Towards Distributed Intelligence and Controls for Emerging Energy Systems

August 25, 2022

Soumya Kundu
Senior Engineer, PNNL

PNNL is operated by Battelle for the U.S. Department of Energy

Acknowledgement

- Collaborators, postdoc, and intern mentees!
  - PNNL: K Kalsi, SP Nandanoori, V Adetola, S Choudhury
  - U-Mich: IA Hiskens, S Geng (PNNL intern)
  - UIUC: M Ornik, JB Bouvier (PNNL intern)
  - U of Vermont: MR Almassalkhi
  - WSU: S Roy
  - LANL: M Anghel
- Our sponsors: US Department of Energy, PNNL-LDRD (RD2C Initiative)

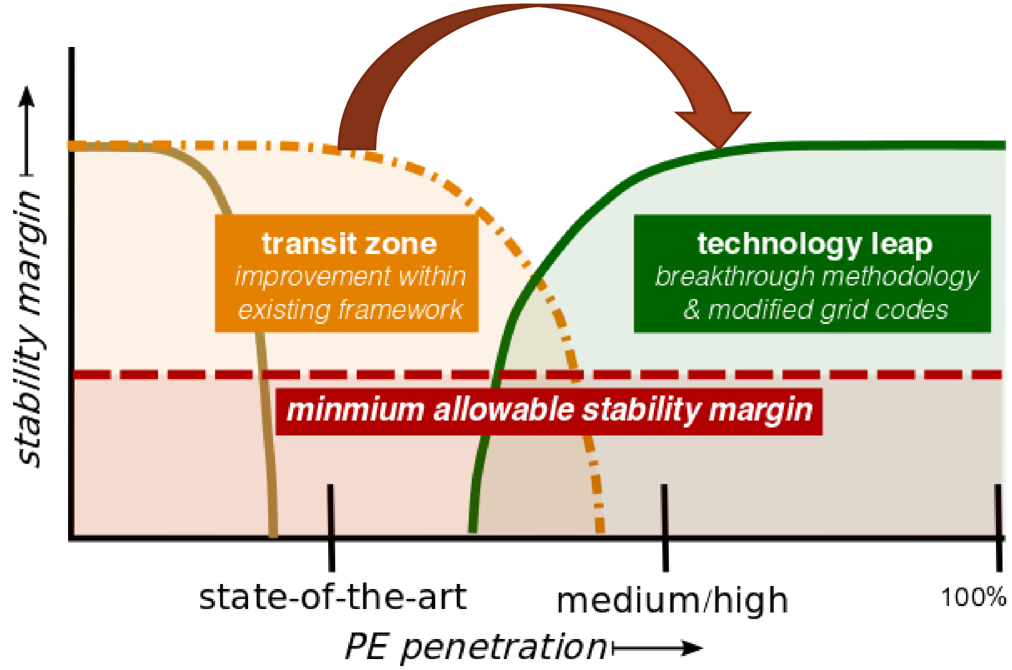
Pacific Northwest NATIONAL LABORATORY

Acknowledgement

- Collaborators, postdoc, and intern mentees!
  - PNNL: K Kalsi, SP Nandanoori, V Adetola, S Choudhury
  - U-Mich: IA Hiskens, S Geng (PNNL intern)
  - UIUC: M Ornik, JB Bouvier (PNNL intern)
  - U of Vermont: MR Almassalkhi
  - WSU: S Roy
  - LANL: M Anghel
- Our sponsors: US Department of Energy, PNNL-LDRD (RD2C Initiative)

Power Electronics (PE) Interfaced Grid

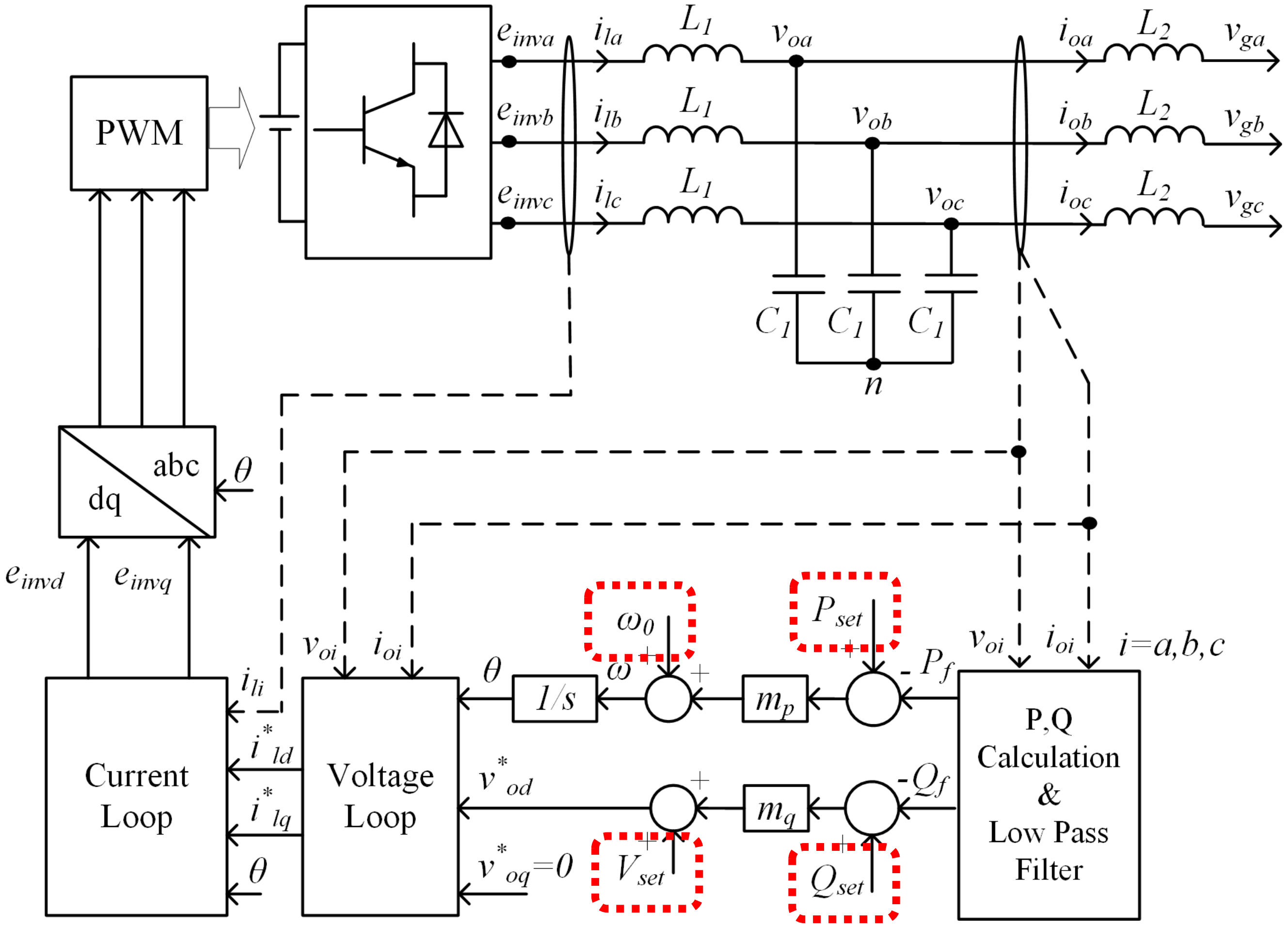
- Existing operational framework is insufficient to deal with the evolving challenges of extreme high (100%) power electronics (PE)-interfaced grid
  - Lower of inertia
  - Larger transients at fast (electromagnetic) timescales
  - Higher uncertainties in power generation
  - Reduced stability and safety margins



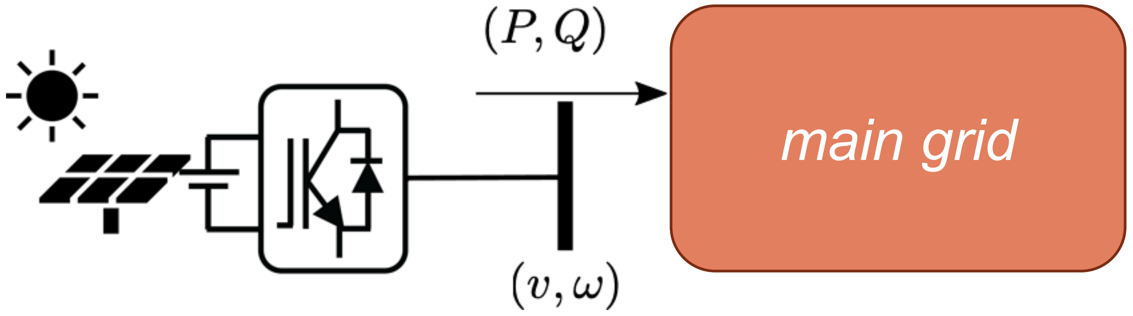
Source: EU MIGRATE Report

… need transformational change to achieve extreme high >75% PE penetration

Emerging Technologies: Grid-Forming Inverters



Multi-loop droop-control (P-ω, Q-V)

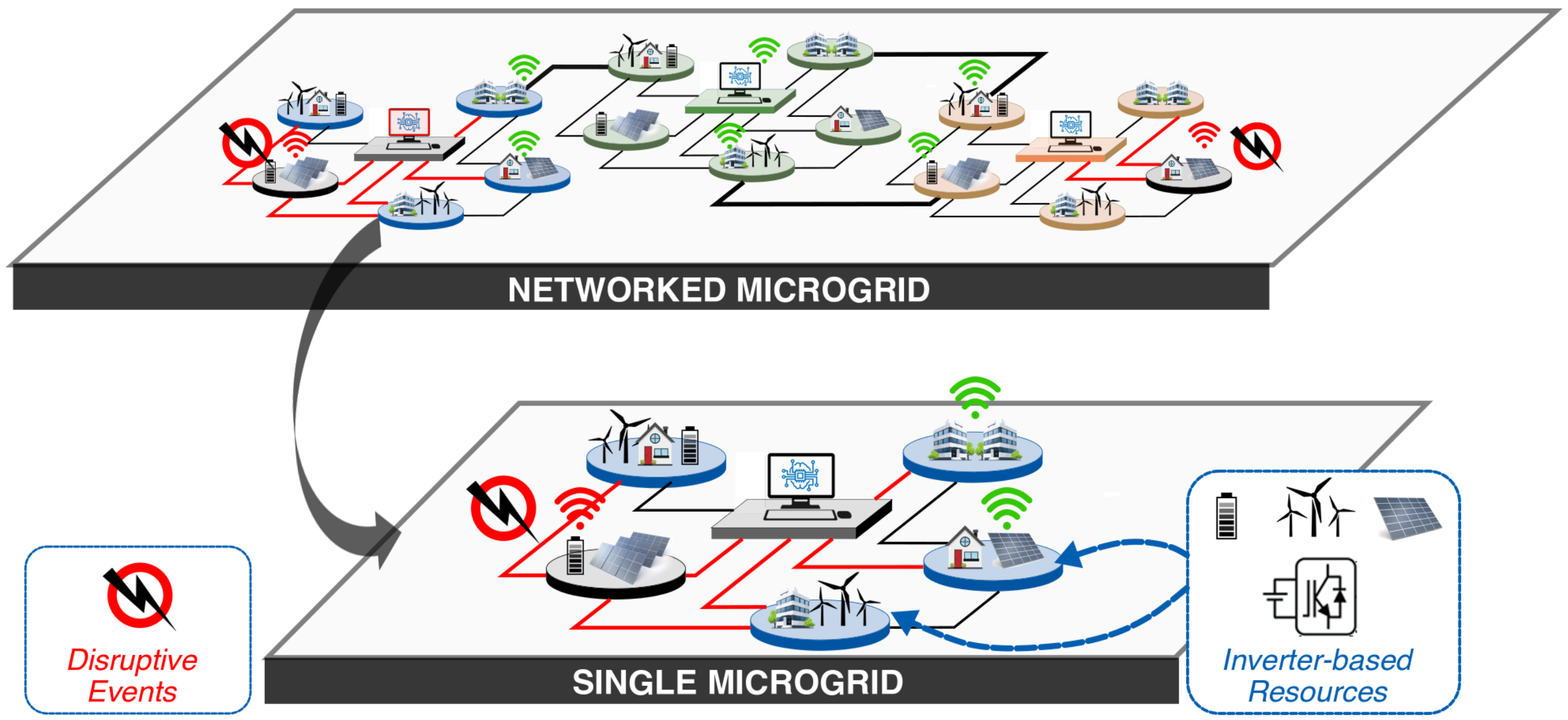


- Grid-forming inverters
  - Provides virtual inertia; acts as a voltage source; stable synchronization via inner control loops; black-start, and more …
- *Multi-loop droop-control* regulates voltage and frequency by controlling power (P,Q)

$$\omega_{\text{set}} = \omega^*_{\text{set}} - \lambda_p (P - P_{\text{set}}) \qquad \text{(P-}\omega\text{ droop)}$$

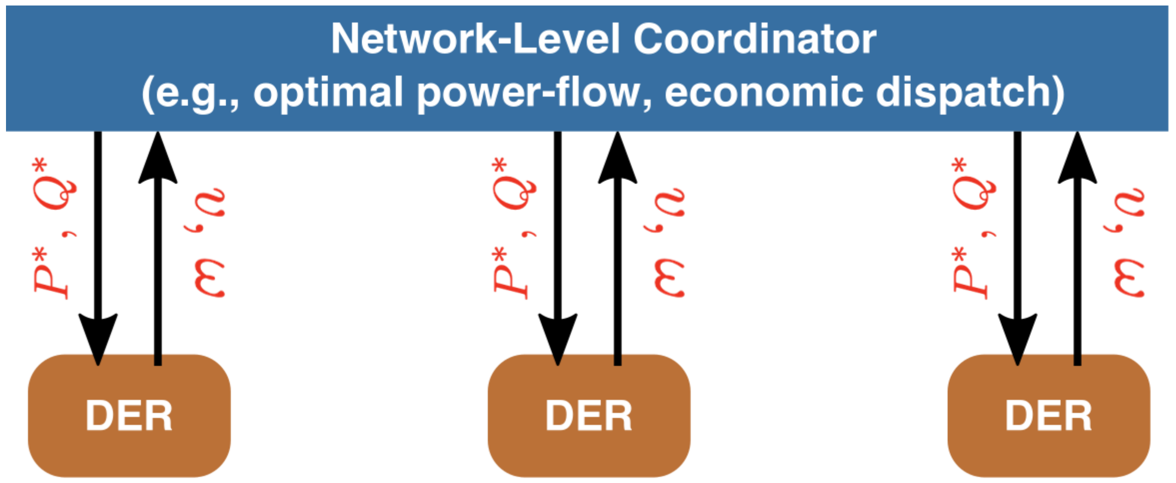
$$v_{\text{set}} = v^*_{\text{set}} - \lambda_q (Q - Q_{\text{set}}) \qquad \text{(Q-}V\text{ droop)}$$

Hierarchical and Distributed Framework



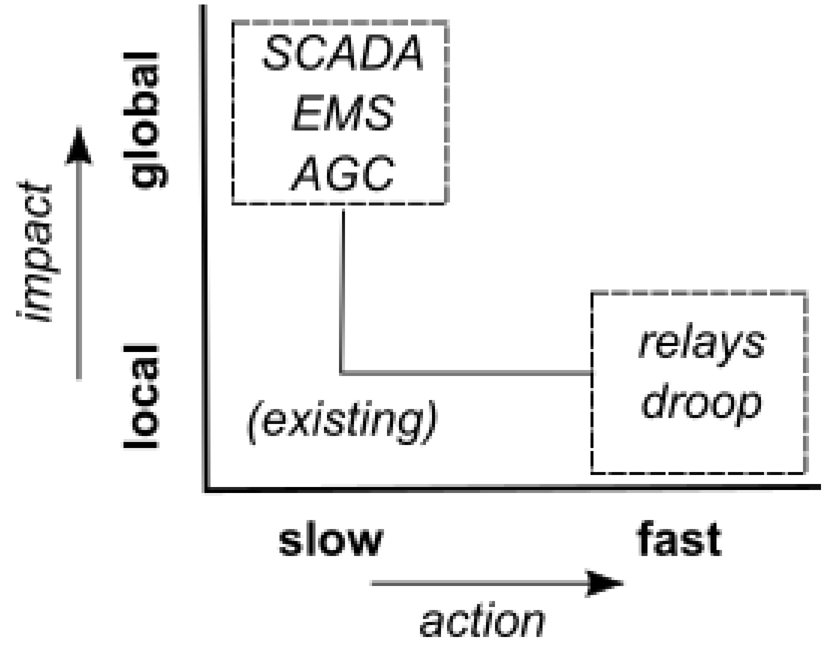
- Hierarchical and distributed operations to coordinate many distributed energy resources (DERs) over the network
- Individual resources (e.g., inverters) received control set-points to track

Example: Optimal Power-Flow
- DERs receive set-points; in turn regulates voltage and frequency

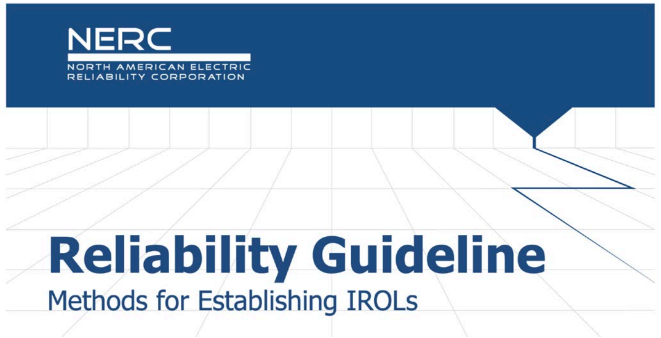


Controls Problem: Multi-timescales Resilience

State-of-the-art operational practices lack the spatiotemporal granularity required to proactively prevent transient safety and stability violations which are often local and fast-evolving in nature



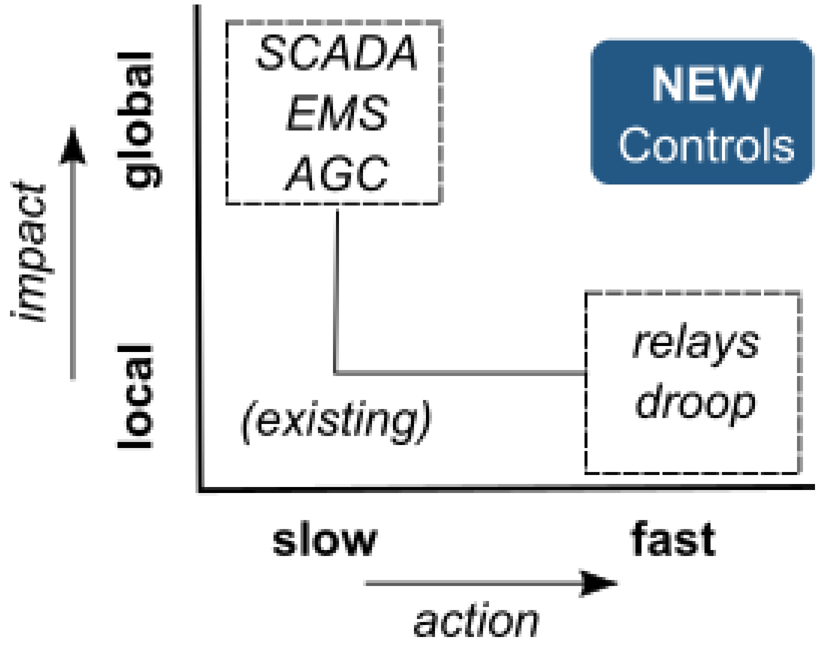
- Controls with global-impact are slow-acting
- Fast-acting controls have only local-impact, and *do not guarantee* safety



Long operating limits (voltage, frequency) violations trigger protective relays which could lead to system-wide blackout (WSCC 1996 blackout)

Controls Problem: Multi-timescales Resilience

State-of-the-art operational practices lack the spatiotemporal granularity required to proactively prevent transient safety and stability violations which are often local and fast-evolving in nature

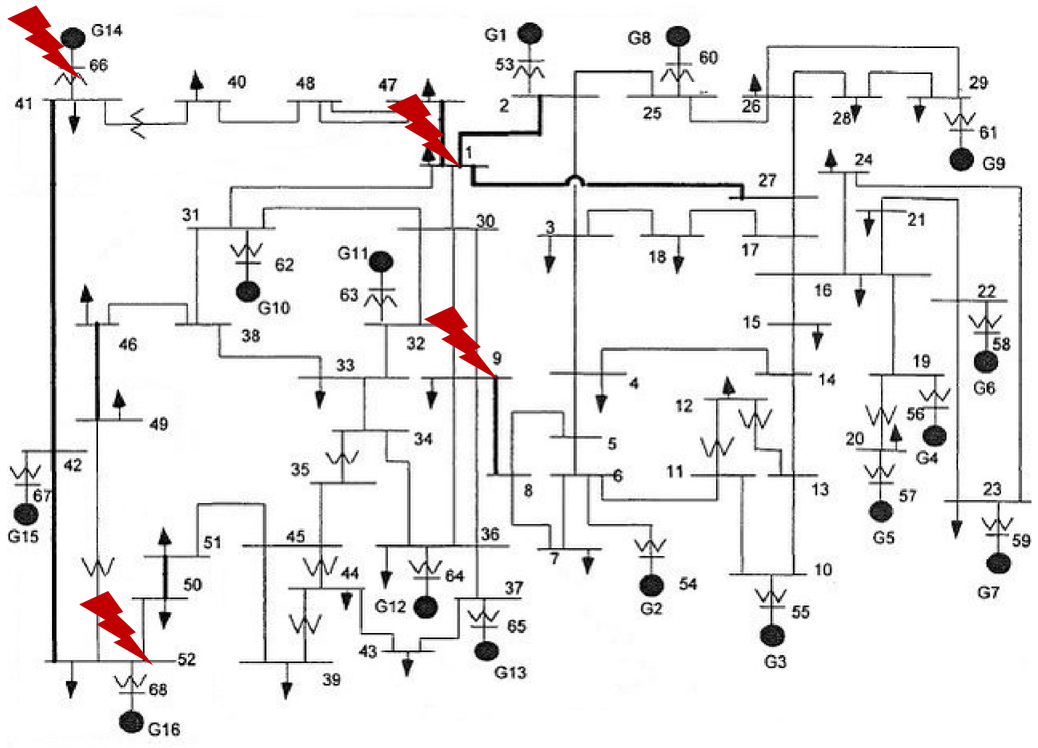


- Controls with global-impact are slow-acting
- Fast-acting controls have only local-impact, and *do not guarantee* safety

Need new controls that act fast and have system-level resilience impact

Sensors Problem: Identify Coordinated Attacks

In a distributed controls setting where local agents are acting based on sensor measurements, it is critical to identify coordinated attacks on sensors



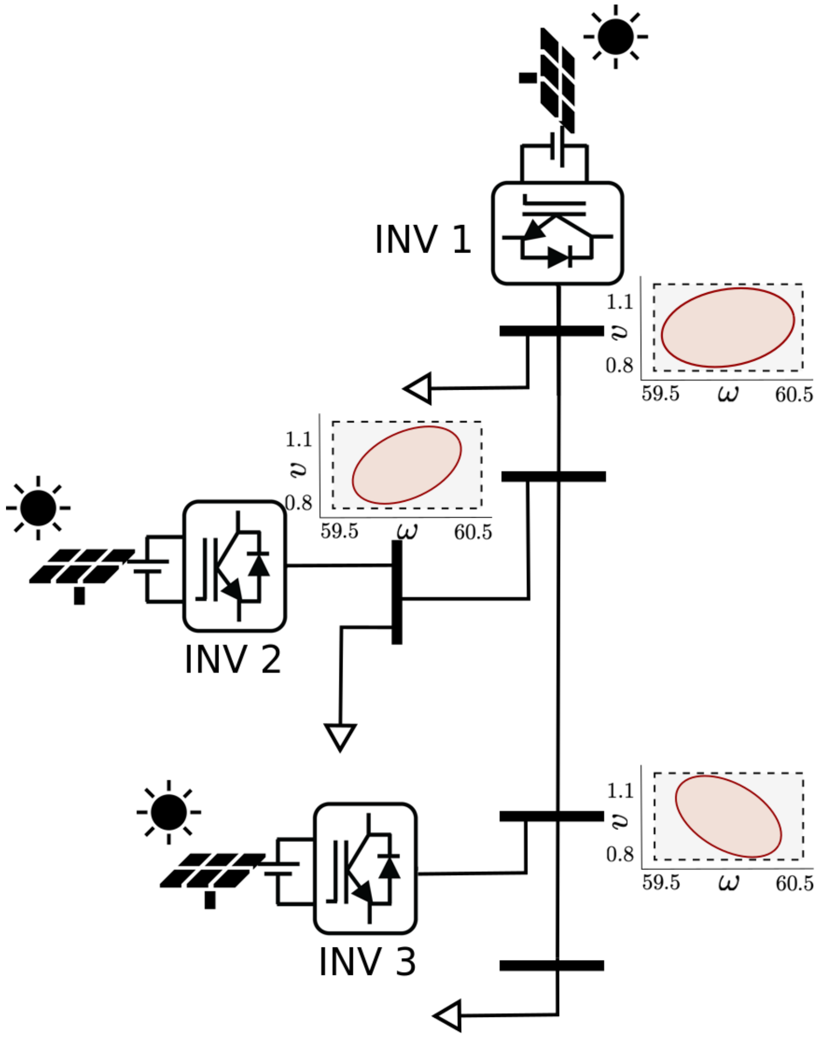
- Existing model-based (physical/statistical) are inaccurate during transients
- Machine learning methods typically require labelled data that are often unavailable

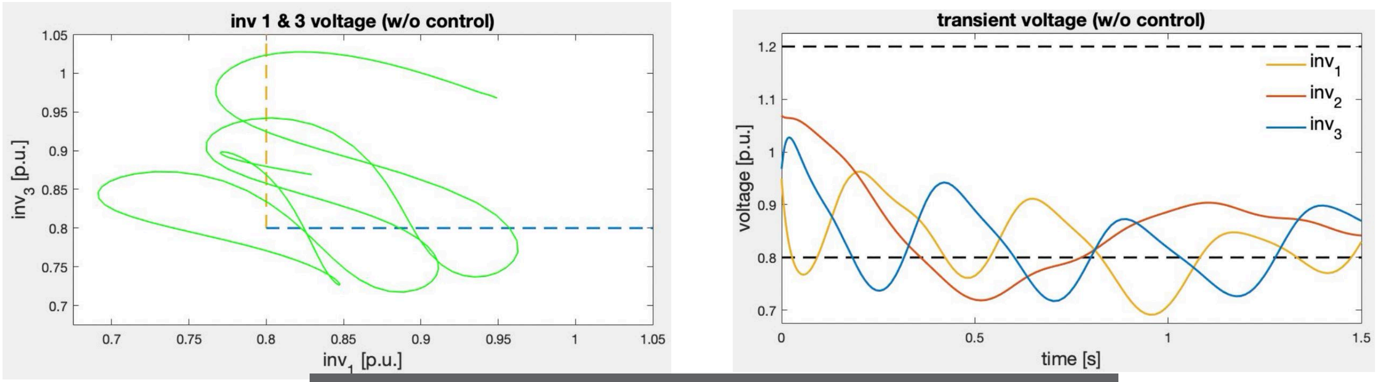
Need identification methods that are lightweight, and do not require prior knowledge and/or labelled data

- **Part 1: Distributed Transient Safety Verification**

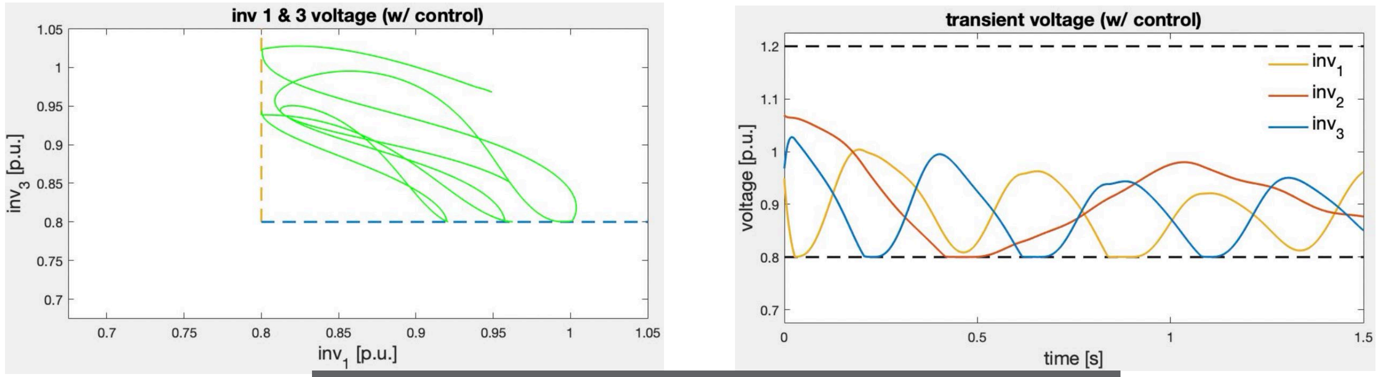
- **Part 2: Koopman-Based Online Attack Identification**

Local Transient Safety Constraints





unsafe excursions in voltages

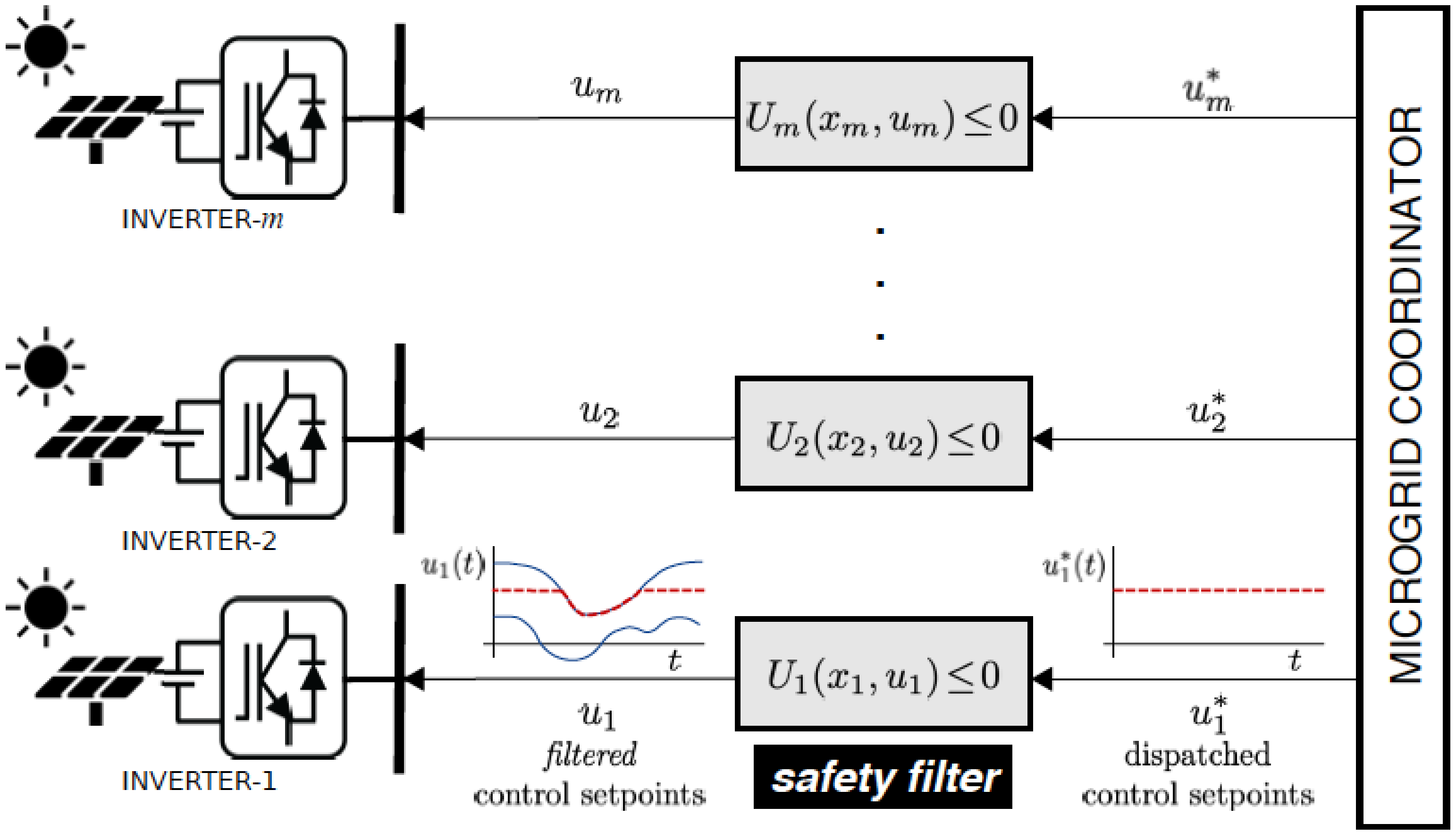


desired transient safe control

Local disturbances (e.g., solar fluctuations) cause unsafe excursions in voltages

Safety Filter: The Concept

Decouple network-level objectives from local transient safety constraints



- Safety filters are deployed locally at the inverter terminals, and act as gatekeepers for allowable (safe) set-points
  - *Bounds on the allowable control set-points*
- In a robust design, guarantees transient safety constraint satisfaction under bounded uncertainties in the network

Kundu and Kalsi, "Transient Safety Filter Design for Grid-Forming Inverters," ACC 2020.

Distributed Transient Safety Problem

$$\dot{\theta}_i = \omega_i$$
$$\tau_i \dot{\omega}_i = -\omega_i + \lambda_i^p \left(P_i^0 + u_i^p - P_i\right)$$
$$\tau_i \dot{v}_i = v_i^0 - v_i + \lambda_i^q \left(Q_i^0 + u_i^q - Q_i\right)$$

Local (Inverter) Dynamics

$$P_i = v_i \sum_{k \in \mathcal{N}_i} v_k (G_{i,k} \cos\theta_{k,i} - B_{i,k} \sin\theta_{k,i})$$
$$Q_i = -v_i \sum_{k \in \mathcal{N}_i} v_k (G_{i,k} \sin\theta_{k,i} + B_{i,k} \cos\theta_{k,i})$$

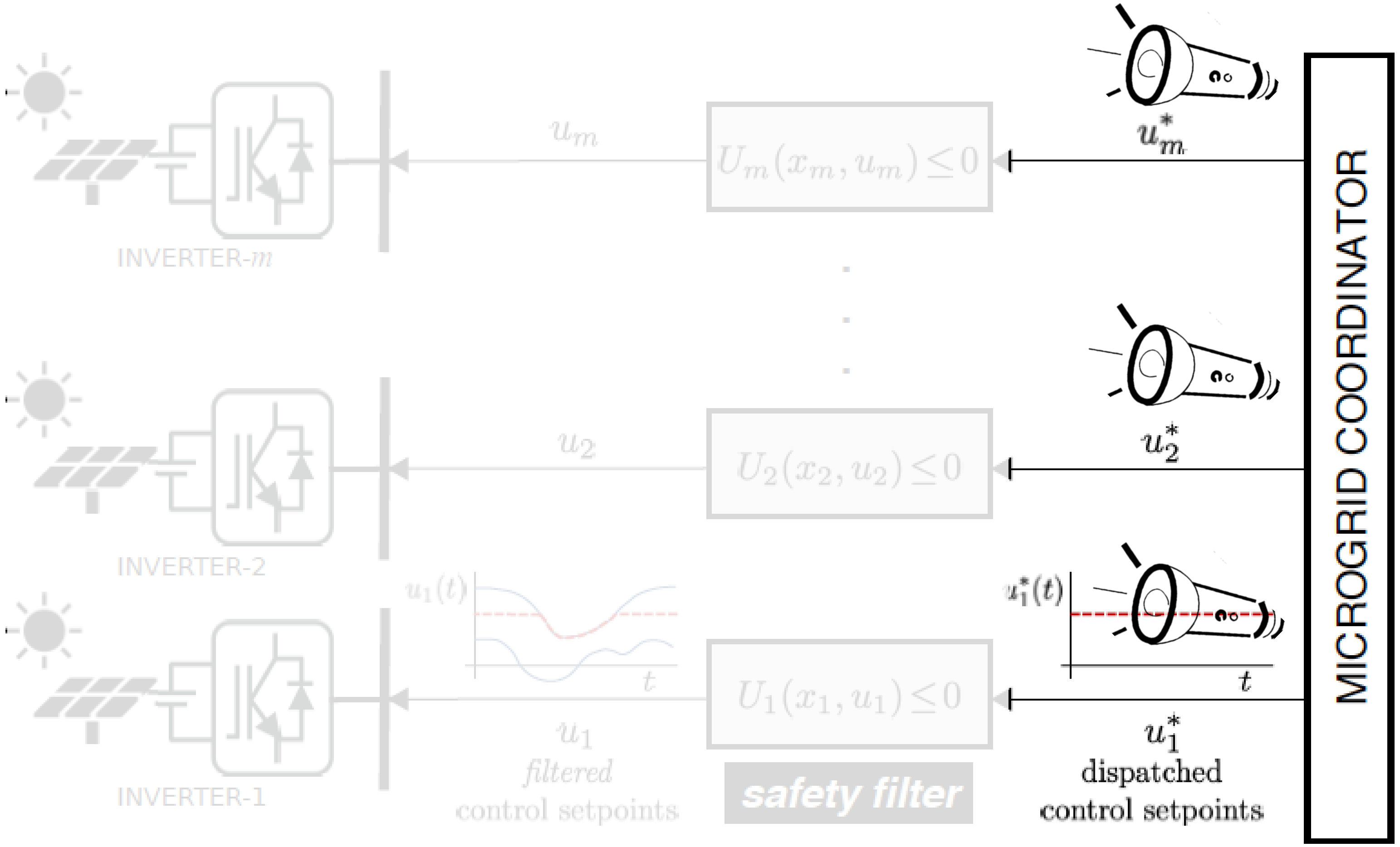
Network Interactions (Power-Flow)

Objective (Transient Safety): $\underline{v_i} \leq v_i(t) \leq \overline{v_i}\,, \quad \underline{\omega_i} \leq \omega_i(t) \leq \overline{\omega_i}$

Control Set-points: $u_i^p,\, u_i^q$

Goal: Identify the set of control set-points that robustly satisfy transient safety under disturbances in the network

Distributed Safety: System Perspective, Proactive



Objective (Safety): $\underline{v_i} \leq v_i(t) \leq \overline{v_i}$,

$\underline{\omega_i} \leq \omega_i(t) \leq \overline{\omega_i}$

Control Set-points: u_i^p , u_i^q

- ***Inaccessible local information***
- ***State-independent control bounds***

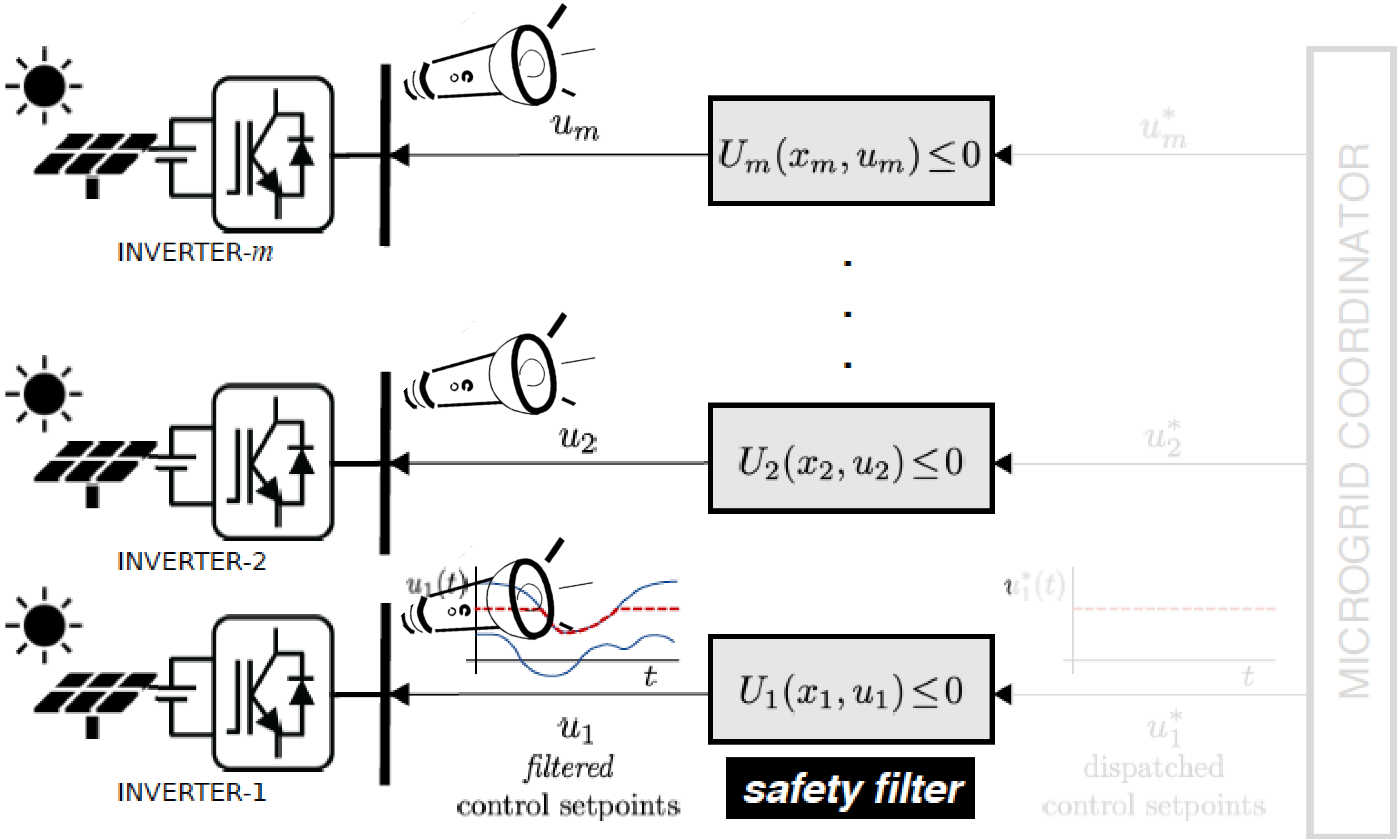
$$\mathcal{U}_i = \{u \mid \underline{u}_i \leq u_i \leq \overline{u}_i\}$$

- ***Known system-wide set-points:***

$$u_i \ \forall i$$

Goal: Identify the set of control set-points that robustly satisfy transient safety under disturbances in the network

Distributed Safety: Local Perspective, Reactive



Objective (Safety): $\underline{v_i} \leq v_i(t) \leq \overline{v_i}$, $\underline{\omega_i} \leq \omega_i(t) \leq \overline{\omega_i}$

Control Set-points: u_i^p, u_i^q

- ***Accessible local information***

$$\theta_i, \omega_i, v_i, \lambda_i^p, \lambda_i^q$$

- ***State-inclusive control bounds***

$$\mathcal{U}_i(x_i) := \{u \mid U_i(x_i, u) \leq 0\}$$

- ***Unknown bounded interactions:*** P_i, Q_i

Goal: Identify the set of control set-points that robustly satisfy transient safety under disturbances in the network

Preliminaries

- Set Invariance
- Control Barrier Functions
- Sum-of-Squares Optimization

Safety vs. Stability

$$\dot{x} = f(x), \quad f(0) = 0$$ (Dynamical System)

Safety: Barrier Certificates

- Constraints on states

$$\begin{aligned} B(x) &\geq 0, & x &\in \mathcal{C}_{\text{safe}} \\ B(x) &< 0, & x &\notin \mathcal{C}_{\text{safe}} \\ \dot{B}(x) &\geq 0, & x &\in \partial\mathcal{C}_{\text{safe}} \end{aligned}$$

Stability: Lyapunov Certificates

- Convergences of states

$$\begin{aligned} V(x) &\geq \varepsilon_1 \|x\|_2^2, & x &\in \mathcal{N}(0) \\ \dot{V}(x) &\leq -\varepsilon_2 \|x\|_2^2, & x &\in \mathcal{N}(0) \end{aligned}$$

… finding these functions for generic nonlinear systems is not always trivial

Polynomial Systems: Sum-of-Squares

- Sum of squared polynomials: $s(x) \in \Sigma[x] \iff s(x) = \sum_{i=1}^{m} s_i(x)^2$
  - Gramm matrix representation and equivalence with SDPs:

$$s(x) = z(x)^T \, Q \, z(x)\,, \quad s(x) \in \Sigma[x] \iff Q \succeq 0$$

  - **(Putinar's) Positivstellensatz: deal with semi-algebraic conditions!!**

$$p(x) > 0 \text{ on } \{x | \, g_1(x) \geq 0, \ldots, g_n(x) \geq 0\}$$

$$\iff \exists \sigma_i \in \Sigma[x] \text{ so that } p - \sum_{i=1}^{n} \sigma_i \, g_i \in \Sigma[x]$$

✓ MATLAB tools (example): SOSTOOLS, SeDuMi.

Constructive method for Lyapunov and barrier functions – if polynomial!

- M. Putinar, "Positive polynomials on compact semi-algebraic sets," 1993.
- A. Papachristodoulou, et al, "SOSTOOLS: Sum of squares optimization toolbox for MATLAB," 2013.
- J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," 1999.

Power-Flows have Non-Polynomial Terms …

- Power system dynamics are *non-polynomial ODEs*
  - … because of trigonometric terms (sine, cosine) in power-flow

$$P_{e,i}(\delta) = \sum_j E_i E_j \left(G_{ij} \cos(\delta_i - \delta_j) + B_{ij} \sin(\delta_i - \delta_j) \right)$$

- Lift the state-space to convert into polynomial representation

$$\text{Recasting: } (\delta_k \,,\, \dot{\delta}_k) \;\mapsto\; (x_{k,1} \,,\, x_{k,2} \,,\, x_{k,3})$$

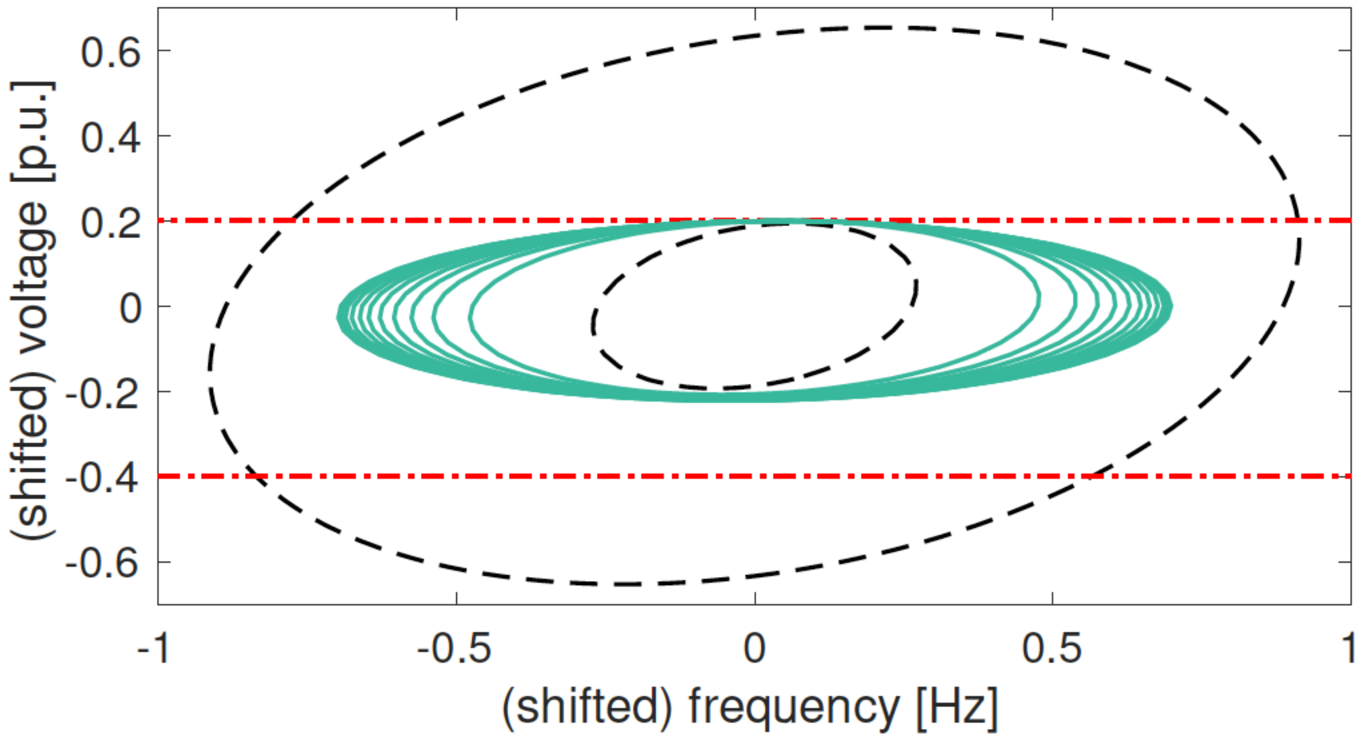
$$x_{k,1} = \sin \delta_k \,,\;\; x_{k,2} = (1 - \cos \delta_k) \,,\;\; x_{k,3} = \dot{\delta}_k$$

$$\text{with, } 0 = x_{k,1}^2 + x_{k,2}^2 - 2\, x_{k,2} \quad \text{[algebraic constraints]}$$

Obtain set of polynomial DAEs from non-polynomial ODEs

Iterative Lyapunov & Barrier Function Computation

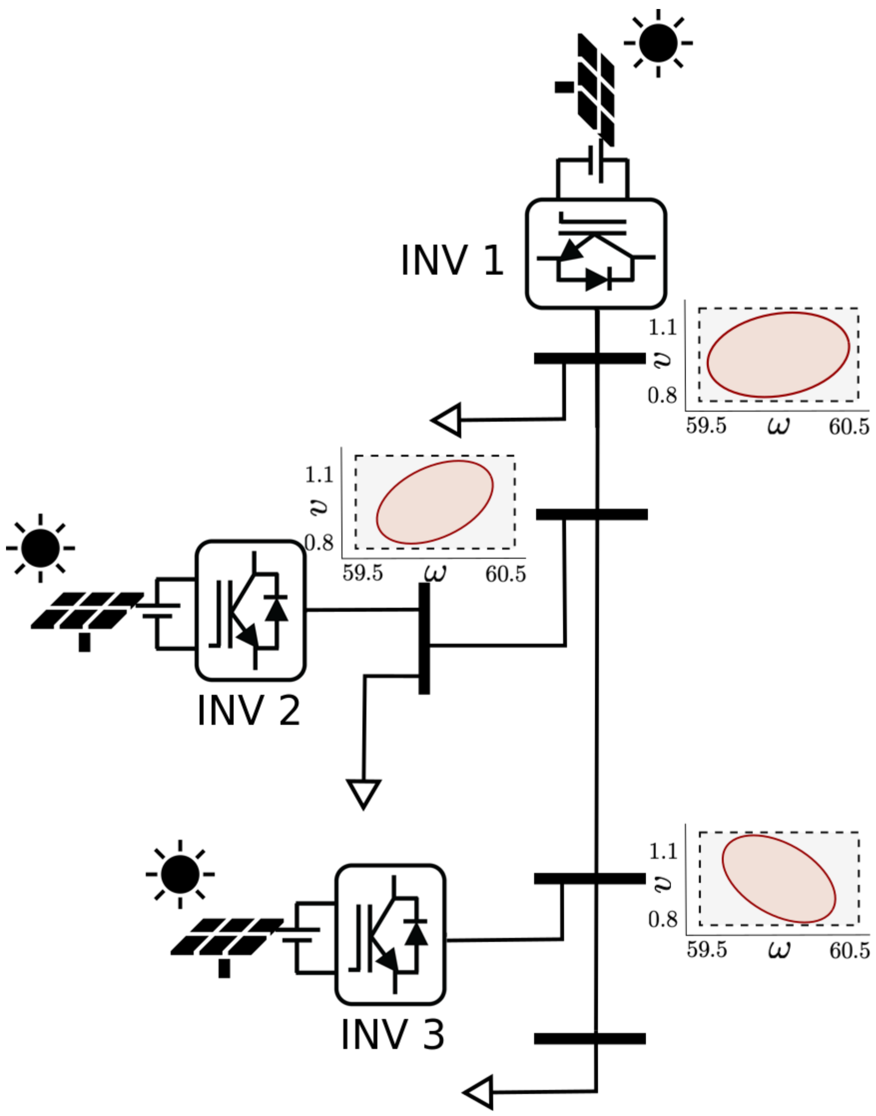
- Efficient iterative algorithms exist to compute the barrier and Lyapunov functions
- Brief outline: warm-start Barrier Computation with Lyapunov Level-sets*



Safety-constrained set as a subset of the region of attraction

Wang, Han, and Egerstedt, "Permissive barrier certificates for safe stabilization using sum-of-squares," ACC 2018.
Kundu, Geng, Nandanoori, Hiskens and Kalsi, "Distributed Barrier Certificates for Safe Operation of Inverter-Based Microgrids", ACC 2019.

Local Nominal Safety Control Policy



- Microgrid as an interconnected polynomial system:

$$\boxed{\dot{x}_i = f_i(x_i) + g_i(x_i)u_i} + \boxed{\sum_{j\in\mathcal{N}_i} h_{ij}(x_i, x_j)}$$

(isolated dynamics) (interactions)

- Robust Safety: (define a safe neighborhood) $\mathcal{N}_i(0)$

$$\implies \mathcal{N}_1(0) \times \mathcal{N}_2(0) \times \cdots \times \mathcal{N}_n(0) \subset \mathcal{C}_{\text{safe}}$$

(construct distributed barrier functions)

$B_i(x_i) \geq c_i$ on $\mathcal{N}_i(0)$, for some $c_i > 0$

(design feedback policies) u_i

$$\nabla B_i(f_i + g_i u_i + \sum_j h_{ij}) \geq 0 \text{ on } x_i \in \partial\mathcal{N}_i(0),\ x_j \in \mathcal{N}_i(0)$$

Kundu, Geng, Nandanoori, Hiskens and Kalsi, “Distributed Barrier Certificates for Safe Operation of Inverter-Based Microgrids”, ACC 2019.

A Family of Safety Control Policies

- For any nominal control policy u_i^*, the following family of state-feedback controls guarantee robust transient safety under bounded disturbances

$$U_i(x_i, u) = ((u_i^*(x_i) - u) \odot (u_i^* + \beta^{\max} g_i^T \nabla B_i - u)$$

$$\mathcal{U}_i(x_i) := \{u \mid U_i(x_i, u) \leq 0\}$$

We have a family of local control policies, instead of just one, that ensure robust safety guarantees

Challenge: the set has vanishing cardinality around origin (x=0)

Kundu and Kalsi, "Transient Safety Filter Design for Grid-Forming Inverters," ACC 2020.

A Family of Safety Control Policies (Contd.)

- For any nominal control policy u_i^* , the following family of state-feedback controls guarantee robust transient safety under bounded disturbances

$$U_i(x_i, u) = ((u_i^*(x_i) - u) \odot (u_i^* + \beta^{\max} g_i^T \nabla B_i - u)$$

$$\mathcal{U}_i(x_i) := \{u \mid U_i(x_i, u) \leq 0\}$$

- Expand the allowable safety control set by introducing a relaxation term

$$\mathcal{U}_i(x_i) := \left\{ u \,\middle|\, U_i(x_i, u) \leq \gamma \log \left(\frac{1 - c_i}{1 - B_i(x_i)} \right) \right\}$$

  - ***The relaxation term is >0 near origin, but approaches 0 at the safety set boundary***

Kundu and Kalsi, "Transient Safety Filter Design for Grid-Forming Inverters," ACC 2020.

Main Result: A Family of Safety Control Policies

- Summary: Under mild conditions on the distributed barrier functions[1], there exist a family of state-feedback control policies, with non-vanishing cardinality that ensure robust safety guarantees.
- In other words, any control input of the following form is *robustly safe:*

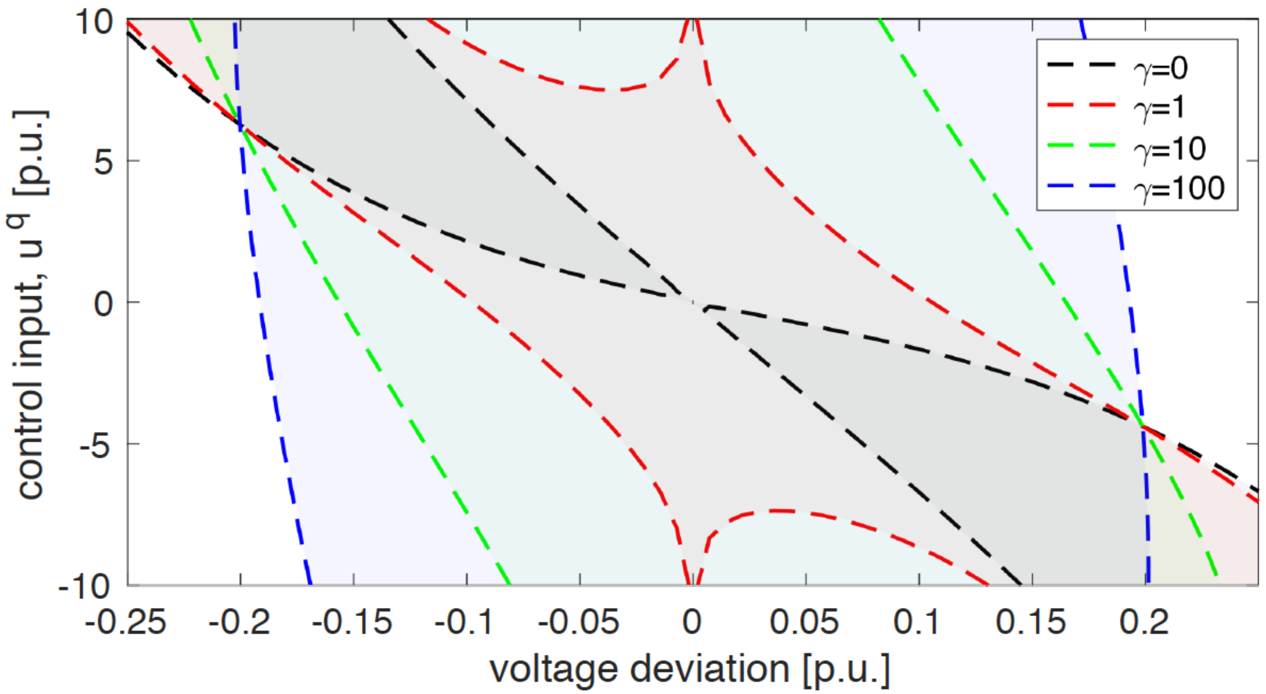
$$u_i(t) \in \left\{ r\, u_i^{\alpha}(x_i(t)) + (1-r)\, u_i^{\theta}(x_i(t)) \,\middle|\, r \in [0,1] \right\}$$

where the existence of these two safe control policies are guaranteed:

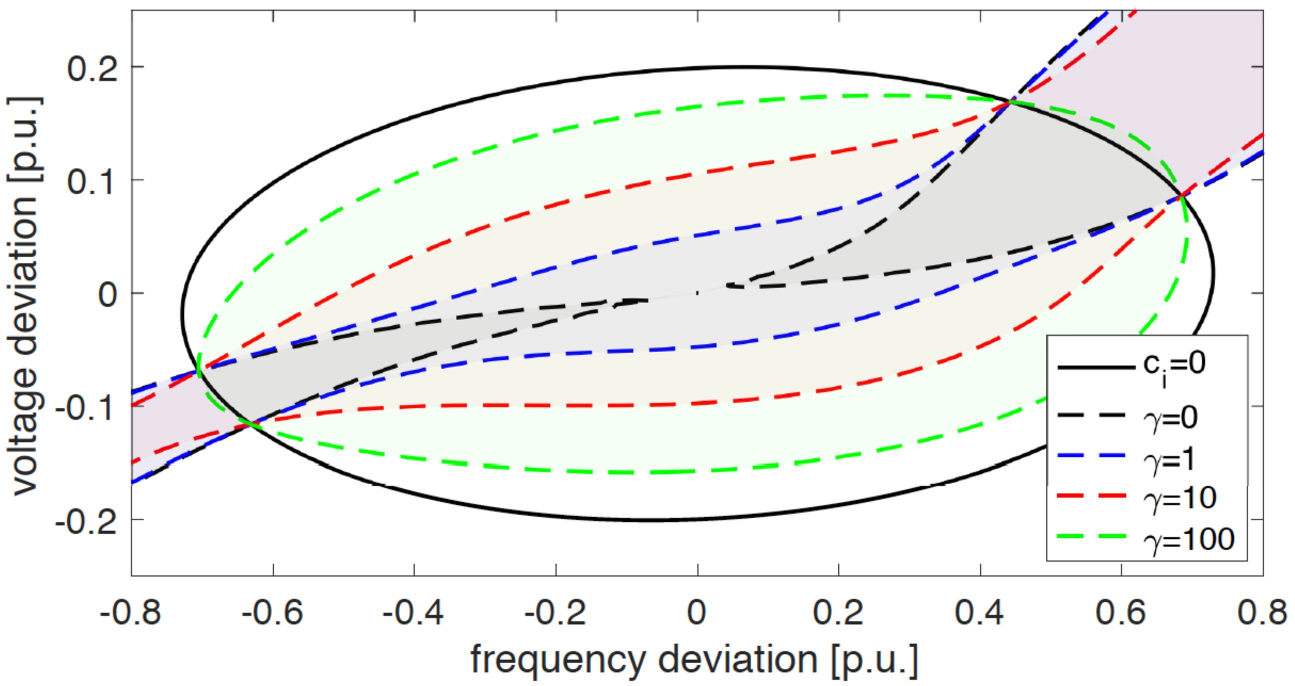
$$u_i^{\alpha}(x_i) < u_i^{\theta}(x_i)$$

Kundu and Kalsi, "Transient Safety Filter Design for Grid-Forming Inverters," ACC 2020.

Visualization of Allowable Safe Control Set



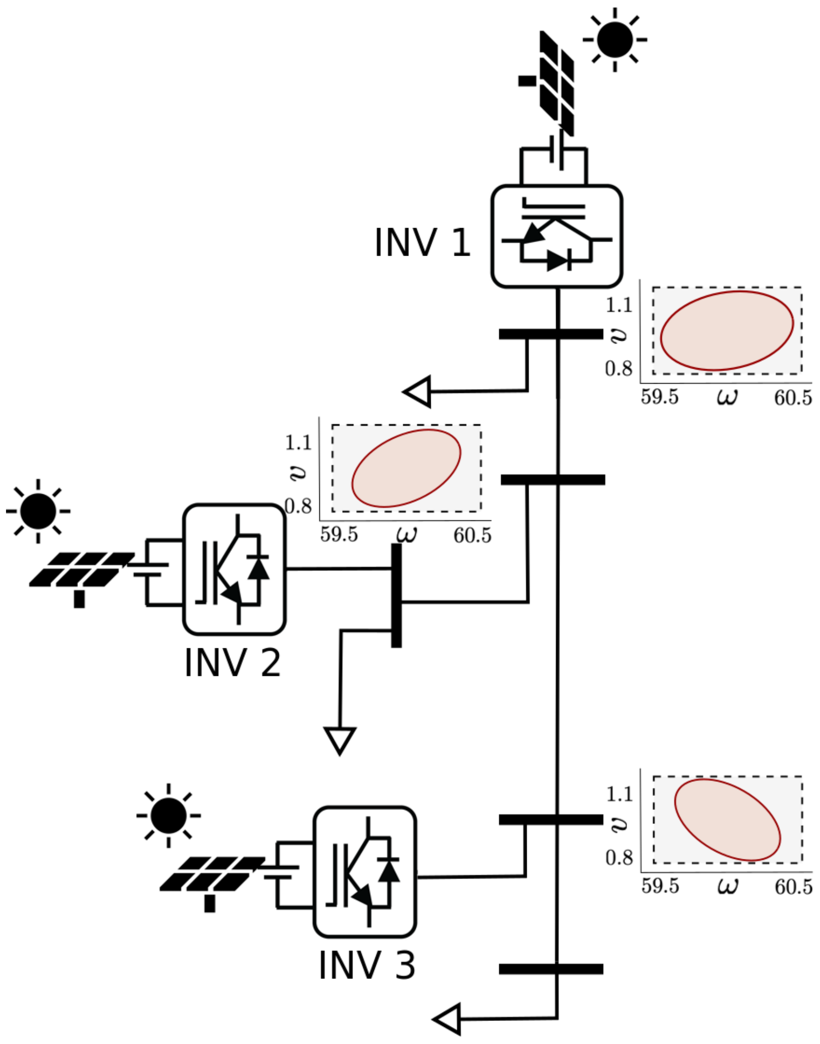
Safe values of reactive power control input, as a function of the voltage deviation for various values of the relaxation coefficient



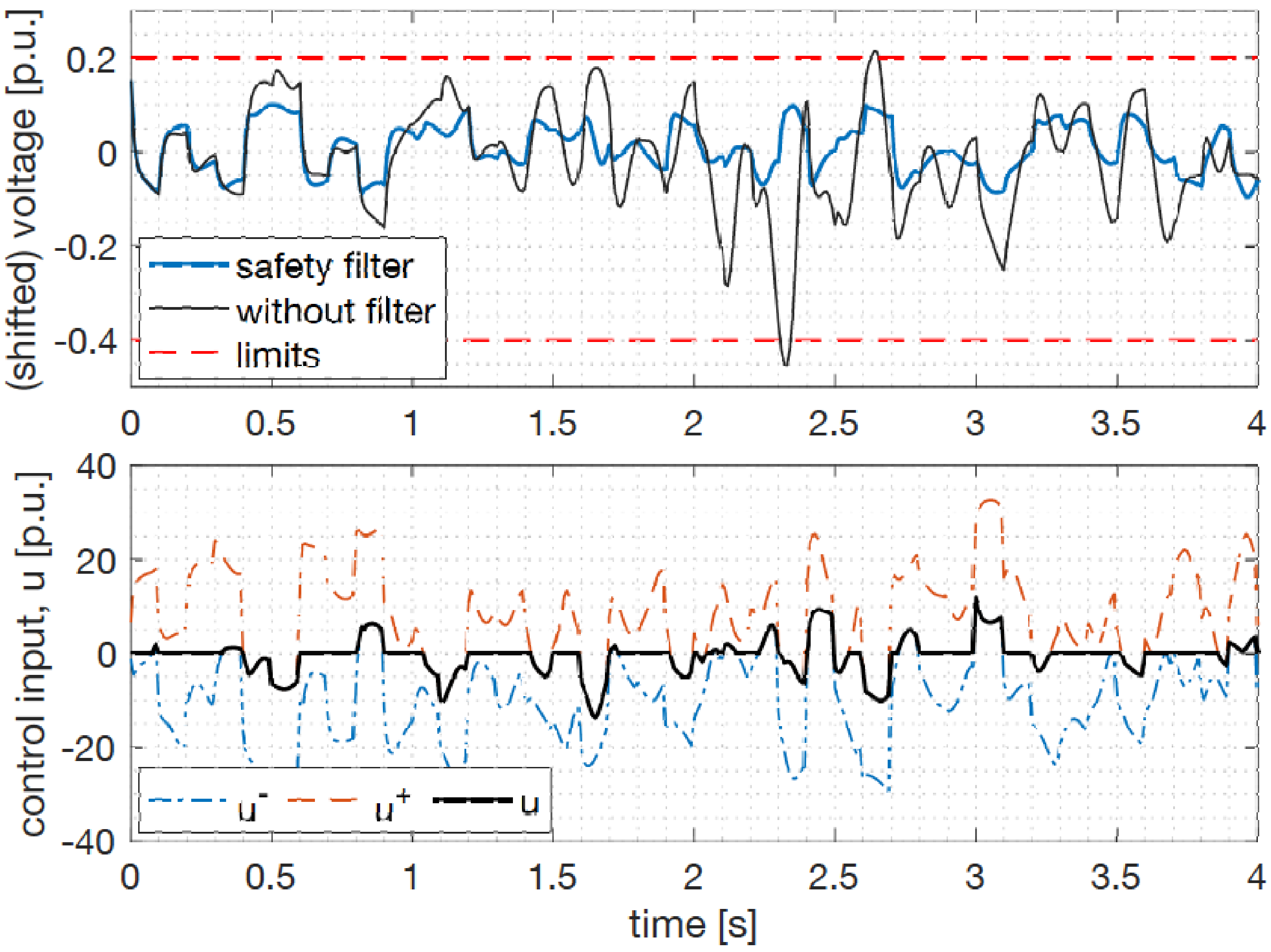
Sets of values on the state-space over which a control set-point $u = 0$ is deemed to be safe, for varying relaxation coefficient γ

Higher values of (design parameter) γ ensures larger allowable safe set

Numerical Example

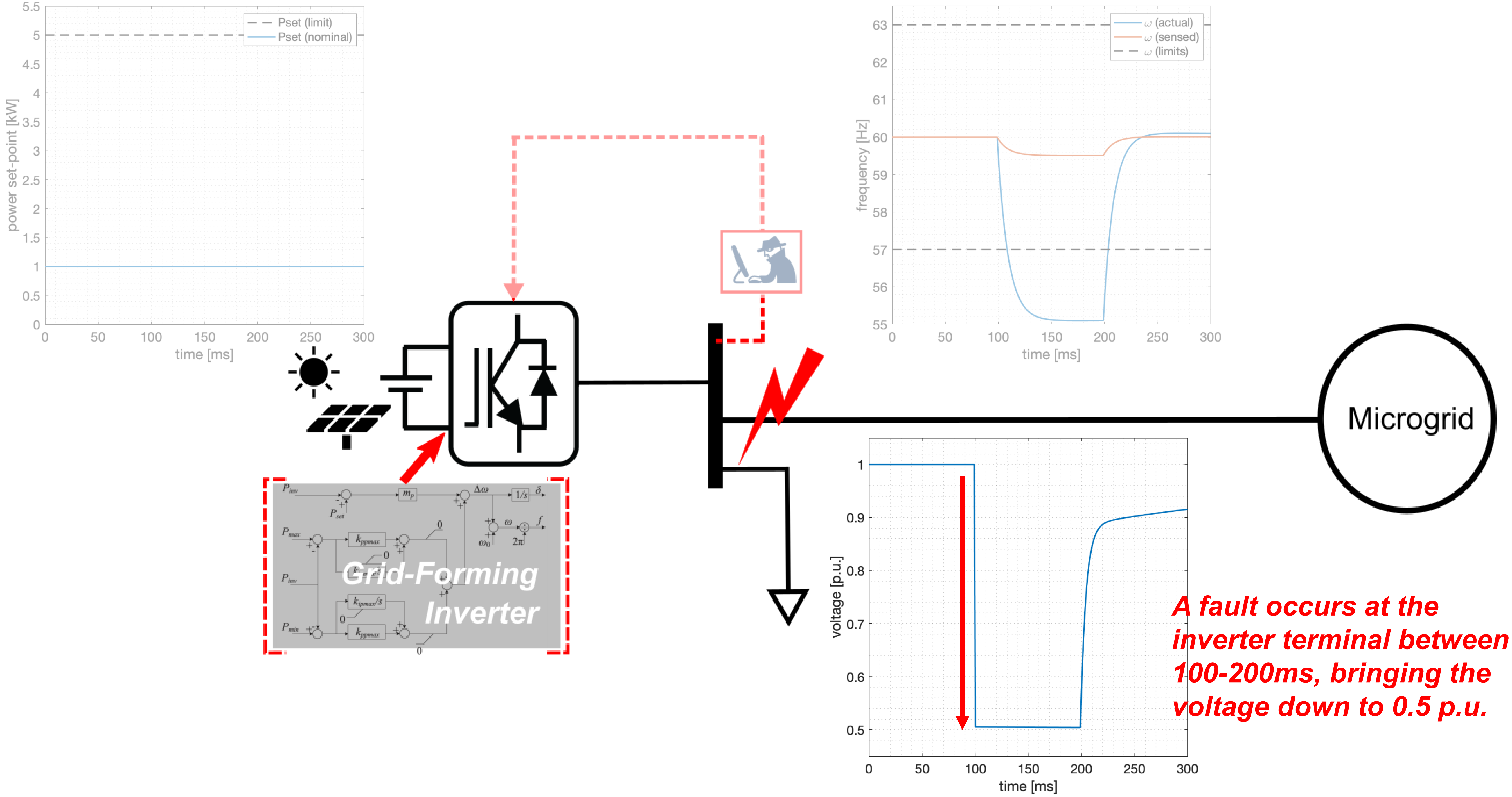


CERTS Microgrid



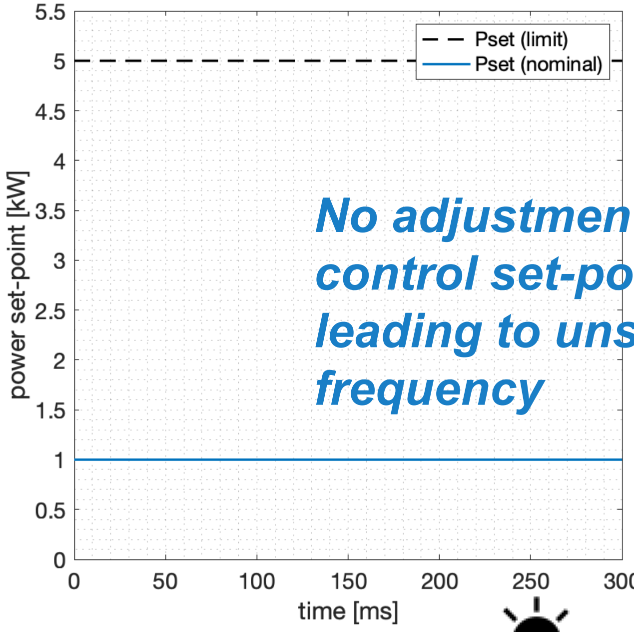
An inverter terminal voltage violates the safety limits in absence of safety filters, but not in presence of it. The filtered reactive power control input and its allowable range, with the centrally dispatched setpoint at $u = 0$.

Numerical Example: Cyber-Physical Resilience

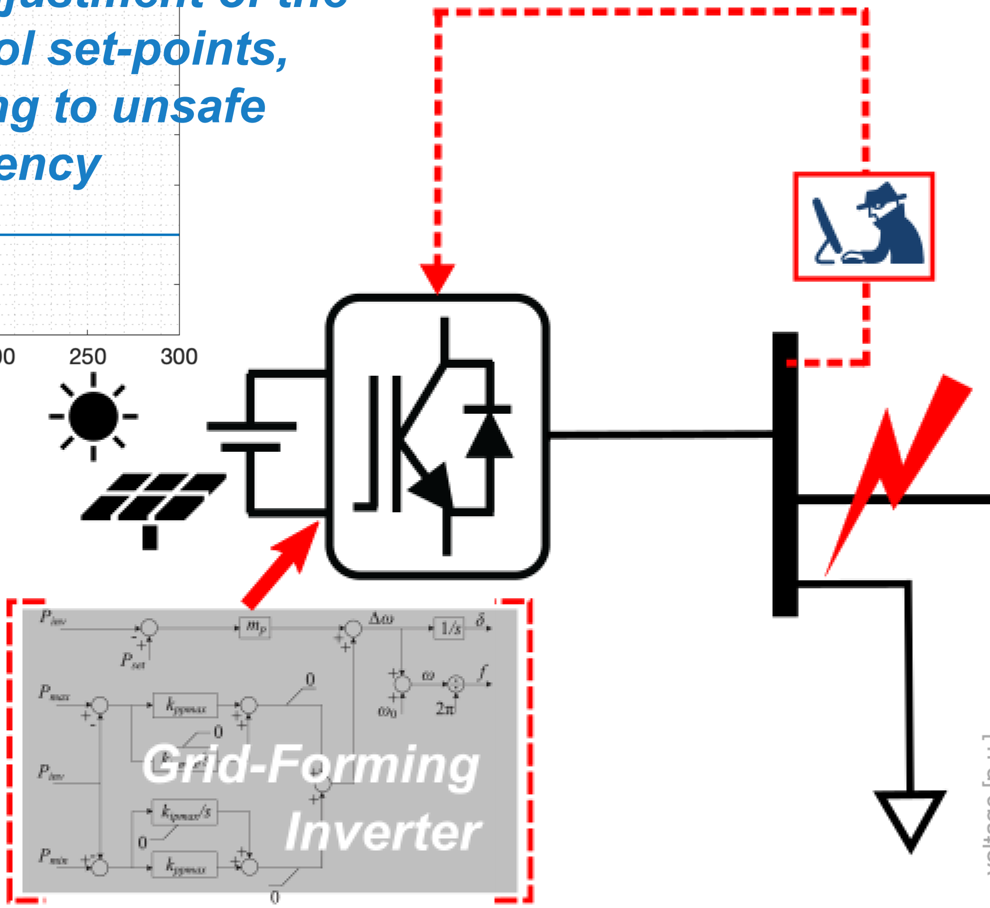


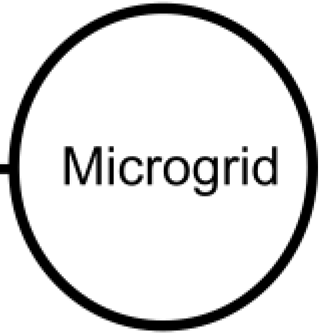
A fault occurs at the inverter terminal between 100-200ms, bringing the voltage down to 0.5 p.u.

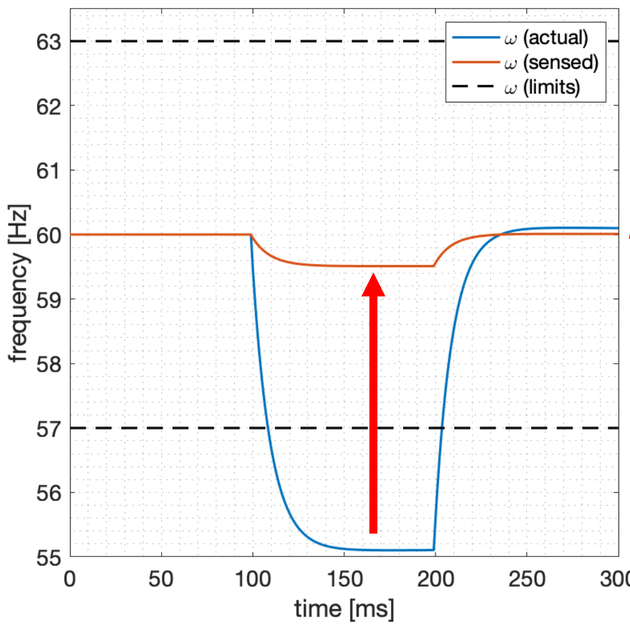
Numerical Example: Cyber-Physical Resilience



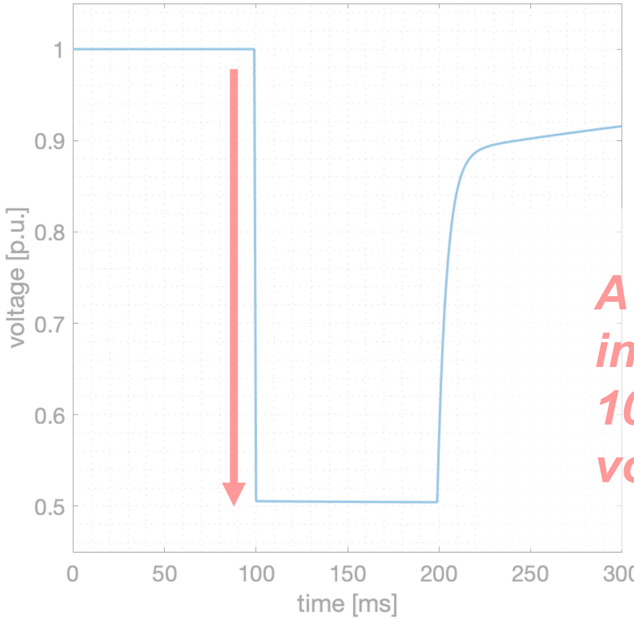
No adjustment of the control set-points, leading to unsafe frequency





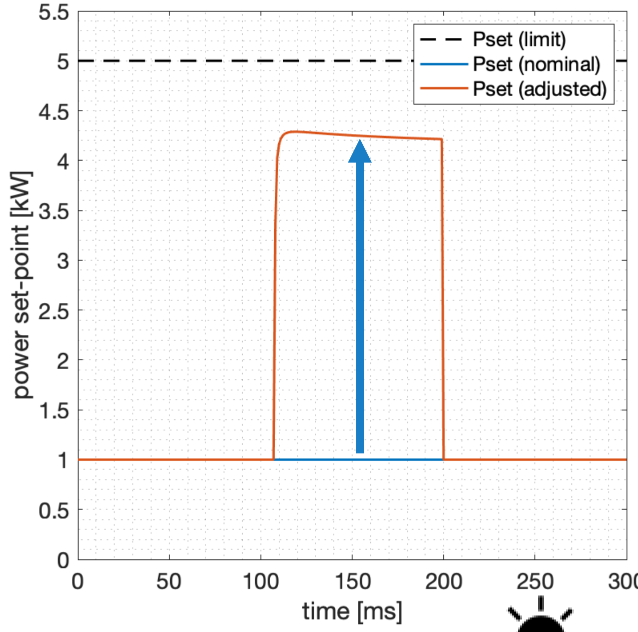


Concurrently, an attacker performs a "masking attack" to hide from the controller the unsafe frequency deviation

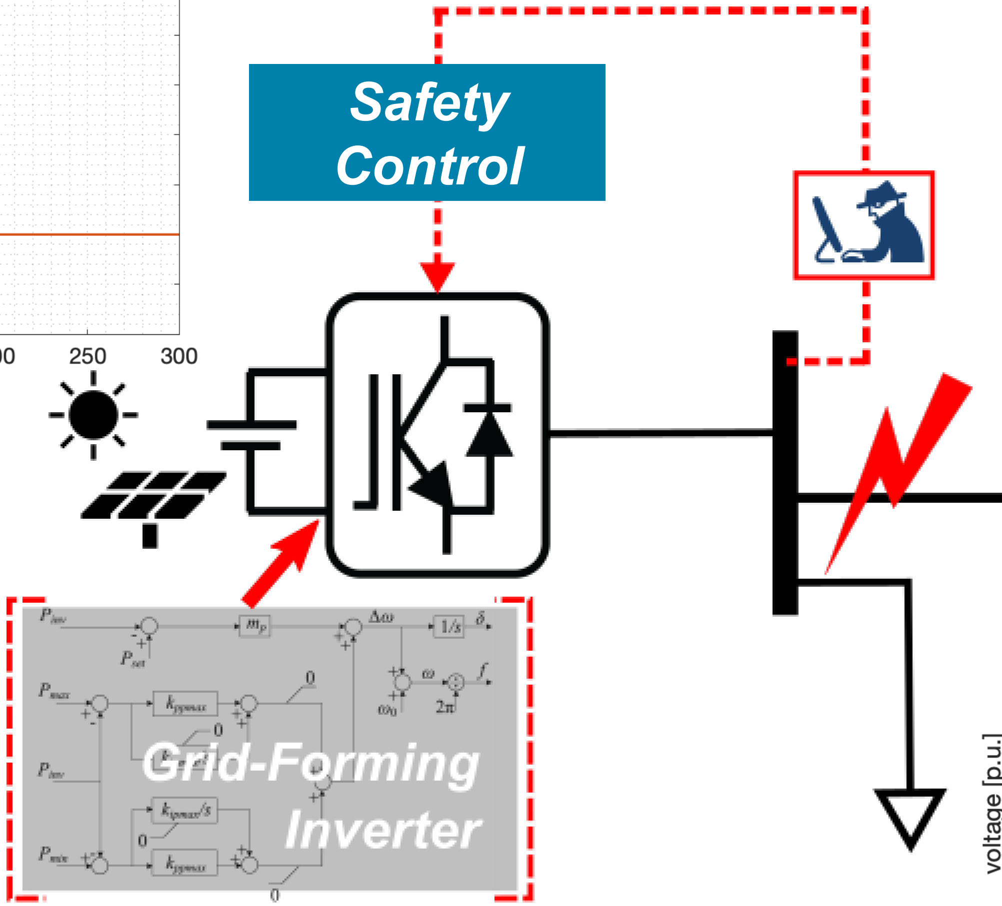


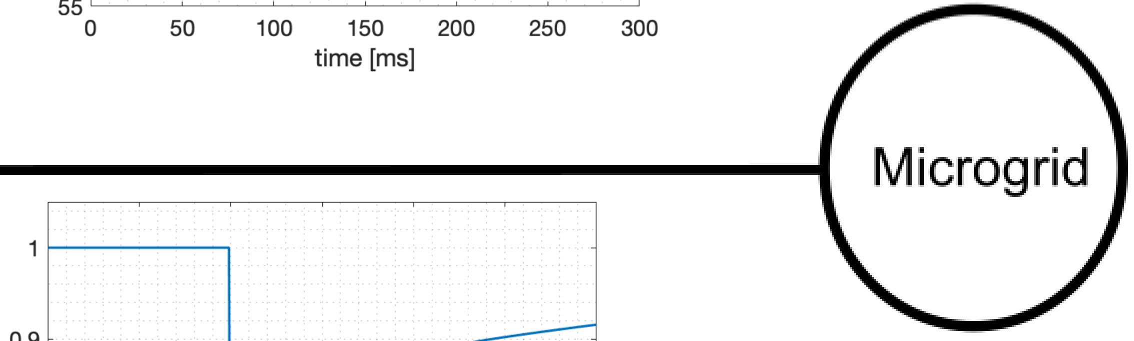
A fault occurs at the inverter terminal between 100-200ms, bringing the voltage down to 0.5 p.u.

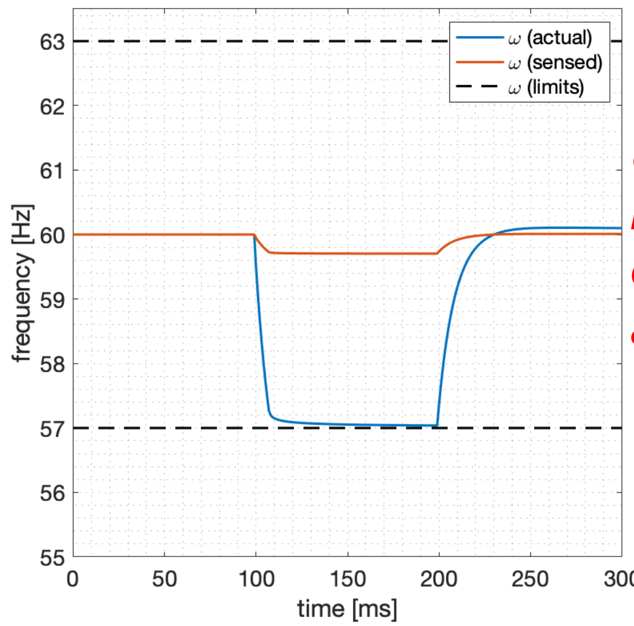
Numerical Example: Cyber-Physical Resilience



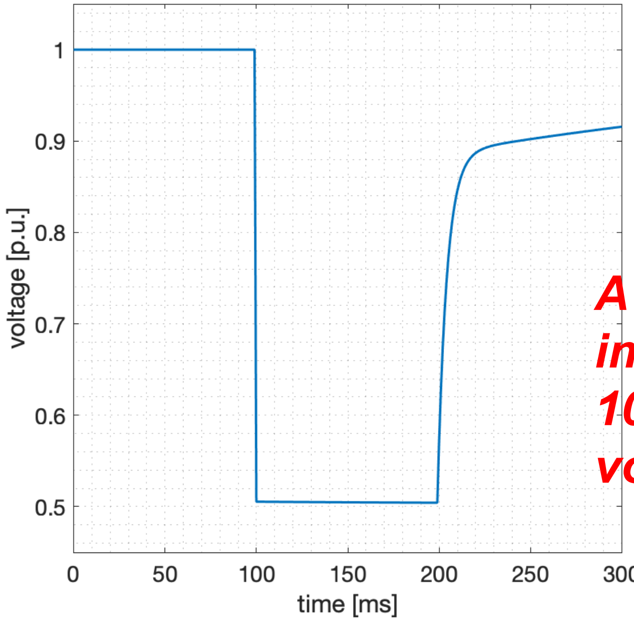
Control adjusts the set-points locally, to bring frequency back to safety, even under attack







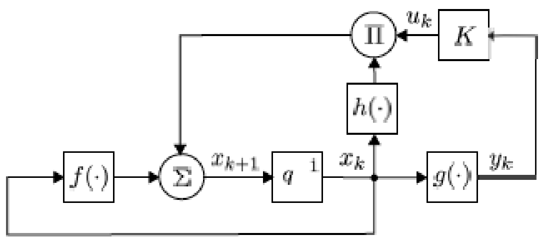
Under controls, frequency is brought back to safety, even though the masking attack is still in place



A fault occurs at the inverter terminal between 100-200ms, bringing the voltage down to 0.5 p.u.

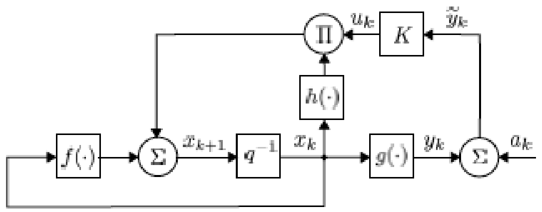
- Part 1: Distributed Transient Safety Verification
- **Part 2: Koopman-Based Online Attack Identification**

Attacks in Cyber-Physical Systems



Closed-loop system under normal operating conditions

$$x_{k+1} = f(x_k) + h(x_k)\,u_k$$
$$y_k = g(x_k)$$



Closed-loop system under attack

$$x_{k+1} = f_c(x_k) + h_c(x_k)\,a_k$$
$$\tilde{y}_k = g(x_k) + a_k$$

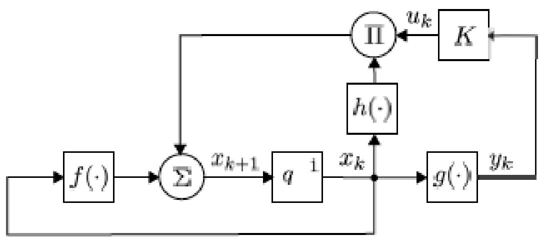
Existing Approaches

- Physics based models coupled with dynamic state estimators
- Statistical analysis such as CUSUM test on measurements
- Machine learning based methods

Drawbacks

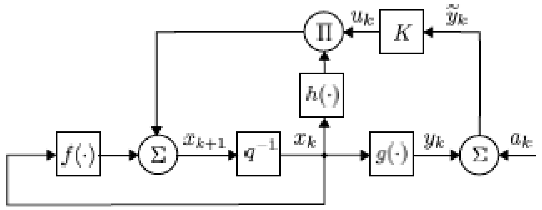
- Challenges of modeling physics based models
- Unforeseen changes, inaccurate estimates during transients
- insufficient training data, need of computational resources

Attacks in Cyber-Physical Systems



Closed-loop system under normal operating conditions

$$x_{k+1} = f(x_k) + h(x_k)\,u_k$$
$$y_k = g(x_k)$$



Closed-loop system under attack

$$x_{k+1} = f_c(x_k) + h_c(x_k)\,a_k$$
$$\tilde{y}_k = g(x_k) + a_k$$

Existing Approaches

- Physics based models coupled with dynamic state estimators
- Statistical analysis such as CUSUM test on measurements
- Machine learning based methods

Drawbacks

- Challenges of modeling physics based models
- Unforeseen changes, inaccurate estimates during transients
- insufficient training data, need of computational resources

Our Approach

Detects and localizes attacks in near real-time from streaming data without the knowledge of models, and does not require any training or computational resources

Koopman Operator and Koopman Modes

- Time-series data: $[x_1 \; x_2 \; x_3 \; \cdots \; x_{n-1} \; x_n]$
- Define vector-valued observables that are functions of state: $g = [g_1 \; g_2 \; \cdots \; g_p]^\top$

Finite dimensional approximation of the Koopman operator:

$$K = K_1 K_2^{\dagger}$$

$$K_1 = \frac{1}{n}\sum_{k=0}^{n-1} g(x_{k+1})g(x_k)^T \text{ and } K_2 = \frac{1}{n}\sum_{k=0}^{n-1} g(x_k)g(x_k)^T$$

Koopman tuple:

[eigenvalue (λ_j), eigen function (ϕ_j), Koopman mode (v_j)]

Koopman Operator and Koopman Modes

- Time-series data: $[x_1 \; x_2 \; x_3 \; \cdots \; x_{n-1} \; x_n]$
- Define vector-valued observables that are functions of state: $g = [g_1 \; g_2 \; \cdots \; g_p]^\top$

Finite dimensional approximation of the Koopman operator:

$$K = K_1 K_2^\dagger$$

$$K_1 = \frac{1}{n}\sum_{k=0}^{n-1} g(x_{k+1})g(x_k)^T \text{ and } K_2 = \frac{1}{n}$$

Koopman tuple:

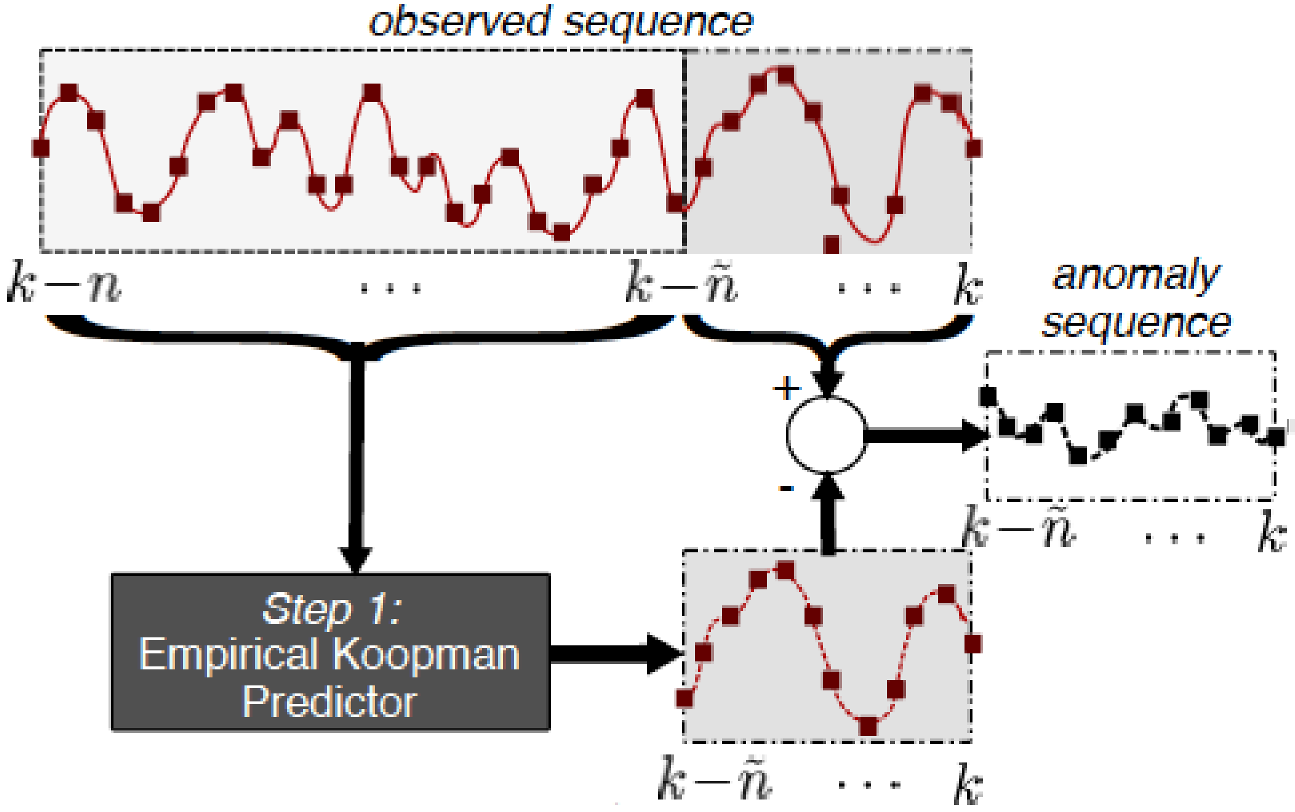
[eigenvalue (λ_j), eigen function (ϕ_j), Koopman mo

- Relation between the observable functions and the Koopman tuple:

$$g(x_k) = \sum_{j=1}^{n-1} \phi_j(x_k)v_j = \sum_{j=1}^{n-1} \lambda_j^k \phi_j(x_0)v_j$$

- Vector valued coefficients $[v_j]$ - Koopman modes (KMs)
- λ_j - encodes the temporal signatures in the dynamics
- $\phi_j(x_0)v_j$ - encodes the spatial signatures

Attack Identification Algorithm: Koopman Modes



Empirical Koopman modes

$$g(x_k) = \sum_{j=1}^{\infty} \phi_j(x_k) v_j = \sum_{j=1}^{\infty} \lambda_j^k \phi_j(x_0) v_j$$

Step 1

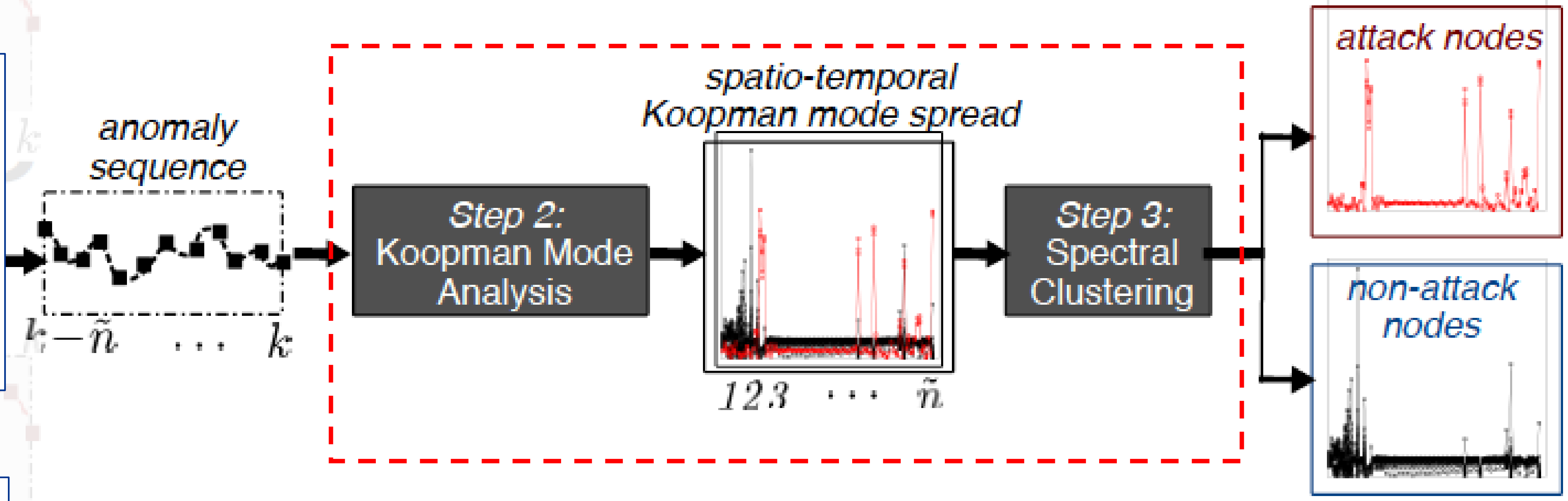
- Split the observation sequence into a *learning sequence* and a *prediction sequency*
- *Learn empirical Koopman modes* from the learning sequency
- Apply the Koopman modes to *compare the prediction sequence*

Together these steps allow us to identify any malicious attack signature which stand out as a separate cluster distinct from others

Attack Identification Algorithm: Koopman Modes

Step 2
- Perform Koopman mode analysis on the *anomaly sequence* (after a *spatio-temporal normalization*)

Step 3
- Apply *KL divergence* on normalized Koopman modes to compute distance
- Perform *spectral clustering*



Together these steps allow us to identify any malicious attack signature which stand out as a separate cluster distinct from others

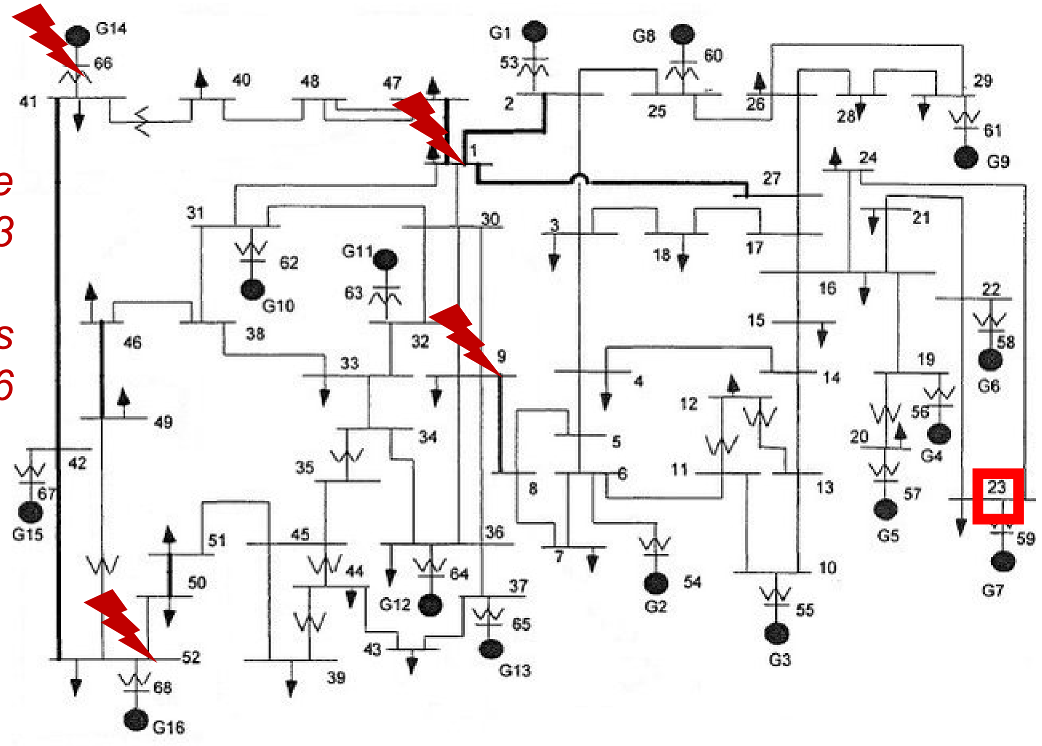
Attack Identification: Example 1

SIMULATION DETAILS: Load changes at bus 23 at 38s, and attacks at bus locations 1,9,52,66 at 39s.
All synthetic attack scenarios generated using ***GridSTAGE*** *(https://github.com/pnnl/GridSTAGE)*, a multivariate spatio-temporal data generation framework for simulation of adversarial scenarios developed under PowerDrone as part of the DOE/OE Advanced Grid Modeling program.

Multiplicative Attack: "Riding the Wave"

Load Change at # 23

Attacks at # 1,9,52,66



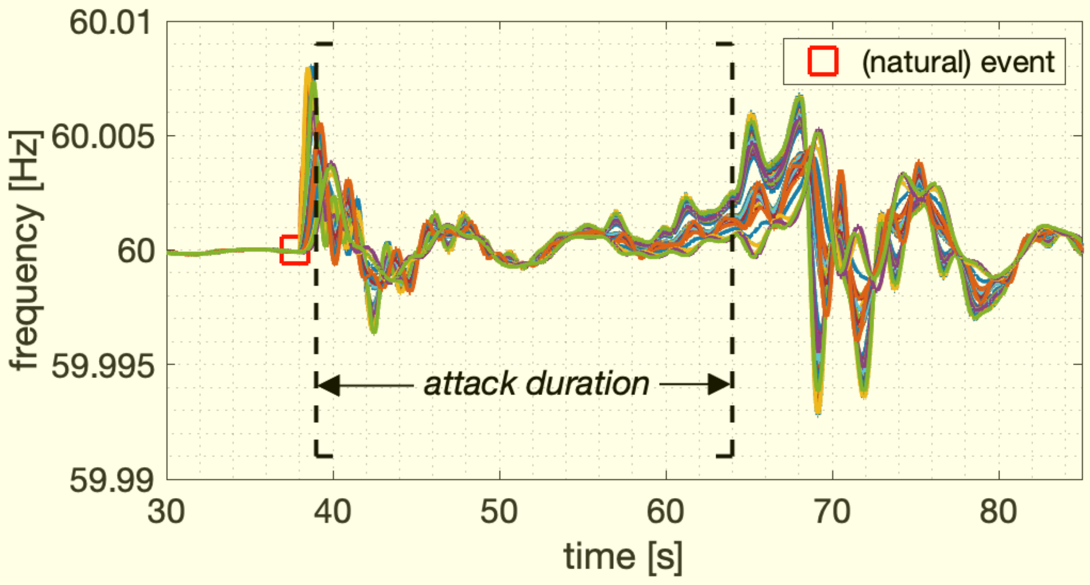
$$a(t) = \alpha\, \Delta t\, \Delta y$$

Riding the Wave Attack:

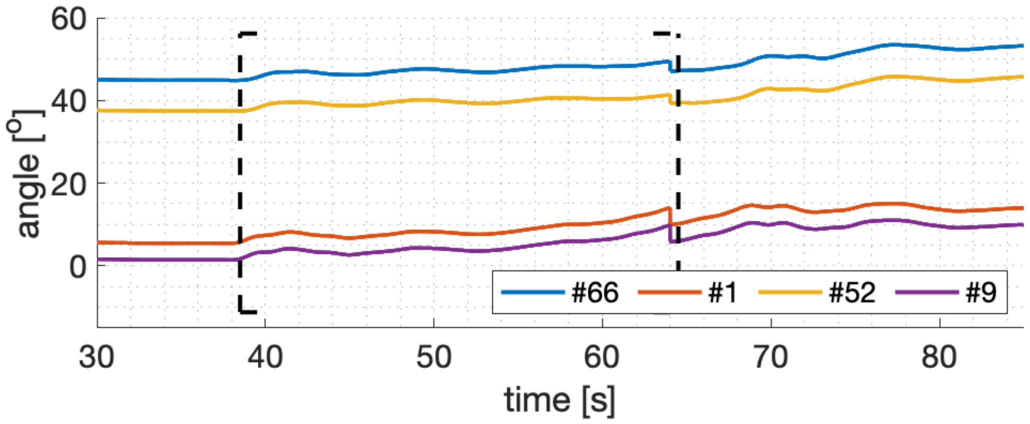
The attacker injects a signal shortly after a natural event, that grows over time in proportion to the disturbance

Hidden Attack Strategy with Delayed Impact

Impact of attack on grid frequencies



- *Delayed impact on system frequencies: large frequency excursions right after attack removal*



Attack on PMU angle measurements

Attack Identification: Example 2

SIMULATION DETAILS: Load changes at bus 23 at 38s, and attacks at bus locations 1,9,52,66 at 39s.
All synthetic attack scenarios generated using ***GridSTAGE*** *(https://github.com/pnnl/GridSTAGE)*, a multivariate spatio-temporal data generation framework for simulation of adversarial scenarios developed under PowerDrone as part of the DOE/OE Advanced Grid Modeling program.

Pacific Northwest
NATIONAL LABORATORY

Selected References

[ACC22] Bouvier, Nandanoori, Ornik, and Kundu. "Distributed Transient Safety Verification via Robust Control Invariant Sets: A Microgrid Application."

[CDC21] Nandanoori, Pal, Sinha, Kundu, Agarwal, and Choudhury. "Data-driven Distributed Learning of Multi-agent Systems: A Koopman Operator Approach”.

[TPWRS21] Nandanoori, Kundu, Lian, Vaidya, Vrabie, and Kalsi. "Sparse Control Synthesis for Uncertain Responsive Loads With Stochastic Stability Guarantees."

[SmartGridComm20] Nandanoori, Kundu, Pal, Agarwal, and Choudhury. "Model-agnostic algorithm for real-time attack identification in power grid using koopman modes.”

[ACC20] Kundu, and Kalsi. "Transient safety filter design for grid-forming inverters.”

[TPWRS20] Nandanoori, Kundu, Du, Tuffner, and Schneider. "Distributed small-signal stability conditions for inverter-based unbalanced microgrids.”

[ACC19] Kundu, Geng, Nandanoori, Hiskens, and Kalsi. "Distributed barrier certificates for safe operation of inverter-based microgrids.”

[ACC19] Kundu, Du, Nandanoori, Tuffner, and Schneider. "Identifying parameter space for robust stability in nonlinear networks: A microgrid application.”

Thank you