Cyber-Resilient Control of Inverter Based Microgrids

IEEE Global Signal & Information Processing Conference

Martine Chlela

McGill University
Electric Energy Systems Laboratory
http://www.power.ece.mcgill.ca/

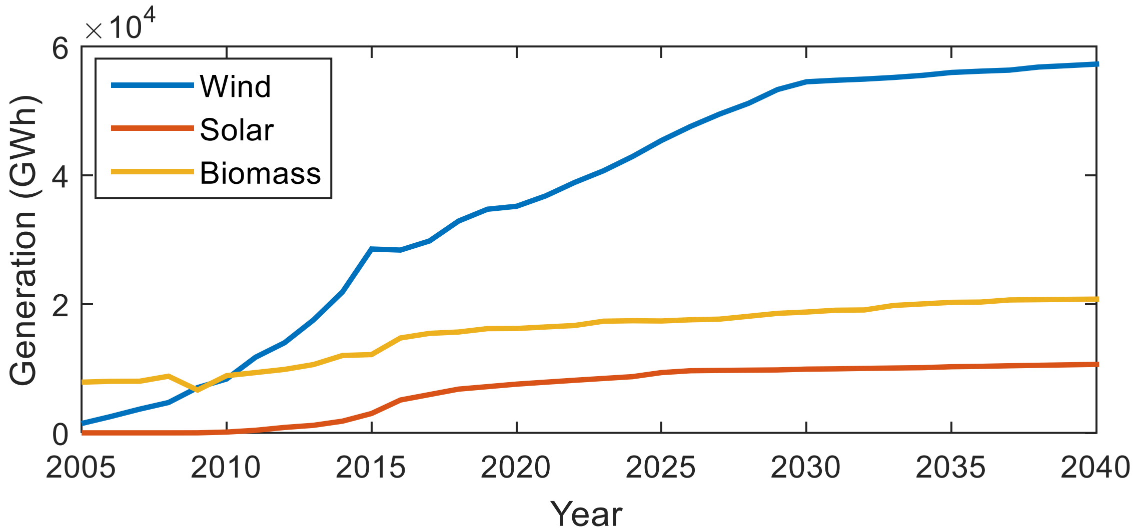
7-9 December 2016

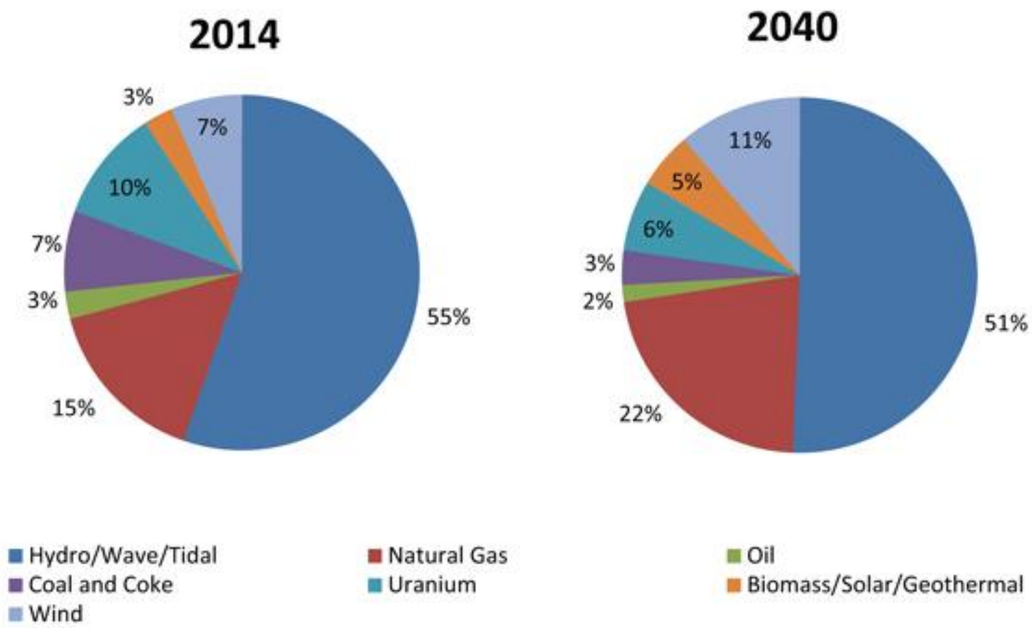
Outline

- Background
- Microgrid Power Electronic Interfaced DERs Types & Control
- Microgrid Control Architecture
- Cyber Security for Microgrids
- Proposed Cyber Resilient Control Strategy
- Microgrid Benchmark System & Simulation Results
- Conclusion

McGill UNIVERSITY

Background –
Renewable Energy Penetration





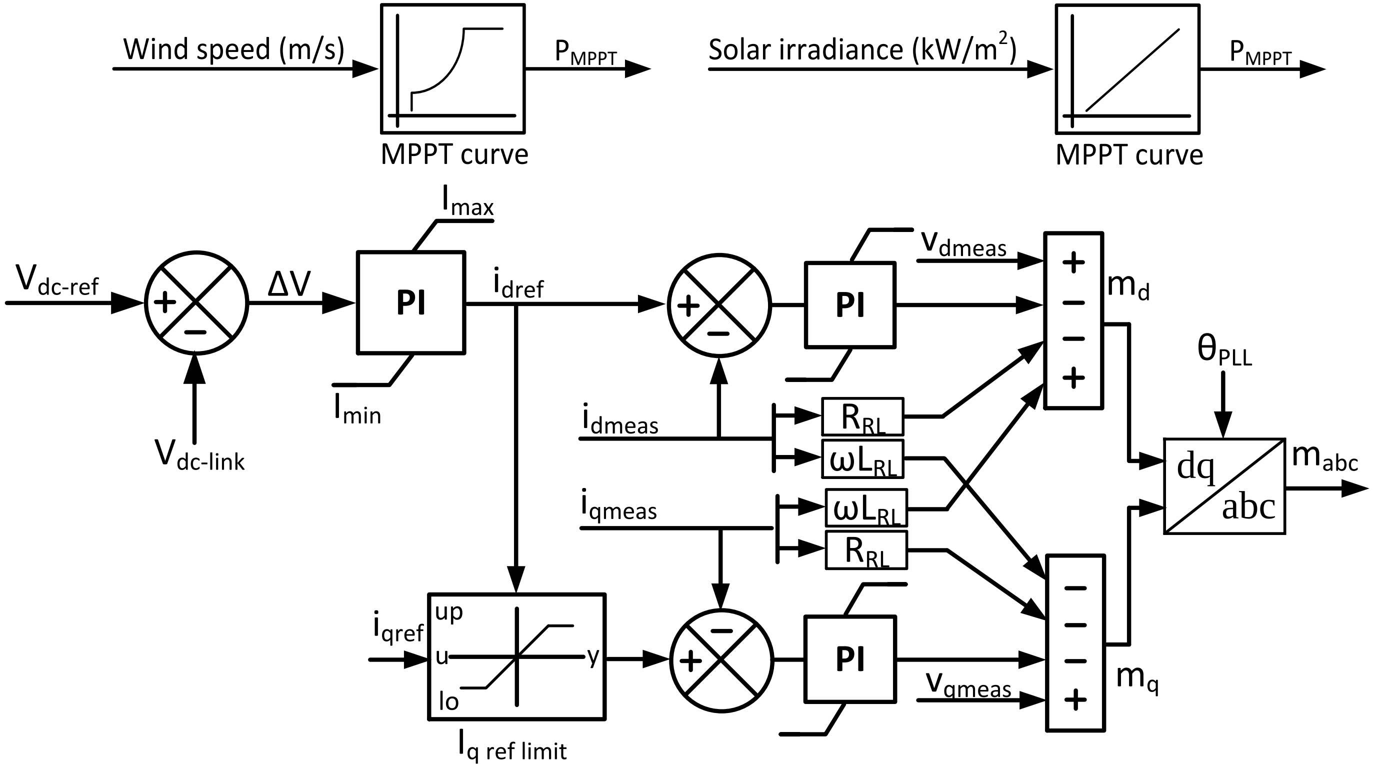
Source: Government of Canada

Background – *Power Electronic Interfaces*

- Power electronic inverters are used to interface the extensively deployed renewable DERs in microgrids
  - Decouple the rotating masses from the grid i.e. type 4 wind turbine
  - Interface systems with no inertia i.e. photovoltaics and energy storage
  - Provide poor V&f response in the event of disturbances due to the lack of inertia
  - Control of PEI DERs is a major concern, specially in 100% inverter-interfaced islanded microgrids

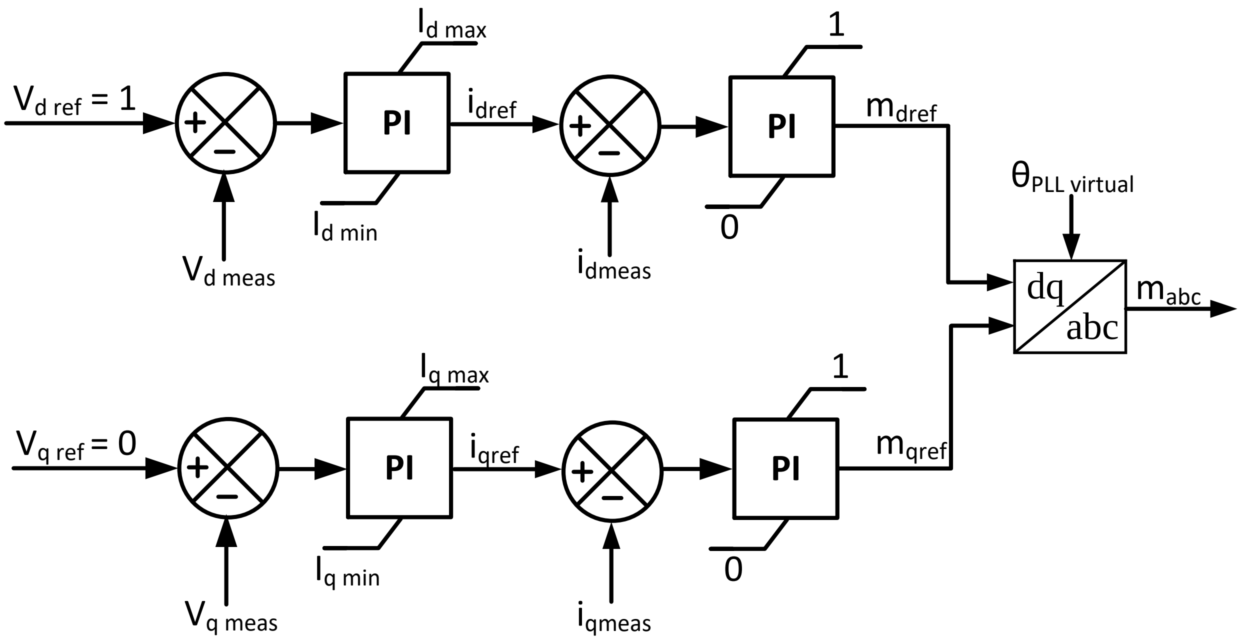
Microgrid PEI DERs Types & Control–
Renewable DER Current-Controlled VSI

- Grid-tie inverters with DC-links fed from DC-DC converters with power control loops following MPPT curves. No active regulation of V&f
- The VSI outer loop generates an inverter current reference to maintain a DC-link voltage

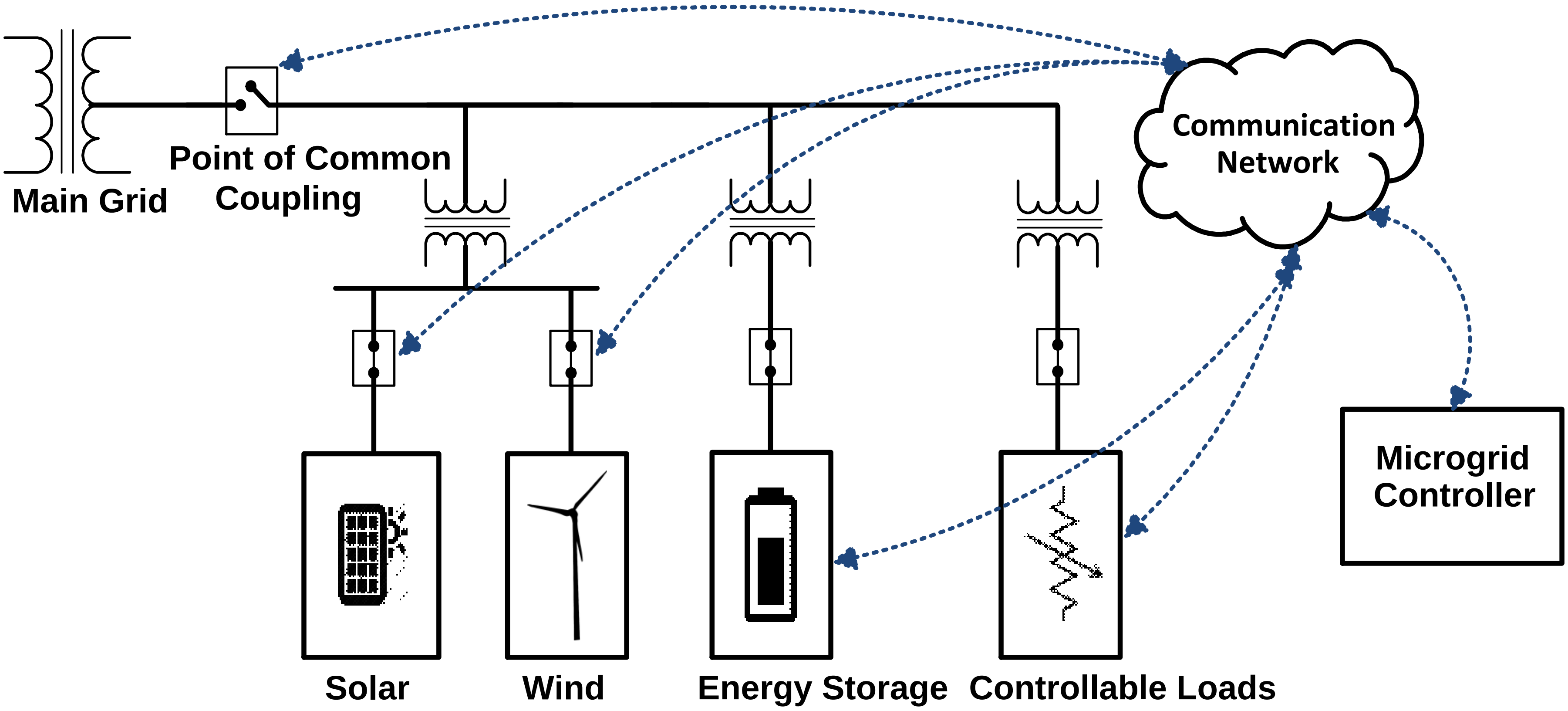


Microgrid PEI DERs Types & Control–
Isochronous ESS Voltage-Controlled VSI

- The ESS is operated as the isochronous resource to set & regulate the islanded microgrids voltage and frequency
- The VSI outer loop regulates the grid voltage to its reference value. The inner loop controls the inverter current. The grid-side frequency is readily imposed by a virtual PLL



Microgrid Control Architecture –
Reliance on Communications



Cyber Security for Microgrids –
Types of Cyber-Attacks

Availability

Block, delay or corrupt communications to make the network resources unavailable

Confidentiality

Eavesdrop on communication network to acquire confidential information

Integrity

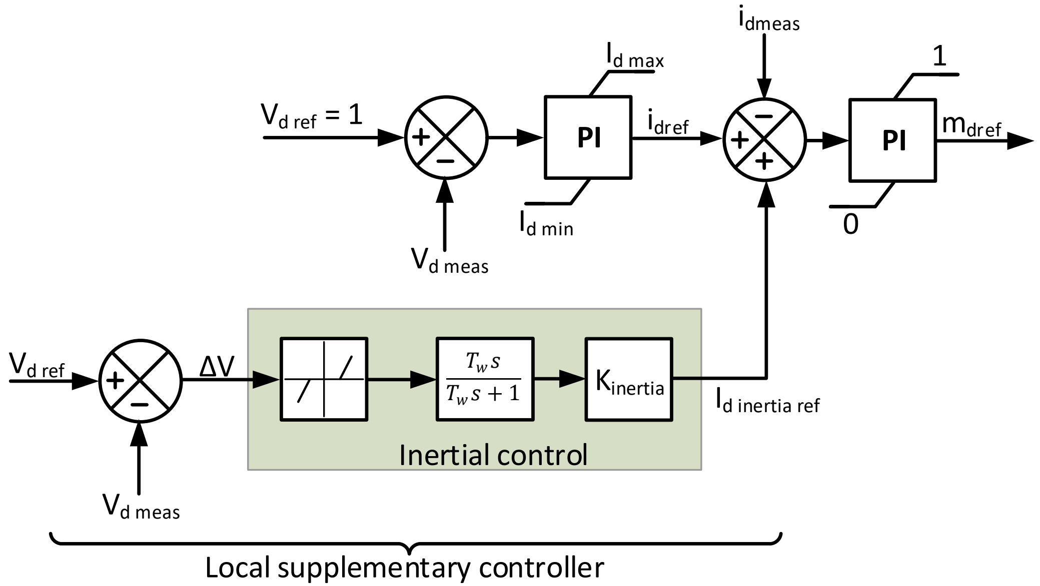
Malicious modification or corruption of measurements and commands exchanged in the grid

Cyber Security for Microgrids –
Data Integrity Cyber-Attack & Performance Metrics

- The cyber-attack tampers with the protection and control commands sent to the DERs circuit breakers to modify their status causing their sudden disconnection
  - A DER disconnection requires a surge in power from the isochronous generator - more current to be supplied by the PEI
  - In 100% inverter-interfaced microgrids, active power is proportional to voltage
  - Large active power imbalances cause severe voltage excursions at the grid side that could not be remediated by local controllers
  - Cyber-resilient & intelligent control algorithms need to be employed to mitigate the attack

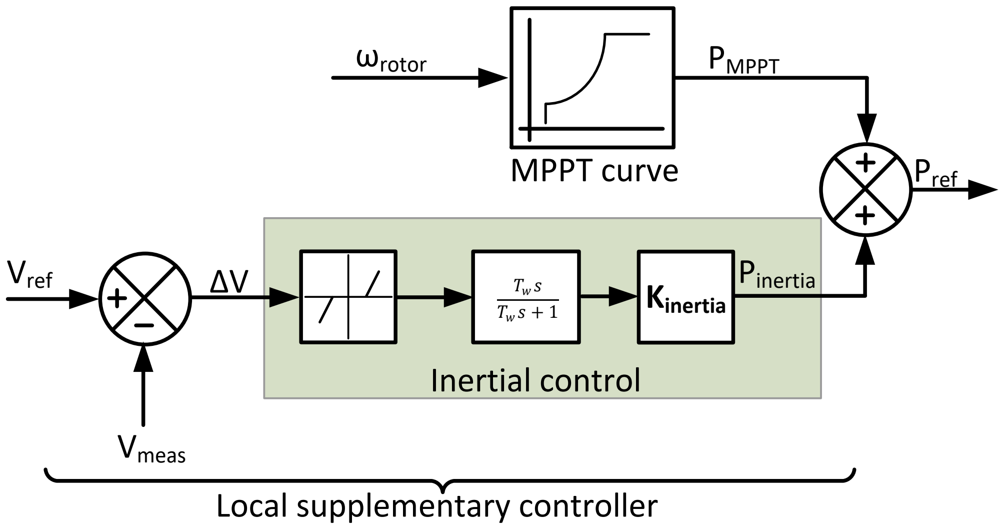
Proposed Cyber-Resilient Control Strategy –
Supplementary Control Loop for the Voltage-Controlled VSI

- In analogy with the virtual inertia concept applied to regulate frequency excursions, a virtual inertial controller is added to the PEI DERs primary control loops to provide transient voltage support
- The inner current regulation control loop of the ESS VSI modified
- $\Delta V \nearrow$ $I_{d\ inertia\ ref} \nearrow$ $I_{d\ ref} \nearrow$ - The resulting contribution is limited by the maximum inverter current



Proposed Cyber-Resilient Control Strategy – *Supplementary Control Loop for the Current-Controlled VSI*

- The MPPT controller of the WTG is also modified to incorporate virtual inertia
- The virtual inertia active power contribution is added to MPPT reference to set the WTG power reference. The supplementary control contribution is limited by the WTG dynamics



Proposed Cyber-Resilient Control Strategy – *Conventional Load Shedding Scheme*

- In the event of large active power disturbances causing the grid-forming ESS and WTG to saturate, virtual inertial control would not be sufficient to provide complete compensation and voltage regulation
- Traditional UVLS employed to shed % of loads in proportion to voltage excursions – in analogy to UFLS of the NERC standard.

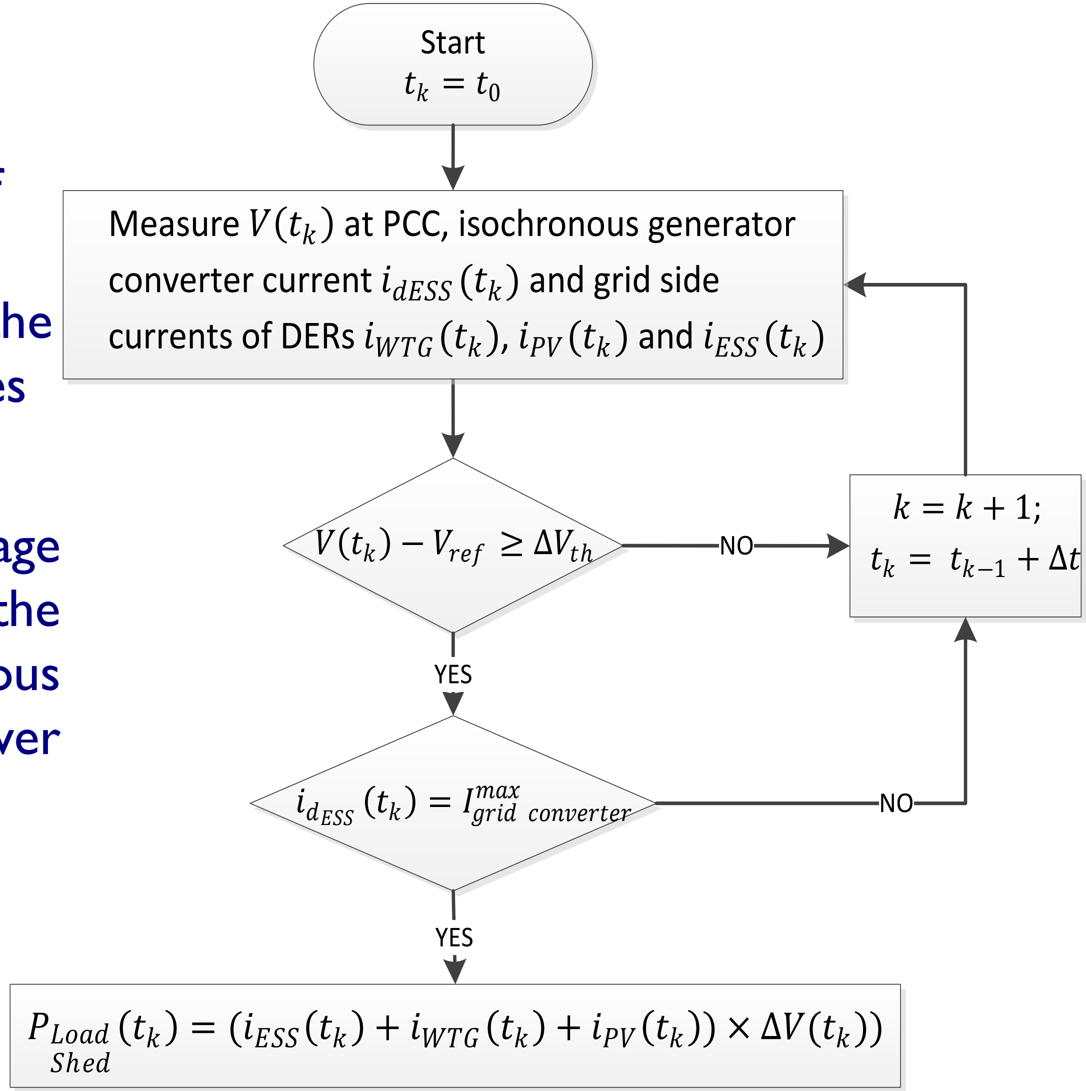
Voltage Threshold (p.u.)	Total time (s)	Load shed at stage (%)	Cumulative load shed (%)
0.9750	10.0	3	31
0.9816	0.30	7	28
0.9850	0.30	7	21
0.9883	0.30	7	14
0.9916	0.30	7	7

McGill UNIVERSITY

Proposed Cyber-Resilient Control Strategy – *Adaptive Load Shedding Scheme*

- The adaptive load shedding scheme developed activate if
  1) $\Delta V_{pcc} \leq \Delta V_{th}$
  2) the current reference of the isochronous DER VSI reaches its maximum rated value

- Load is shed only when voltage excursions are due to the inability of the isochronous DER to generate more power and provide balance



McGill UNIVERSITY

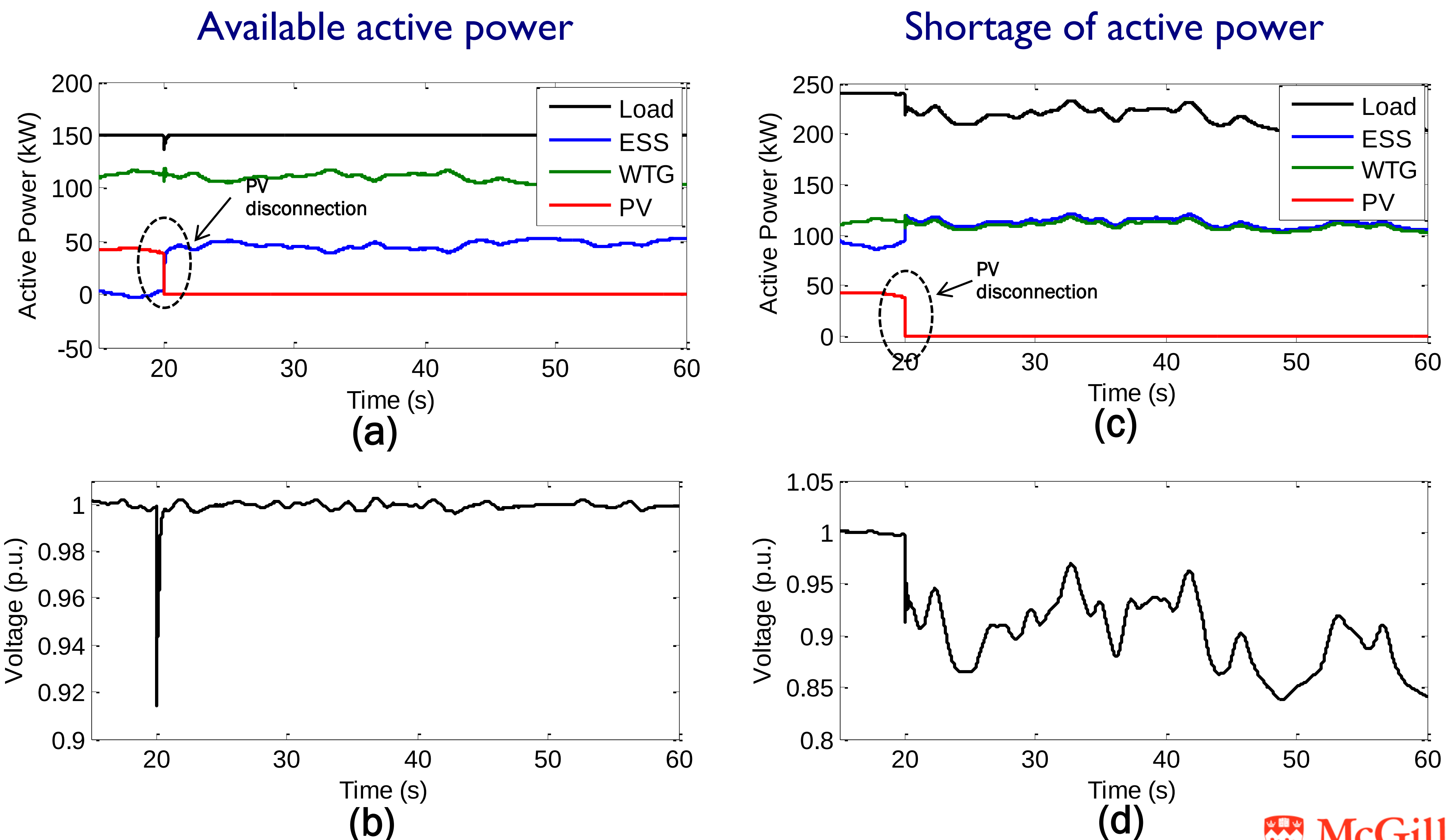
Microgrid Benchmark System

- 25kV distribution system adapted from a utility feeder and reconfigured as a microgrid
- Microgrid PEI DERs & control employed:
  - 150 kW WTG
  - 50 kW PV source

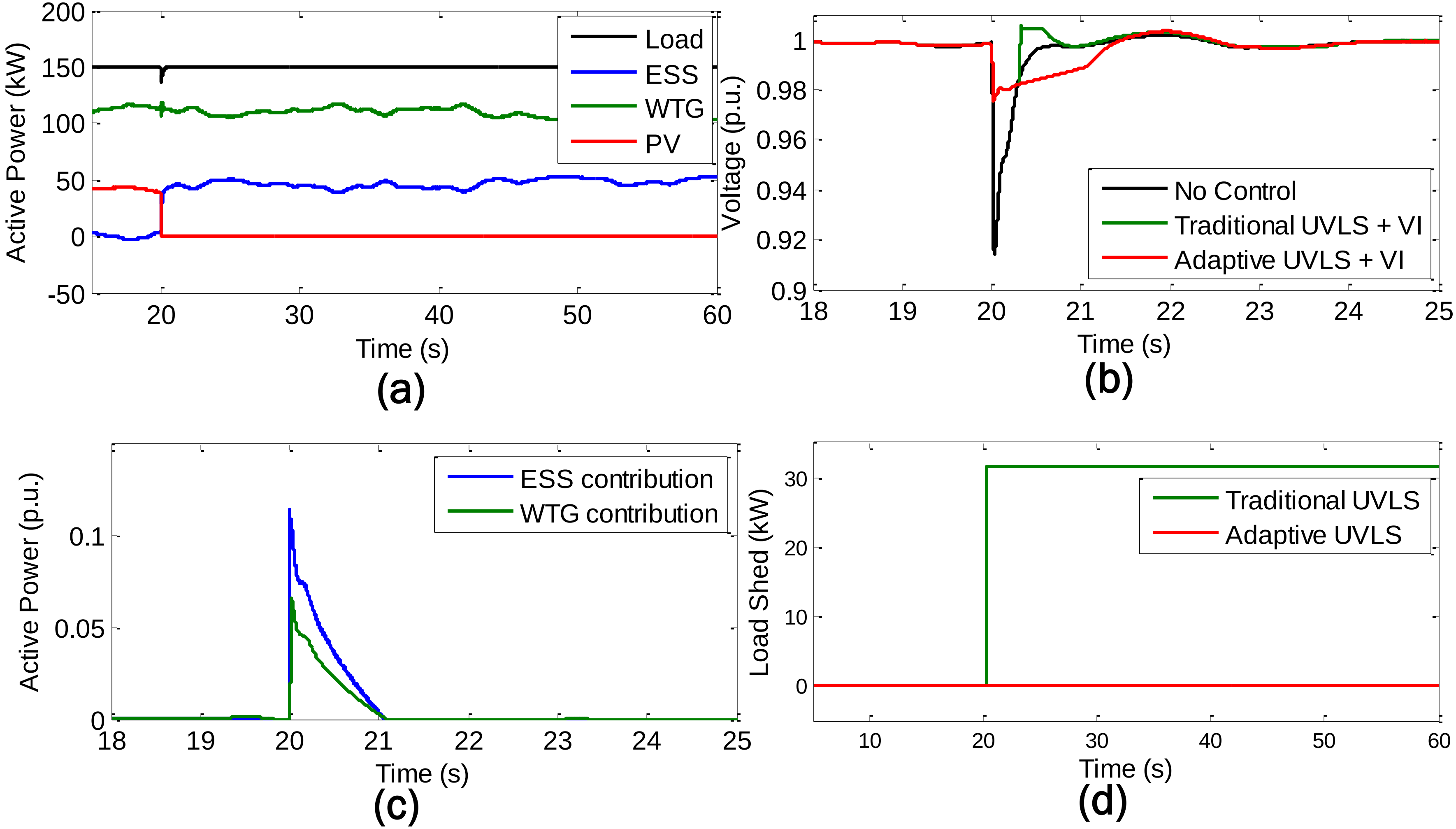
  } interfaced through a current controlled grid-tie inverter, following the corresponding MPPT curves
  - 125 kW/125kWh ESS – operated as the grid forming DER regulating & forming the voltage and frequency of the islanded microgrid
- Cyber-attack considered: Attacker with valid user credential gains access to the operator workstation and tampers with the command sent to the PV unit circuit breaker causing a sudden disconnection of the renewable source at 20 seconds

McGill UNIVERSITY

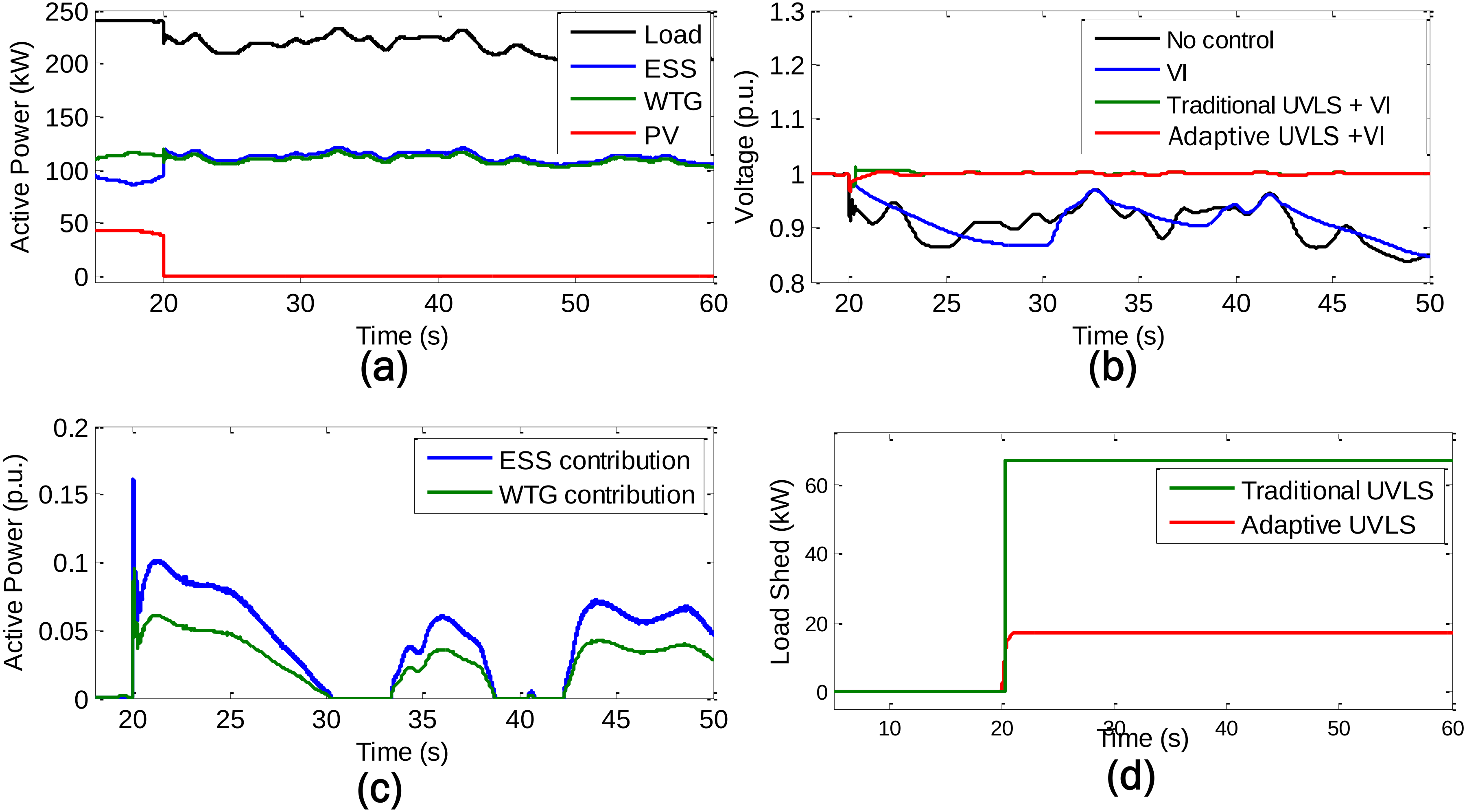
Impact assessment –
Data integrity cyber-attack on Inverter-interfaced microgrids



Case Study 1 – Available Active Power
Mitigation Performance & Validation



Case Study 2 – Shortage of Active Power
Mitigation Performance & Validation



Results Summary

		Voltage nadir (p.u.)	Load shed (kW)
Case 1	No control	0.9139	--
	Virtual Inertia	0.9757	--
	Traditional UVLS + VI	0.9757	31
	Adaptive UVLS + VI	0.9757	0
Case 2	No control	0.8653	--
	Virtual Inertia	0.8682	--
	Traditional UVLS + VI	0.9655	67.2
	Adaptive UVLS + VI	0.9666	17.13

- Virtual inertia provides sufficient compensation
- Virtual inertia does not provide sufficient compensation as the DER capacity limits are reached
- Unnecessary load shedding due to traditional UVLS
- Unnecessary load shedding due to traditional UVLS

Conclusion

- Impact assessment of data integrity cyber-attacks on the power management strategies of 100% inverter-interfaced islanded microgrids
- Two-layer cyber-resilient control consisting of supplementary local control loops and load management schemes to enhance resilience to attacks
  - Virtual inertial control added to the WTG and the ESS primary controllers provides transient voltage regulation by smoothing the ramps streaming from the cyber-attack
  - Adaptive load management strategy to overcome the DERs rated capacity limits ensures post-attack active power balance

McGill UNIVERSITY

Q&A

Thank you!!

Martine Chlela

martine.chlela@mail.mcgill.ca

Electric Energy Systems

Laboratory

http://www.power.ece.mcgill.ca/

McGill University

