UCI University of California, Irvine

Transient and Power Flow Study during Cyber-attack on Distributed Power System

Keyue Smedley, Anto Joseph

March 08, 2018

Overview

- *Cyber-Attack on Distribution Energy Sources*
  - *Attack on Reactive Power Control Set-point*
- *Cyber-Attack on Smart Meter*
- *Participation of Switched Capacitor Banks*
- *Results and Discussions*

Need of Reactive Power Control & IEEE Standard (U.S.)

Standard	Description
IEEE 1547 - 2003	Renewable Energy Sources shall not allow to regulate the grid voltage
IEEE 1547a - 2014	Renewable Energy Sources may help to regulate the grid voltage
IEEE 1547 - 2018	Renewable Energy Sources should provide *grid voltage support* *

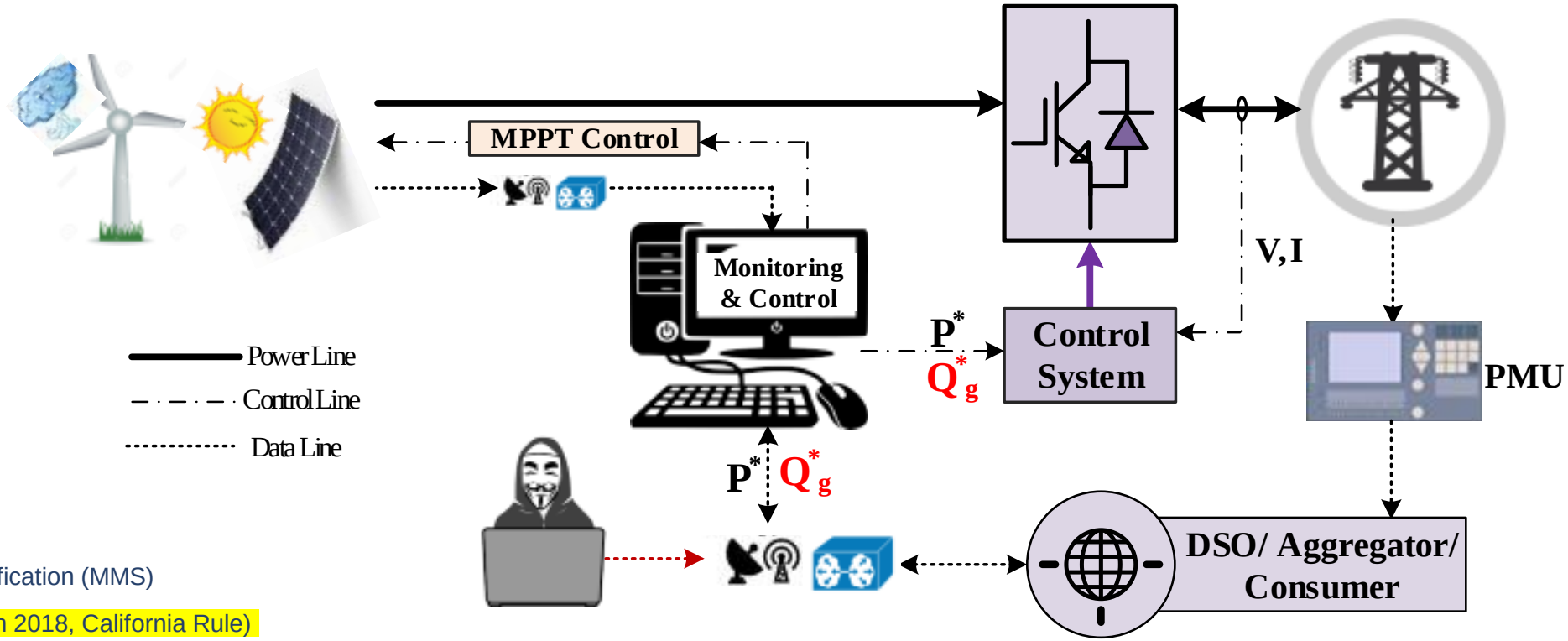
- Grid voltage level varies with power generation (wind, solar, etc.) and customer loading
- Static voltage regulators (switched capacitors, on load tap changers, etc.) are not efficient.
- Renewable energy sources can provide dynamic voltage support through smart inverters.

* *grid voltage support – dynamic volt/var control*

Control System for Distributed Energy Sources

P – Active Power

Q – Reactive Power



Communication Protocols

- Distributed Network Protocol (DNP3)
- IEC 61850 - Manufacturing Message Specification (MMS)
- IEEE 2030. 5 (SEP2) - Newest one (March 2018, California Rule)

Fig. Active and reactive power control

Reactive Power Control Algorithm

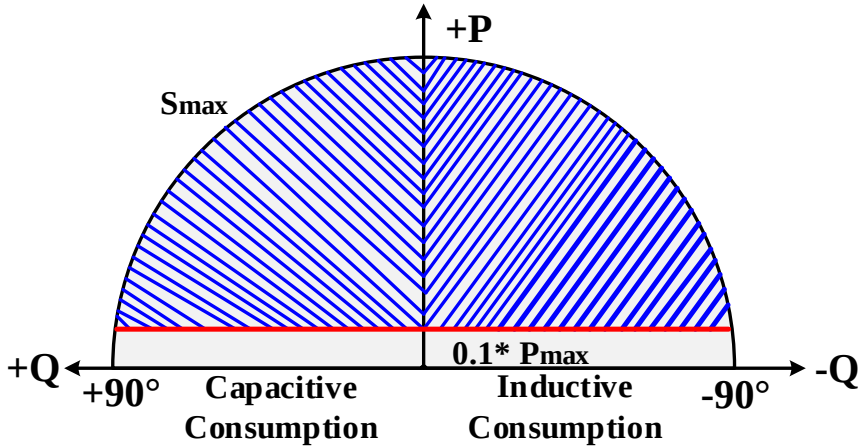


Fig. PQ – diagram of a generator

Active Power, $P_g = \frac{3}{2}\left|\vec{V}_g\right| \vec{I}_{dg}$ (1)

Reactive Power, $Q_g = -\frac{3}{2}\left|\vec{V}_g\right| \vec{I}_{qg}$ (2)

Apparent Power $S_g = \sqrt{(P_g)^2 + (Q_g)^2} << S_{g(\max)}$ (3)

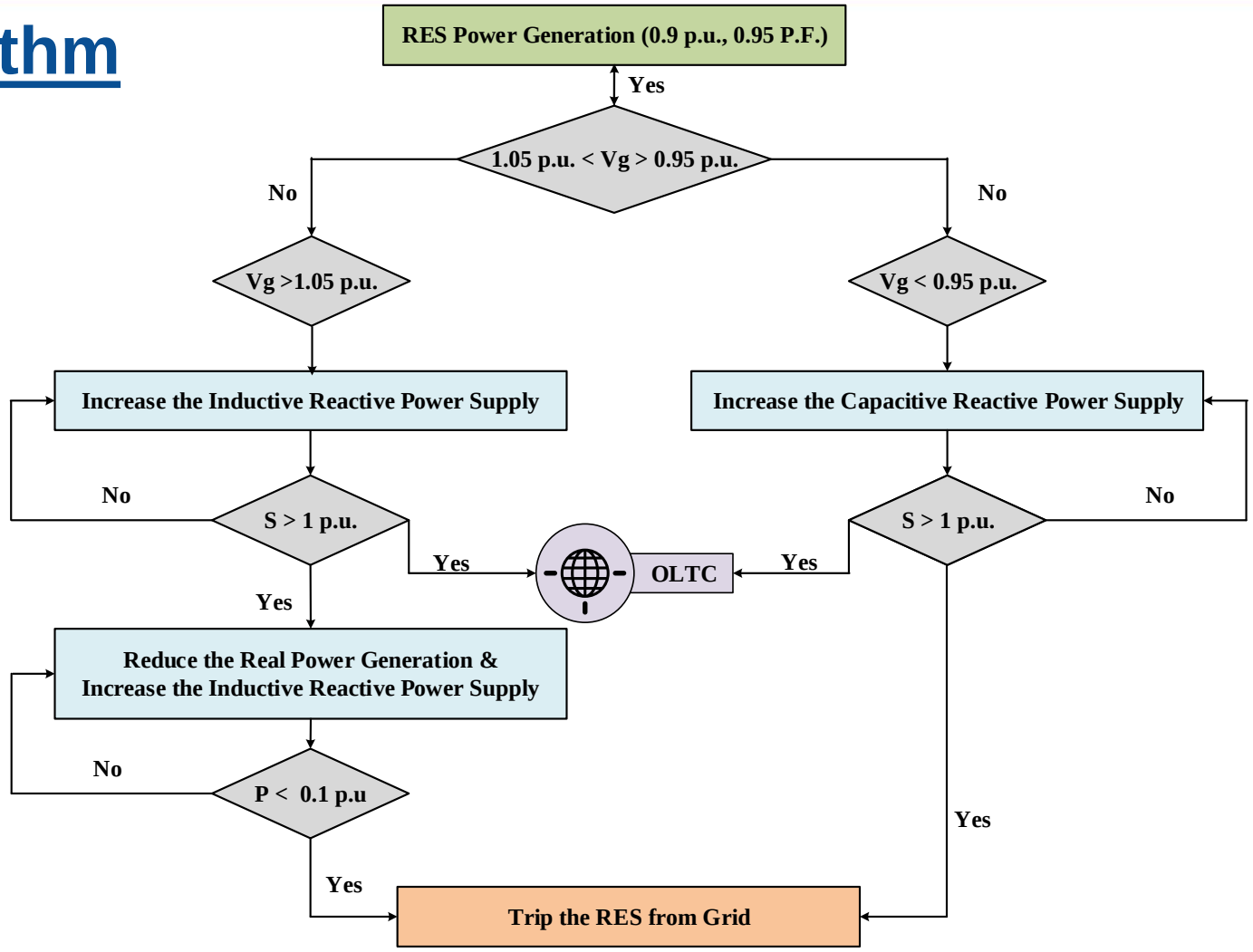


Fig. Flowchart for grid voltage regulation

Possible Attack Scenarios on Reactive Power Control

Case 1: Change the inductive reactive power from minimum to maximum (i.e. from 0.95 lag to 0.1 lag)

- Grid voltage at nearby feeders are significantly reduced.
- Can reduce the active power generation ; activate the voltage regulators (On Load Tap Changer (OLTC)), switch-in capacitors (SC)
- Produce the voltage transients, could activate other electrical components (i.e. switchgears)

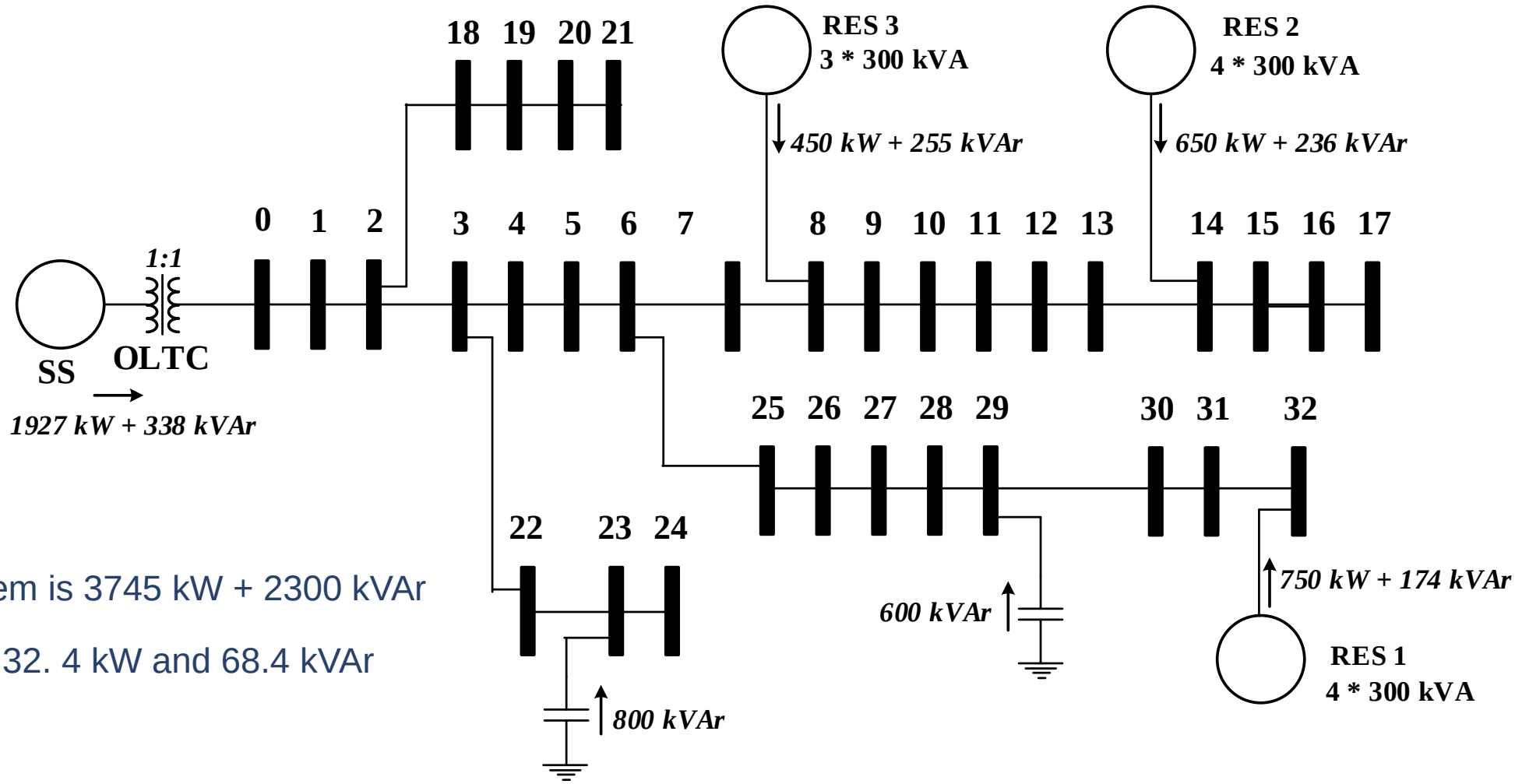
Case 2: Change the minimum inductive reactive power to maximum capacitive reactive power (i.e. from 0.95 lag to 0.1 lead)

- Grid voltage increased beyond the limit (i.e. 1.05 Vg)
- Can reduce the active power generation of its own and nearby sources; activate the voltage regulators (OLTC)

Case 3: Repeatedly change the reactive power control value

- Repeatedly changes the reactive power set-point to maximum inductive/capacitive reactive power.
- It troubles the OLTC in view of voltage transients, arcing current and wear & tear.
- OLTC can be isolated from the DPS and lead to blackout
- It may lead to cascaded failures in the power grid.

Test Unit (Modified IEEE 33- distributed bus)

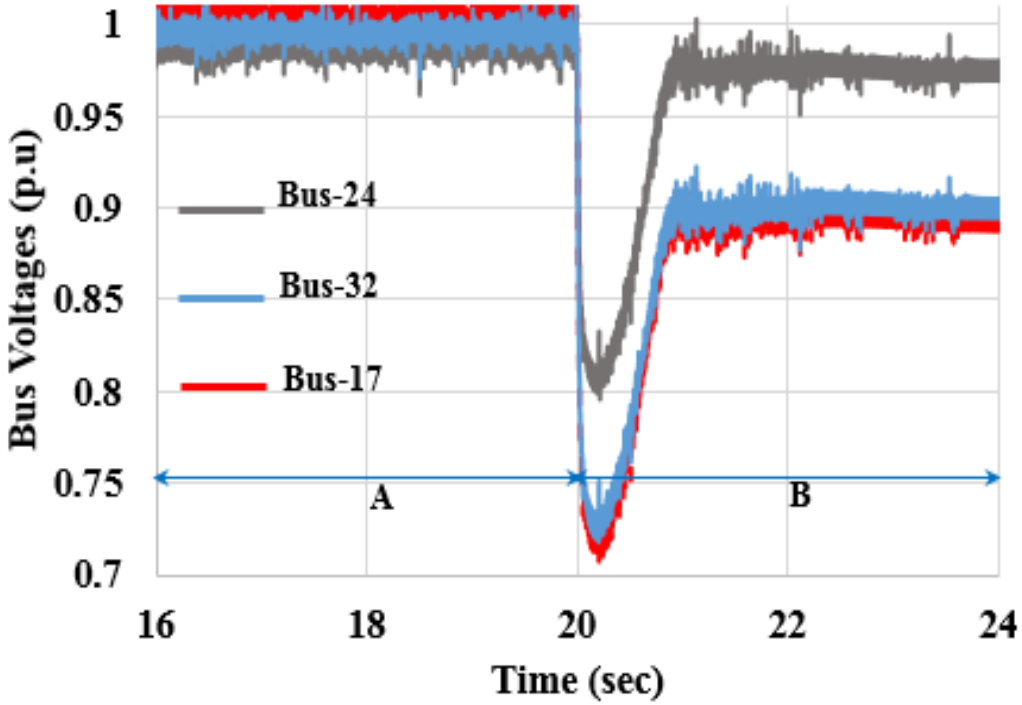


- Total load of the system is 3745 kW + 2300 kVAr
- Total power losses is 32. 4 kW and 68.4 kVAr

Simulation Results…

Case 1 : maximum inductive reactive power supply to the grid (Coordinated attack)

- ***Sources connected with the nearby buses are (i.e. bus-32 and bus 17) are highly affected***
- ***It produces the voltage transients that could influence the other electrical components (i.e. switch gear)***



A – Regular operation
B – Absorbing reactive power from grid

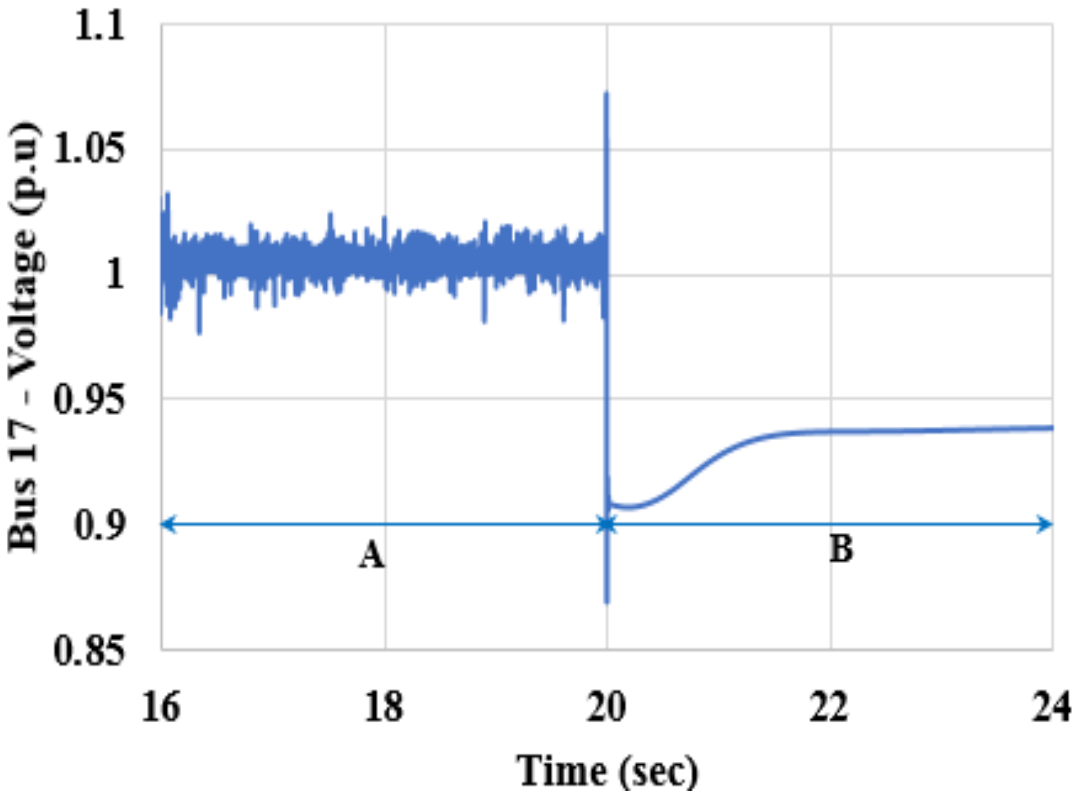
Note: OLTC is deliberately not operated

Simulation Results…

Case 2 : Tripping a renewable energy source (bus-14)

- ***17% of total power generation is tripped***
- ***Causes a voltage violation (i.e. < 0.95 Vg p.u.) from bus 10 – bus 17.***

	Regular Operation (650 kW + 236 kVAr)	RES-2 tripped off from grid
Grid Voltage (Bus-17)	1.004 p.u.	0.938 p.u.
Power Losses	32.4 kW + 68.4 kVAr	74.3 kW + 82.3 kVAr



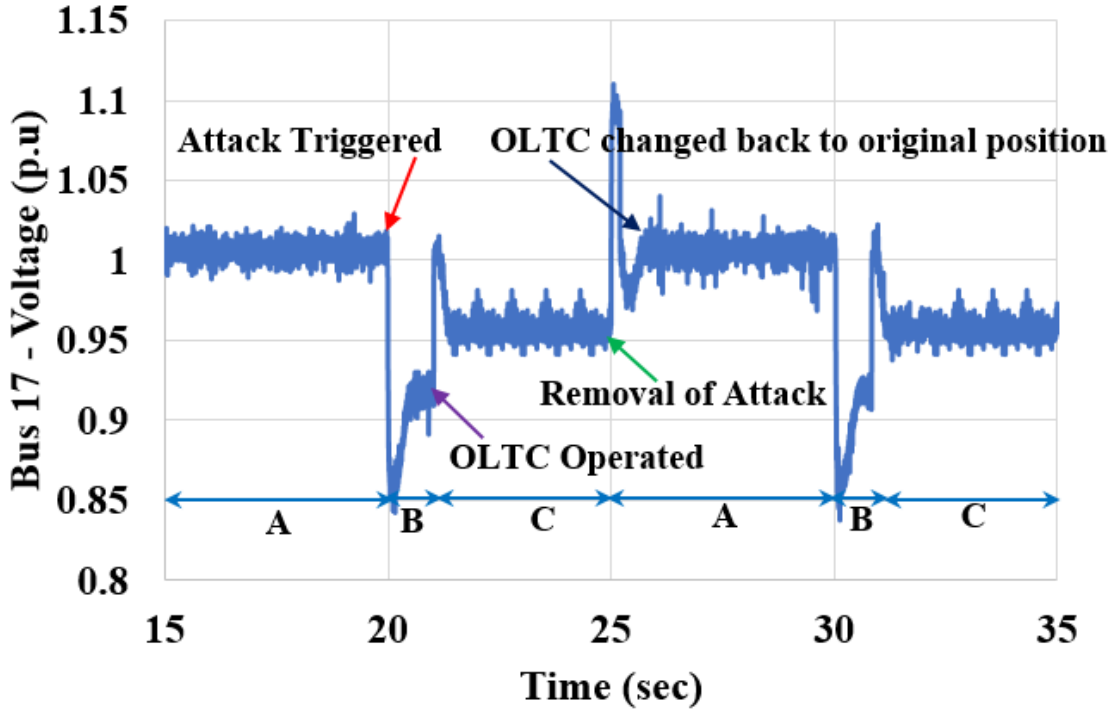
A – Regular operation
B – RES is tripped (bus-14)

Note: OLTC is deliberately not operated

Simulation Results…

Case 3 : Repeatedly changes the reactive power control value

- ***OLTC is not operated during the transient period and repeatedly switch ON/OFF with respect to grid voltage.***
- ***Blackout may occur.***



A – Regular operation
B – Fault triggered (i.e. absorbing reactive power from grid)
C – OLTC Operation

Note: OLTC is operated when grid voltage (Bus-17) reduces to 0.95 p.u.

Smart Meter Architecture

Communication Protocols

- Modbus/TCP
- Distributed Network Protocol (DNP3)
- Zigbee/Wi-Fi

- *Smart meters can control the electrical appliances regarding energy demand management.*

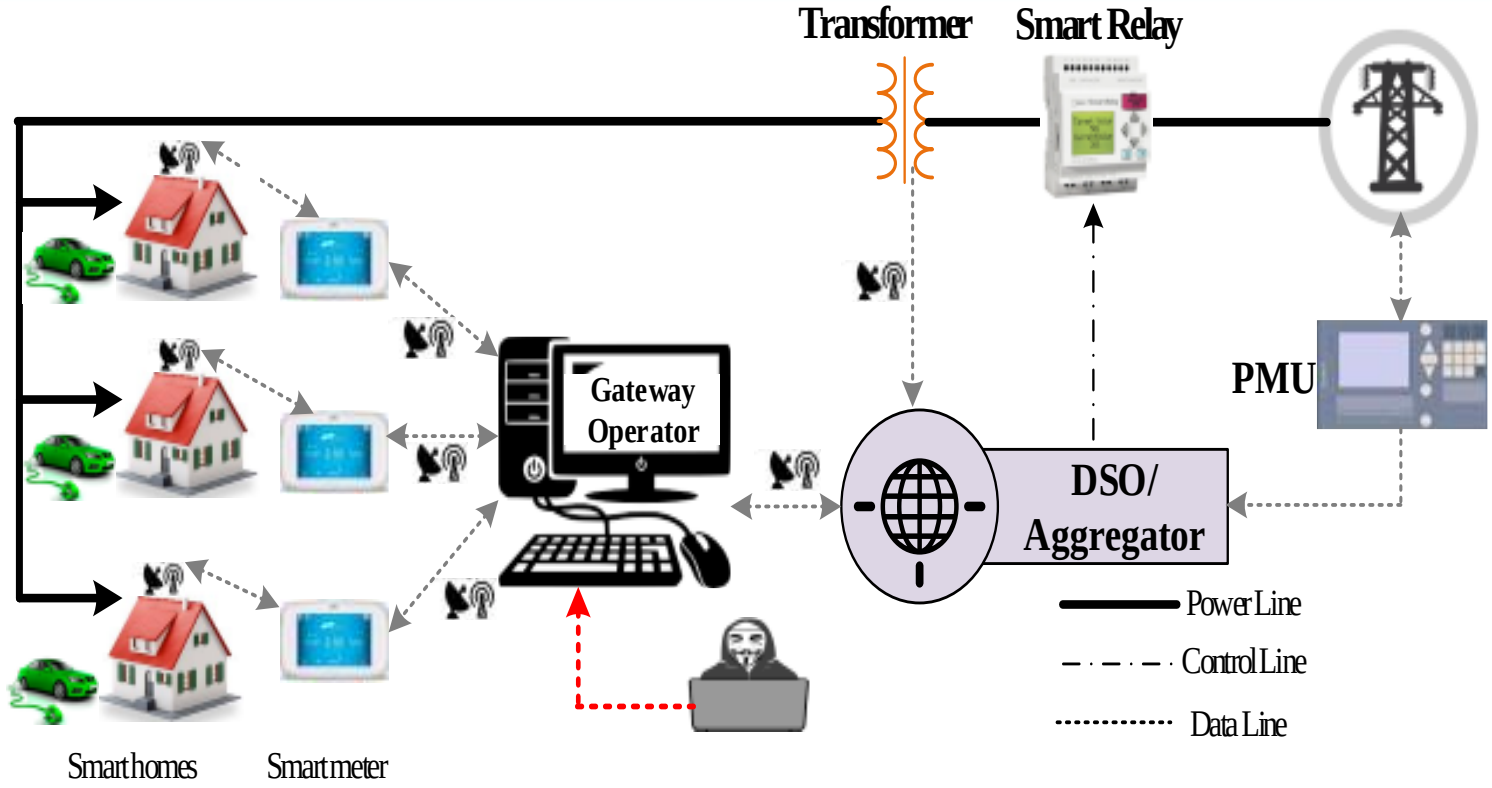
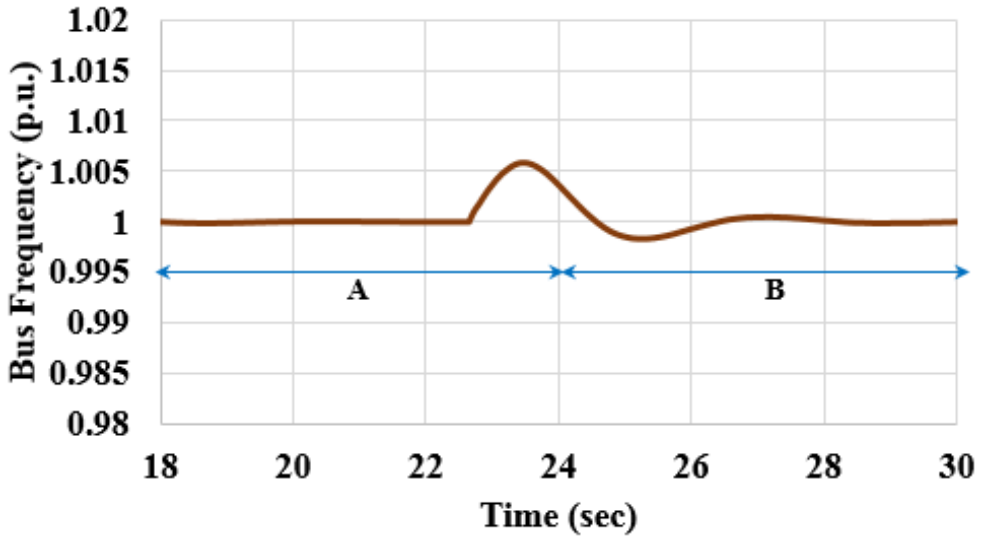


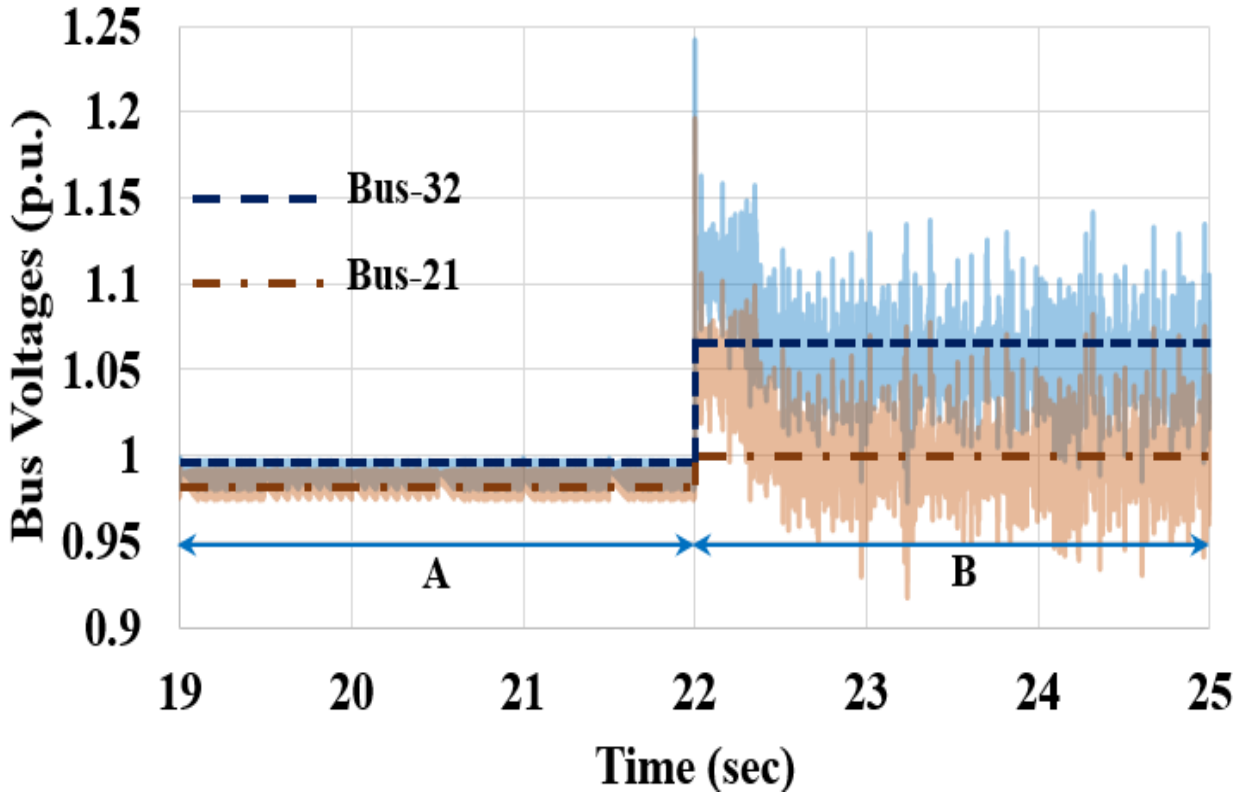
Fig. Connection of smart homes to grid

Disconnection of Loads (Bus 26 – Bus 32)

- ***Grid voltage is increased.***
- ***Could result to shutdown the renewable energy sources.***
- ***Activate the voltage regulators (i.e. OLTC).***



A – Regular operation; B – Load disconnected

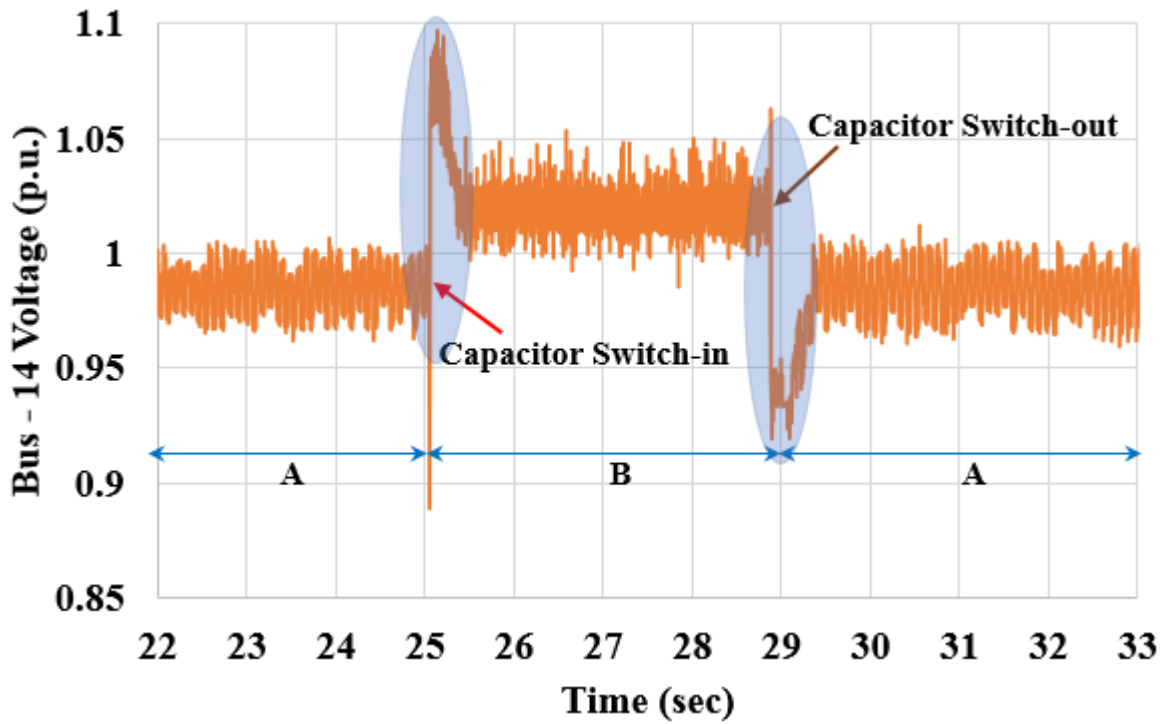


A – Regular operation; B – Load disconnected

Note: OLTC is deliberately not operated

Switched Capacitor Activation (Bus-14)

- *Grid voltage is increased.*
- *Voltage transients*
- *Could result to shutdown the renewable energy sources.*



A – Regular operation; B – Capacitor switch-in

Result and Discussions

Cyber-Attack on Reactive Power Control

- *Highly capacitive reactive power lead to reduce the active power feed-in and could trip off the RES from DPS.*
- *High Inductive reactive power lead to voltage reduction/large voltage transients in buses and could affect the electrical devices connected in it.*
- *Coordinated and repeated attack on reactive power control may result in blackout.*

Cyber-Attack on Smart Meter

- *Could lead to increase/decrease the grid voltage.*

Participation of Switched Capacitor Banks

- *Could lead to increase the grid voltage and affect the renewable energy sources and voltage regulators; cascaded failure could happen*

Table: Impact of Cyber-Attack to the Distributed Power System Components

Electrical Power Systems/Equipment's	Distribution Energy Sources	Reactive Power Controller	Energy Storage Devices	Electric Vehicle Charging Station	Micro Phase Measurement Unit	Smart Meters	Connected Loads	Switchgears	Transformer
Distribution Energy Sources [1]	Medium	Very High	Very High***	Medium	High	Medium	Low*	High	High
Reactive Power Controller [2]	Very High	Medium	High	Medium	High	Medium	Medium	Medium	High
Energy Storage Devices [3]	Very High***	High	Medium	Medium	High	Medium	Medium	Medium	Medium
Electric Vehicle Charging Station	Medium	Medium	Medium	Medium	High	Medium	Low*	Medium	Medium
Micro Phase Measurement Unit	High	High	High	High	High	High	High	High	High
Smart Meters	Medium	Medium	Medium	Medium	High	Low	Low*	Medium	Medium
Connected Loads [4]	Low	Medium	Medium	Low	High	Low	Low*	Medium	Medium
Switchgears [5]	High	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium
Transformer [6]	High	High	Medium	Medium	High	Medium	Medium	Medium	Medium

[1] Wind power generation, Solar power generation, etc.
[2] Capacitor banks, Static VAR compensators, Reactive power control in DER, etc.
[3] Batteries, Flywheel Energy Storage, Micro Pumped Storage Power Plant, etc.
[4] Industrial and Commercial Loads, etc.
[5] Relays, Circuit Breakers, etc.
[6] Load Tap Changers
* depends on percentage of load disconnection (e.g. more than 50% of withdrawal of load from the network affects the utility of the grid)
** distribution power system fully or more than 75% depend on renewable power generation

Low	- Affect the group of users connect to the same network (e.g. blackout the single apartment)
Medium	- Affect the group of users (e.g. blackout the group of apartments)
High	- Affect the entire housing community of the town (e.g. blackout the entire town)
Very High	- Affect the utility of the power grid (e.g. blackout the entire city)

References

1. *T.T. Ku, C.H. Lin, C.S. Chen, and C.T. Hsu, "Coordination of transformer on-load tap changer and PV smart inverters for voltage control of distribution feeders," IEEE Trans. Ind. Appl., vol. 55, no. 1, Jan./Feb. 2019.*
2. *NM Albuquerque, "IEEE 1547 standard for interconnecting distributed energy resources with electric power systems - Enabling advanced power electronics technologies for the next generation electric utility grid", July 2018.*
3. *J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28-39, 2016.*
4. *B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber-attacks on transient stability of smart grids with voltage support devices," IEEE Power and Energy Society General Meeting (PES), pp. 1-5, Vancouver, BC, 2013.*
5. *B. Chen, Z. Lu and H. Zhou, "Reliability assessment of distribution network considering cyber-attacks," IEEE Conference on Energy Internet and Energy System Integration (EI2), pp. 1-6, Beijing, 2018.*
6. *Y. Isozaki et al., "Detection of cyber-attacks against voltage control in distribution power grids with PVs," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1824-1835, July 2016.*
7. *A. Teymouri, A. Mehrizi-Sani and C. Liu, "Cyber security risk assessment of solar pv units with reactive power capability," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 2872-2877, Washington, DC, 2018.*
8. *B. Kang et al., "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), pp. 1-8, Luxembourg, 2015, pp. 1-8.*

THANKS FOR YOUR ATTENTION !

Any Questions