cost.

How to model CTS in RT SCED?

- Directly model CTS in RT SCED by using binary variables to indicate the status of switching element.
  - Convert RT SCED from a **simple** linear programming (**LP**) problem into a **complex** mixed-integer LP (**MILP**) problem.

SCED with CTS

How to model CTS in SCED?

- Directly model CTS in SCED by using binary variables that indicate the status of switching element.
  - Convert SCED from a simple linear programming (LP) problem into a complex mixed-integer linear programming (MILP) problem. - ***Impractical***
- Heuristic method…
  - Remember how to determine the limit (MW) for contingency-case network constraints?

Actual limit (MW): $LimitC_{kc} = \sqrt{RateC^2 - \{\max(|Q_{kc,from}|, |Q_{kc,to}|)\}^2}$

where $Q_{kc,from}$ and $Q_{kc,to}$ denote the reactive power on line k flowing out of from-bus and to-bus under contingency c respectively; ***RateC*** denotes short-term thermal limit in **MVA**.

SCED with CTS

How to model CTS in SCED?

Actual limit: $LimitC_{kc} = \sqrt{RateC^2 - \{\max(|Q_{kc,from}|, |Q_{kc,to}|)\}^2}$

As concluded in Part-I:

- CTS can provide benefits even when system condition varies.
- CTS can reduce flows on overloaded lines under contingency.

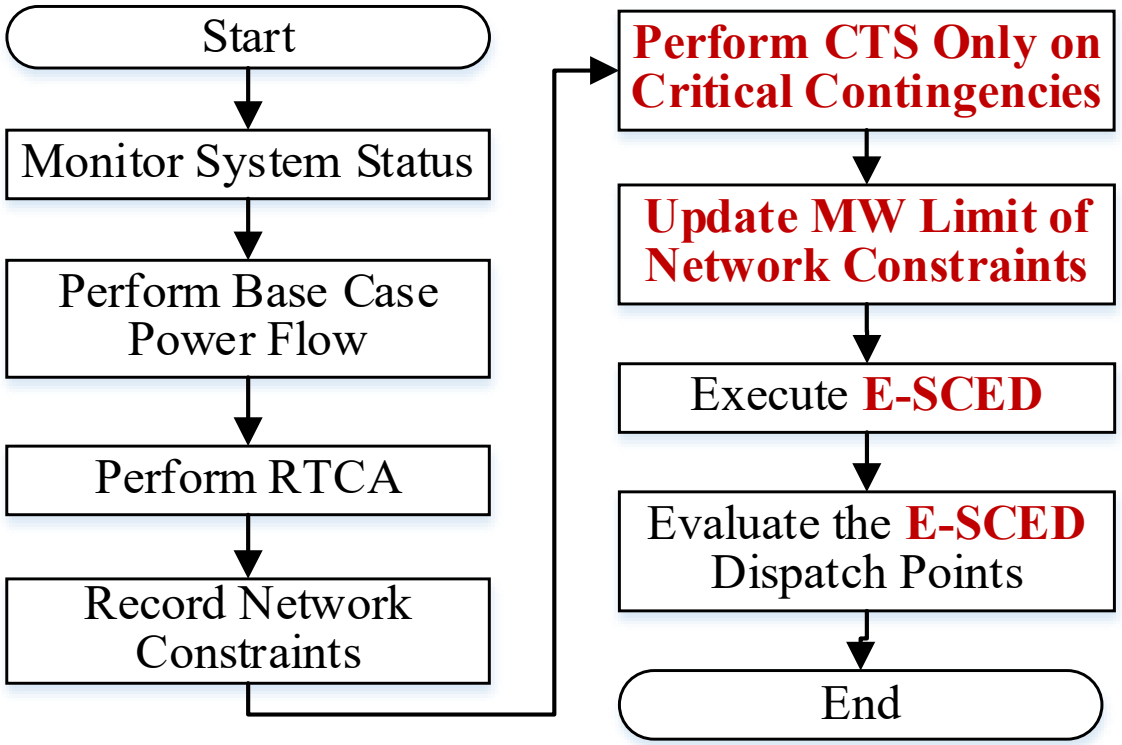
Thus, extra power beyond the limit may be allowed on those lines under the same contingency when simulating SCED.

Pseudo limit:

$$LimitC_{kc} = \sqrt{\{RateC + (f_{kc} - f_{kc,CTS})\}^2 - \{\max(|Q_{kc,from}|, |Q_{kc,to}|)\}^2}$$

f_{kc} denotes the flow violations in the post-contingency situation;
$f_{kc,CTS}$ denote the flow violations in the post-switching situation.

Energy management system (EMS)



The proposed procedure of EMS (**Procedure-B**)

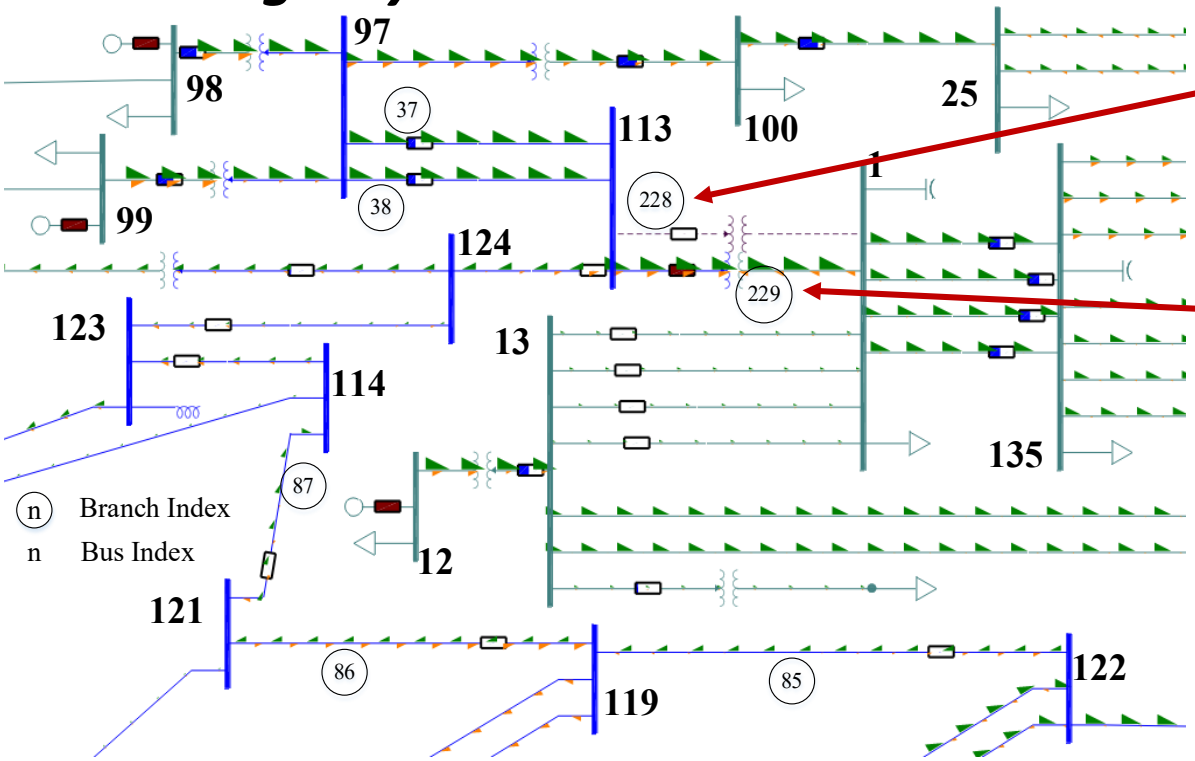
Results

Case studies

- The Cascadia system
  - Created by Dr. Robin Podmore (IncSys Academy) and is used in their operators training business.
  - # of buses: 179.
  - # of branches: 245.
  - # of online generators: 40.
  - In-service load: 7.4 GW.

Procedure-A

post-contingency situation



Contingency (branch 228)

Violation (branch 229)

Branches 228 and 229 are two **parallel** branches.

RTCA identifies two violations on the Cascadia system:

1) Overloads (245 MVA) on branch 229 under **contingency 228**.
2) Overloads (245 MVA) on branch 228 under **contingency 229**.

Sent to RT SCED

Procedure-A

- The two network constraints are sent to RT SCED.
- Then, RT SCED executes
  - to obtain the least-cost solution that eliminates those two post-contingency violations.
- SCED: simplified DC model -> evaluate the SCED solution with full AC model by re-running RTCA with new *Pg*.
  - the contingency list is the **same** with the pre-SCED stage.
  - still, the same 2 post-contingency violations.
  - but, the overload is reduced by over 99%, from 2*245 MVA (pre-SCED) to 2*2.3 MVA (post-SCED).

The proposed Procedure-A can successfully connect AC based RTCA and DC based RT SCED, and it can effectively reduce system violations.

Procedure-B

CTS results under contingency 228 on the Cascadia system

CTS Ranking	CTS Branch	Pareto Improvement Flag	Violation Reduction (MVA)	Violation Reduction in Percent
1st Best	37	Yes	81.2	33.1%
2nd Best	38	Yes	81.2	33.1%
3rd Best	85	Yes	70.2	28.7%
4th Best	87	Yes	49.2	20.1%
5th Best	86	Yes	48.8	19.9%

Monitor branch: 229

Actual-Limit: 1281.7 MW

Pseudo-Limit with 3rd best CTS: 1352.5 MW

Contingency 228 results in a flow overload of 245 MVA on branch 229 in the pre-SCED situation.

Procedure-B

Results of three SCED models on the Cascadia system

SCED models	Total Cost ($/h)	Congestion Cost ($/h)	Congestion Cost Reduction (%)	Solution time (s)
No network constraint	49771	0	NA	0.02
without CTS	50203	**431.5**	NA	0.19
with the 3rd best CTS	49814	**42.6**	**90.1%**	0.21

With consideration of CTS in E-SCED, the congestion cost is reduced by 90%.

The solution time for a traditional SCED and E-SCED is very similar.

Given the size of real power systems, even 10% congestion cost reduction can be huge.

- e.g., the congestion cost of the PJM system is over *600 million dollars* in 2013.

Procedure-B

Results of RTCA with CTS in the **post E-SCED** stage

CTS	Branch Emergency limit (MVA)	flow in the post-contingency (MVA)	Flow in the post-switching situation (MVA)	Flow change caused by CTS (MVA)	Violation reduction in percent
1st Best	1292.5	1371.2 (violation: 1371.2-1292.5=78.6)	1291.6	-79.6	100%
2nd Best			1291.6	-79.6	100%
3rd Best			1222.6	-148.6	100%
4th Best			1273.6	-97.6	100%
5th Best			1278.8	-92.4	100%

Contingency element: branch 228.
Monitor element: branch 229.
Post-contingency violation: 78.6 MVA.

In the post E-SCED stage, RTCA is performed on all contingency cases and identifies only two critical contingencies (228 and 229) or only two post-contingency violations.

Conclusions (SCED with CTS)

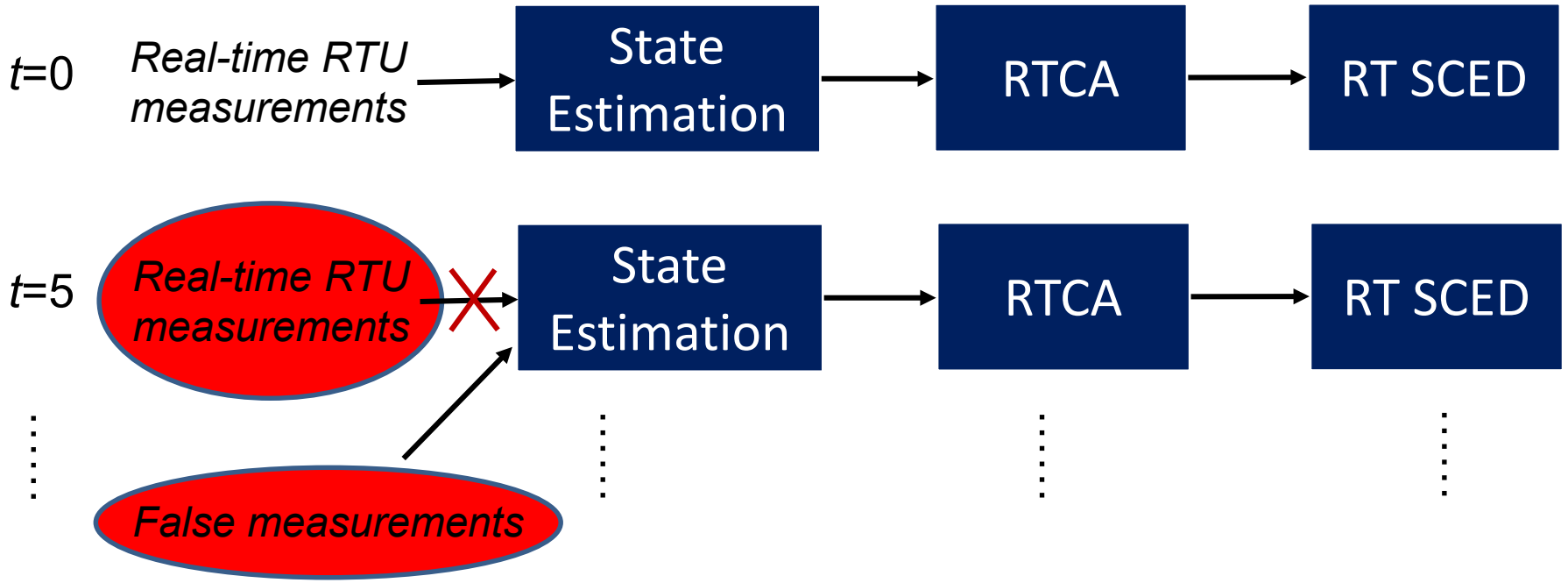
- The proposed Procedure-A can successfully connect AC based RTCA and DC based RT SCED, which is consistent with industrial practice.
- With the proposed Procedure-B, RT SCED can fully utilize the violation reduction benefits provided by CTS in a **practical** way.
- The E-SCED of Procedure-B can significantly reduce congestion cost.
- The CTS solutions identified in the pre-SCED stage can reduce violation in the post-SCED stage.
- Built on existing SCED tools, the **only** change required to implement the proposed Procedure-B is to **replace** the **actual limit** with the proposed **pseudo limit** for contingency-case network constraints.

False Data Injection Cyber-attack Detection

(Part-III: Enhancing state estimation with FDID)

Introduction

Current industry practices of power system **real-time** operations



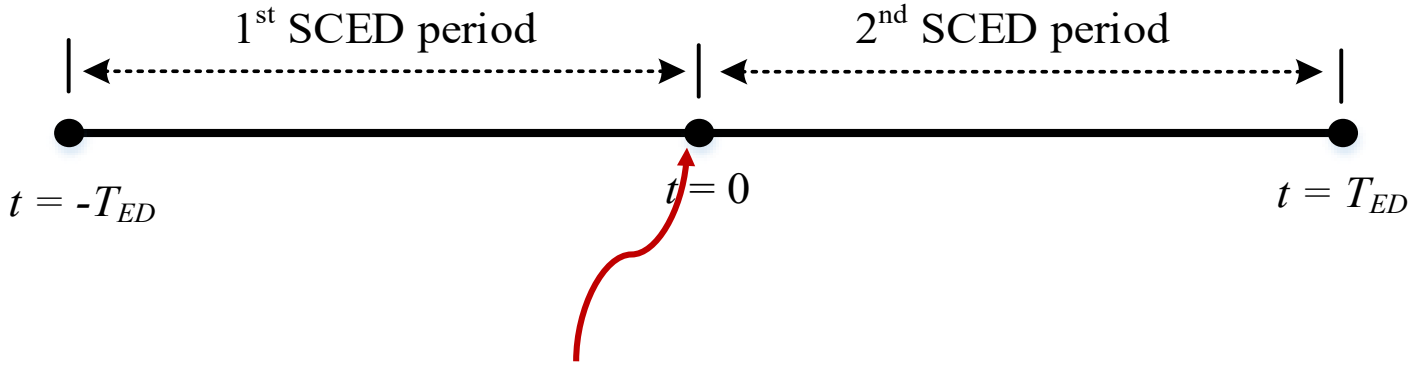
This process repeats continuously in real time.

FDI Cyber-attack

- Prior work in literature shows that FDI cyber-attacks can cause unobservable network violations.
- Developing an efficient approach to detect FDI cyber-attacks is vital for improving system reliability.
  - A modified version of an existing heuristic algorithm in literature is implemented for testing the proposed **two-stage FDID** approach.

Case studies

- Assumptions
  - The system operators have accurate information $t=-T_{ED}$.
  - The attacker launches an FDI attack at $t=0^-$.



The attack is launched at $t=0^-$, right before the start of the 2nd SCED interval.

FDID Metrics

- Metric 1: Branch overload risk index (BORI)
- Metric 2: Malicious load deviation index (MLDI)

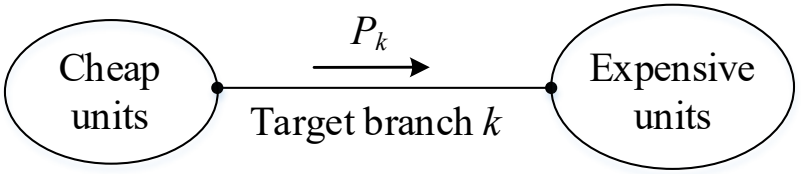
- An FDI alert system
  - *Danger*
  - *Warning*
  - *Monitor*
  - *Normal*

FDID Metric: *BORI*

Metric 1: Branch overload risk index

How does the attacker launch an FDI attack on a congested branch *k*?

Example



- In the **cyber-world**, the **attacker** can deliberately **reduce the flow** on branch *k*
  - **mislead operators** to believe there is **extra available capacity** on branch *k*
- Operators may take advantage of the extra available capacity on branch *k*
  - which increases the flow on branch *k*
- Flow violations then may occur
  - since there is **NO** "extra available capacity" in **reality**.

BORI monitors suspicious changes in branch flows.

$$BORI_k = (flow\_drop_k + original\_flow_k) / Limit_k$$

Alert level	$BORI_k$
Danger	>115%
Warning	>110%
Monitor	>105%
Normal	<105%

FDID Metric: *MLDI*

Metric 2: Malicious load deviation index

$$MLDI_k = \frac{\sum_{d \in D(k)} Indicator_{d,k}}{\sum_{d \in D(k)} 1}$$

where,

$$Indicator_{d,k} = \begin{cases} 1, & \text{if load change contributes to flow drop on branch } k \\ 0, & \text{if load change is trivial} \\ -1, & \text{if load change contributes to flow increase on branch } k \end{cases}$$

$D(k)$ denotes the set of loads that are critical to branch k.

MLDI can recognize load change patterns and identify malicious load deviation.

Alert level	$MLDI_k$
Danger	>50%
Warning	>35%
Monitor	>20%
Normal	<20%

Two-stage FDID Approach

Stage 1: FDI Attack Awareness

Stage 2: Target Branch Identification

Two-stage FDID Approach

Stage 1: FDI Attack Awareness

System-wide MLDI (SMLDI): $$SMLDI = \frac{\sum_{k \in KA} MLDI_k}{\sum_{k \in KA} 1}$$

where, KA is a set of ten branches that have the top ten $MLDI_k$ values.

Note that $MLDI_k$ is a metric for a specific line.

Alert level	*SMLDI*
Danger	>50%
Warning	>35%
Monitor	>20%
Normal	<20%

A system would be considered to be FDI **cyber-attack free** if the associated alert level is marked as ***Normal*** or ***Monitor***.

Only the cases that have either ***Warning*** **or** ***Danger*** alert flags will be **sent to stage 2** for FDI target branch identification.

Two-stage FDID Approach

Stage 2: Target Branch Identification

- A comprehensive FDI attack alert system
- A comprehensive FDI attack index

Comprehensive alert level

Alert level (*EMLDI*)	Alert level (*BORI*)			
	Normal	Monitor	Warning	Danger
Normal	*Normal*	*Monitor*	*Monitor*	*Warning*
Monitor	*Monitor*	*Monitor*	*Warning*	*Warning*
Warning	*Monitor*	*Warning*	*Warning*	***Danger***
Danger	*Warning*	*Warning*	***Danger***	***Danger***

Comprehensive FDI attack index (*CI*)

$$CI_k = EMLDI_k * BORI_k$$

Note that EMLDI is an enhanced MLDI by considering PTDF value and load magnitude.

Suspicious target branches include

- branches that are identified as "***Danger***", or
- branches that have a ***CI* ranking** in the ***top three***.

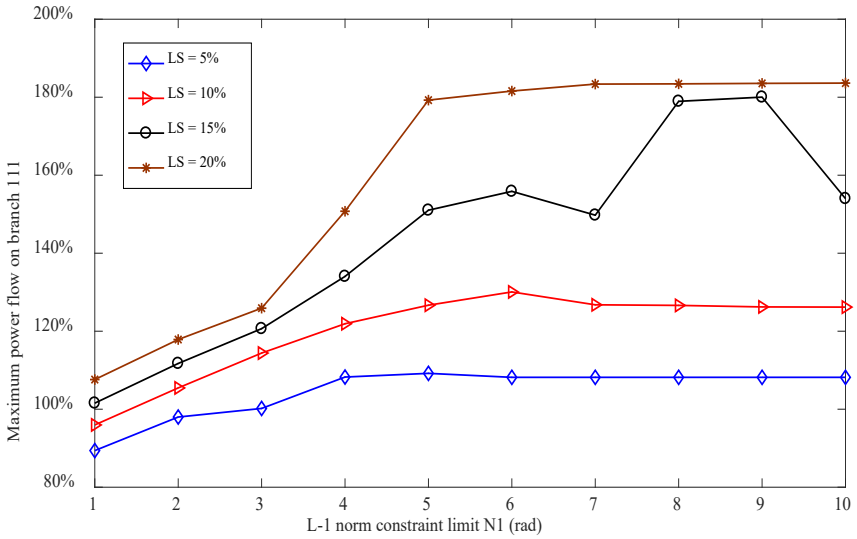
Results

Case studies

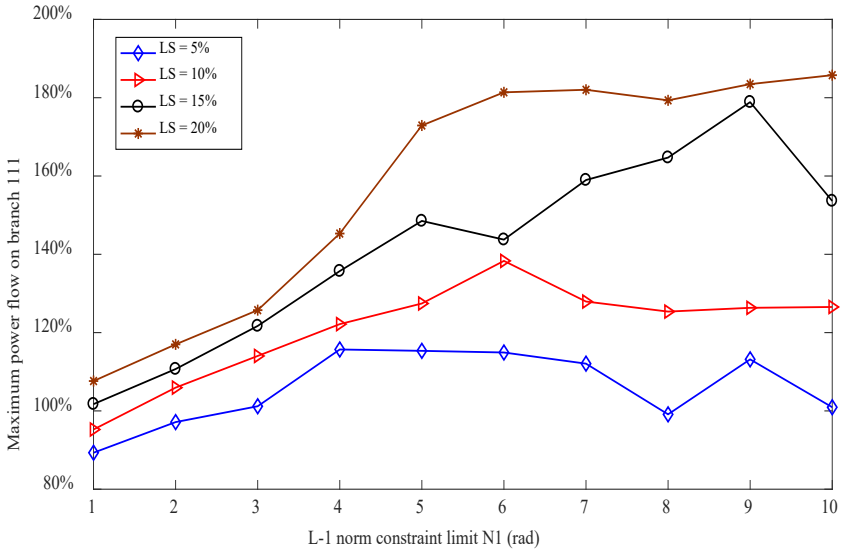
- Test case: IEEE 118-bus system
  - 118 bus
  - 186 branches
  - 19 online units
  - Total in-service load: 4.2 GW.

FDI results

FDI attack results with various load shift factors and l_1-norm constraint limits



Maximum flow on line 111 with constant load



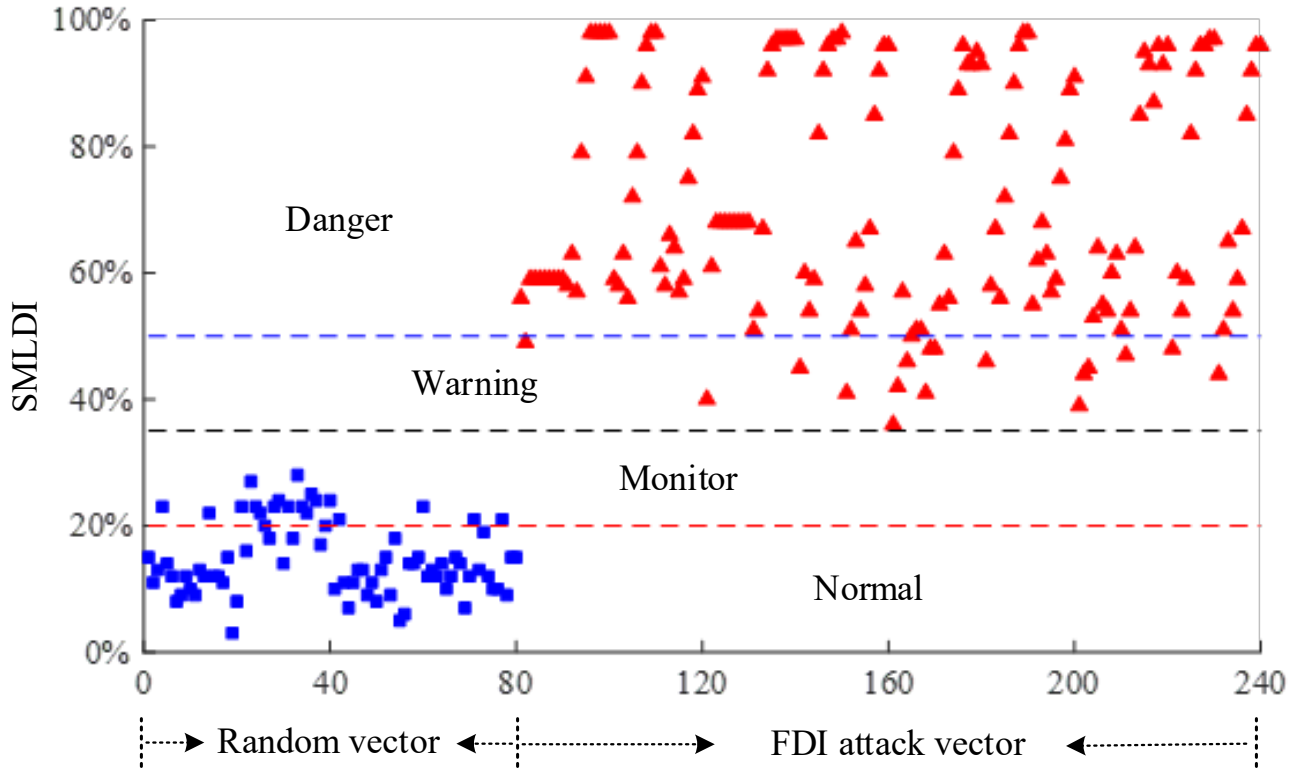
Maximum flow on line 111 with random load fluctuation

LS denotes load shift factor.

L_1-norm constraint ensures the summation of absolute angle change over all buses is limited by the parameter N_1.

FDID results

Stage 1: FDI Attack Awareness



SMLDI values for random load fluctuation vectors and FDI malicious load deviation vectors

FDID results

Stage 2: Target Branch Identification

Statistical results of target line identification

Number of scenarios simulated	**160**
Average CI_k rank of the target line	**1.4**
Percent of scenarios for which the target line is marked as Danger	**82%**
Percent of scenarios for which the target line is identified	**97%**

CI_k denotes the comprehensive FDI attack index for branch k.

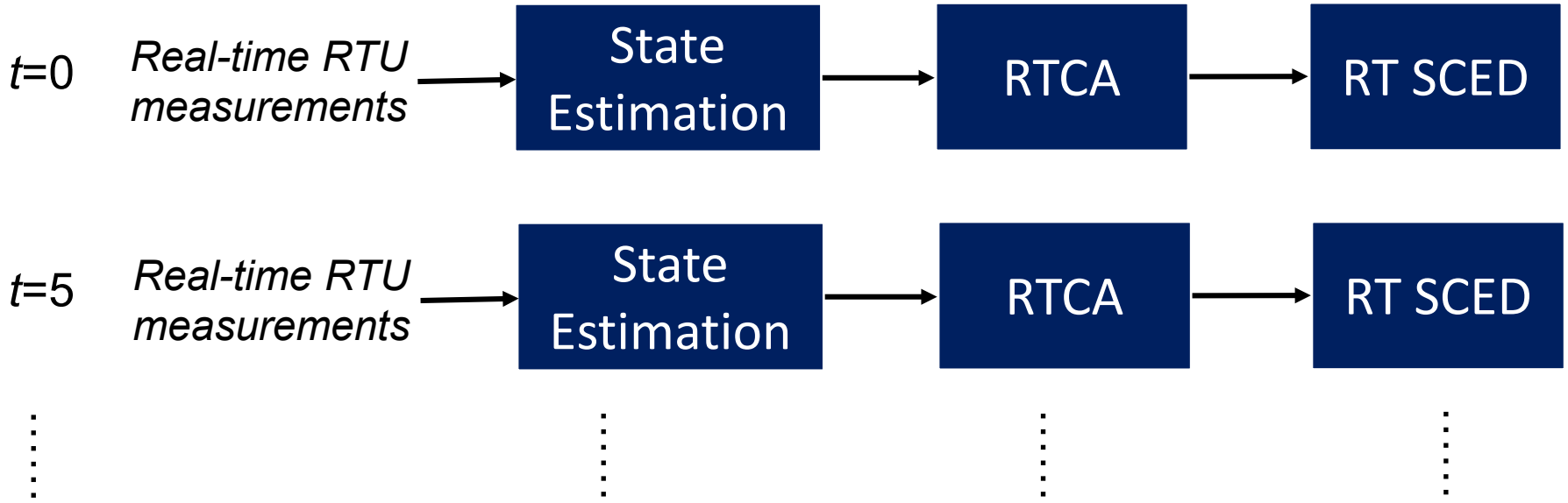
Conclusions (FDID)

- **FDI** cyber-attacks can cause unobservable flow **violations**.
- The proposed metric MLDI recognizes **malicious load changes** while BORI identifies **suspicious flow changes**.
- Simulation results demonstrate the **effectiveness** of the proposed **two-stage FDID approach**.
- The proposed two-stage FDID approach successfully detects **all** FDI attacks and correctly identifies the target for about **97%** of the cases.
- **Random** load fluctuations do **not activate** the FDID alert system.

Conclusions

Conclusions

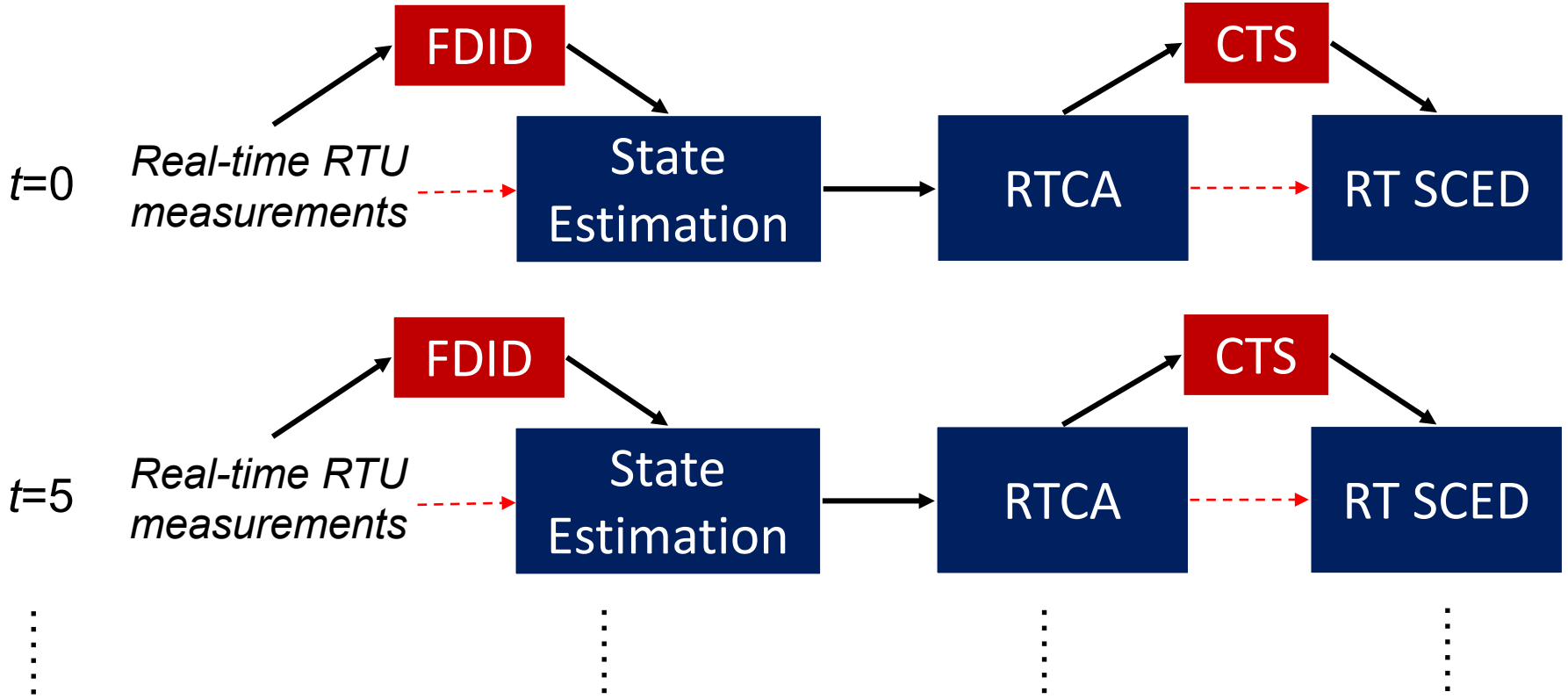
Current industry practices of power system **real-time** operations



This process repeats continuously in real time.

Conclusions

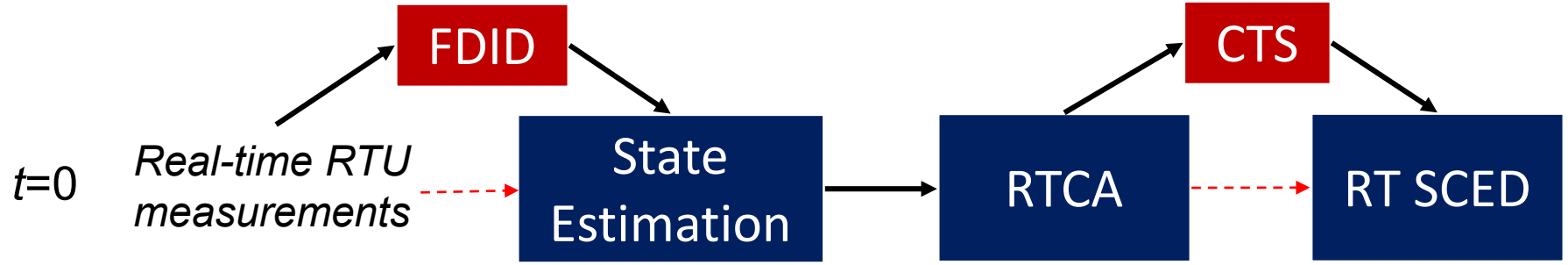
Enhancements of power system **real-time** operations



This process repeats continuously in real time.

Conclusions

Enhancements of power system **real-time** operations



- CTS can **reduce** post-contingency **violations** identified by RTCA and **reduce** RT SCED **congestion cost** by relieving network congestion.
- With the proposed CTS, the **flexibility** in transmission networks can **be utilized** in RTCA and RT SCED in a **practical** way.
- The proposed two-stage FDID approach can enhance state estimation by effectively **detecting** potential **FDI attacks**.

Future Work

Future Work

1) Investigation of *N*-1 in the post-switching situation
   - NERC requires systems to withstand the loss of a single bulk element (*N*-1).
   - This work demonstrates that CTS can enhance system reliability by reducing post-contingency violations.
   - However, the *N*-1 requirements in the post-switching situation are not studied in this work.
   - One future work is to investigate the system ***N*-1 reliability in the post-switching situation**.

Future Work

2) RT SCED with CTS

- This work demonstrates the effectiveness of the proposed Procedure-A and the proposed Procedure-B with a 179-bus artificial system.
- One future work is to investigate the proposed procedures on **large-scale real** power systems.

Future Work

3) FDI cyber-attack detection

- Simplified DC power flow model is used for this work.
- The attacker is assumed to have access to the entire system.
- The test case is IEEE 118-bus artificial system.
- Potential future work
  - extend this work to **AC** framework
  - assume the attacker has **limited access** (e.g. access to only a single area)
  - and use **large-scale practical** power systems for case studies.

Publications

- **Xingpeng Li**, P. Balasubramanian, M. Sahraei-Ardakani, et al. "Real-Time Contingency Analysis with Correct Transmission Switching," *IEEE Transactions on Power Systems*, vol. 32, no. 4, Jul. 2017.
- J. Lyon, S. Maslennikov, M. Sahraei-Ardakani, T. Zheng, E. Litvinov, **Xingpeng Li**, et al. "Harnessing Flexible Transmission: Corrective Transmission Switching for ISO-NE," *IEEE Power and Energy Technology Systems Journal*, vol. 3, no. 3, pp. 109-118, Sep. 2016.
- P. Balasubramanian, M. Sahraei-Ardakani, **Xingpeng Li**, et al. "Towards Smart Corrective Switching: Analysis and Advancement of PJM's Switching Solutions," *IET Generation, Transmission, and Distribution*, vol. 10, no. 8, pp. 1984-1992, May 2016.
- M. Sahraei-Ardakani, **Xingpeng Li**, P. Balasubramanian, et al. "Real-Time Contingency Analysis with Transmission Switching on Real Power System Data," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2501-2502, May 2016.
- **Xingpeng Li**, P. Balasubramanian, K. W. Hedman, "A Data-driven Heuristic for Corrective Transmission Switching," *North American Power Symposium (NAPS)*, Denver, CO, Sep. 2016.
- **Xingpeng Li**, K. W. Hedman. "Fast Heuristics for Transmission Outage Coordination," *19th Power Systems Computation Conference (PSCC 2016)*, Genoa, Italy, Jun. 2016.
- **Xingpeng Li**, P. Balasubramanian, Mojdeh Abdi-Khorsand, et al. "Effect of Topology Control on System Reliability: TVA Test Case," *Cigre US National Committee Grid of the Future Symposium*, Oct. 2014.

Thank You!

Questions?