Grid Vulnerability in Remote Configuration of Generator Controllers:

The Threat of Hacking with Megawatts

Chris DeMarco
Power System Engineering Research Center
Department of Electrical & Computer Engineering
University of Wisconsin-Madison, USA
demarco@engr.wisc.edu

Motivation

- Idealized economic viewpoint on competitive generating units: one would like to view each as independent entity, interacting with other gens only through the market.

- Reality: Synchronous generators interconnected in AC grid form a *single, unified dynamical system*, *with significant electromechanical coupling on a continental scale*
(as witnessed August 14, 2003)

Motivation (cont.)

- More specifically: on electromechanical time-scale, dynamic coupling acts over large geographic distances through interarea modes.
- This dynamic coupling makes grid stability dependent on control parameters acting on time scales much faster than vast majority of present day ISO’s monitoring and sensing.

Motivation (cont.)

- Observation: with admirable goal of increasing flexibility of equipment and reducing personnel costs, vendors offer remote setting of generator control parameters via internet.
- At risk of picking on a “little guy,” consider following control system web advertising from Rapid-Eau Technologies, Inc.
  (page images to follow sampled Nov. 2005 at www.rapid-eau.com/opsystems.html)

Vendor Example

QuickTime™ and a
decompressor
are needed to see this picture.

Vendor Example

QuickTime™ and a
decompressor
are needed to see this picture.

Quoting from Rapid-Eau page:

“System Configuration and Troubleshooting:

An extensive amount of system parameters can be configured by the operator directly from the panel mounted interface. A laptop computer can be easily connected to the PLC to make programming changes and view logic while operating.”

Quoting from Rapid-Eau page:

“Remote Operation:

The Ethernet Bridge module is an add-on for the PLC that allows remote operation of the entire control system. Remote operation can be configured to use any type of dedicated Ethernet or Internet connection. To ensure system security, features ***CAN*** be put into place such as a firewall, data encryption, and user passwords.”

(emphasis mine...)

Abridged version of this talk…

- My strong recommendation to replace:

  “*CAN*”

  in previous slide with:

  “*ABSOLUTELY MUST*”

For the Unabridged Version

- I engaged in work in 90’s to demonstrate that governor controller redesign, deployed in small number of governor feedback loops, could selectively destabilize a power system (fairly complete summary of work in T. Gorski and C. DeMarco, "Application of Dynamic Generation Control for Predatory Competitive Advantage in Electric Power Markets," pp. 517-546, in Restructuring, Power Systems Engineering and Economics, F. Galiana, M. Ilic, L. Fink, ed., Kluwer Academic Publishers, Boston, 1998.)

For the Unabridged Version

Goal today is to revisit and update that work, with perspective that advances in networked control make an intruder “hacking with megawatts” a credible threat, as opposed to a dirty trick for a market player seeking competitive advantage, as I envisioned in work almost a decade ago.

Potential “Weakness” of Previous Formulation

- In ‘98 book chapter, estimate of system dynamic state was needed for control at each generator; assumed full state observer in each control loop.

- Large computational burden might have made predatory control impossible to implement with standard controller hardware: “what’s a quad processor system doing in that generator’s governor loop?”

New Contribution Here

- Show predatory control has special structure that allows much reduced order observers; indeed, only second order controller needed in each loop.

- Consequence: predatory controller take on *extremely* simple feedback structure in governor loop, easily implemented with slight software reconfiguration of standard control functions.

New Issues Here

- Concern 1: ease of “nearly normal” implementation could make predatory control very difficult to police against.
- Concern 2: frequency of continuously sampled measurements in present ISO practice make identification of controller parameters in (anywhere near) real time *extraordinarily* difficult.

Technical Development

- State feedback predatory control is really simple exercise in eigenvector/eigenvalue placement.

- Hacker must have approximate knowledge (our studies suggest ±20%) of linearization of system swing dynamics: state matrix **A**; e-values λ_1, λ_2 , λ_3 …, e-vecs v_1, v_2 , v_3...

Technical Development

- Choose one pair of complex e-values (a swing mode) to destabilize; say $\lambda_1 = \lambda_2^*$. New unstable e-values chosen $\underline{\lambda}_1 = \underline{\lambda}_2^*$.

- Set of small number *m*>1 machines collaborate in predatory control; this determines an input matrix **B** (physically: inputs are Δ power commands at corrupted generators).

Technical Development

- Design state feedback matrix **F** such that:

$$(\mathbf{A} - \mathbf{BF})\, \underline{v}_1 = \underline{\lambda_1}\underline{v}_1; \qquad (1)$$

$$(\mathbf{A} - \mathbf{BF}) v_k = \lambda_k v_k \quad \text{for } k=3, 4, \ldots, n. \quad (2)$$

- $\underline{v}_1$ is new unstable eigenvector; constructed to maximize component magnitudes at targeted machines, mininmize components at control group machines.

Key New Observation

- A bit of algebra on (1)& (2) reveals that any **F** must have rows made *only* of linear combinations of real & imag part of left eigenvector for original λ_1 .

- Payoff: To estimate **Fx**, don’t need whole state **x**, only the two dimensional subsystem associated with the one mode λ_1 !

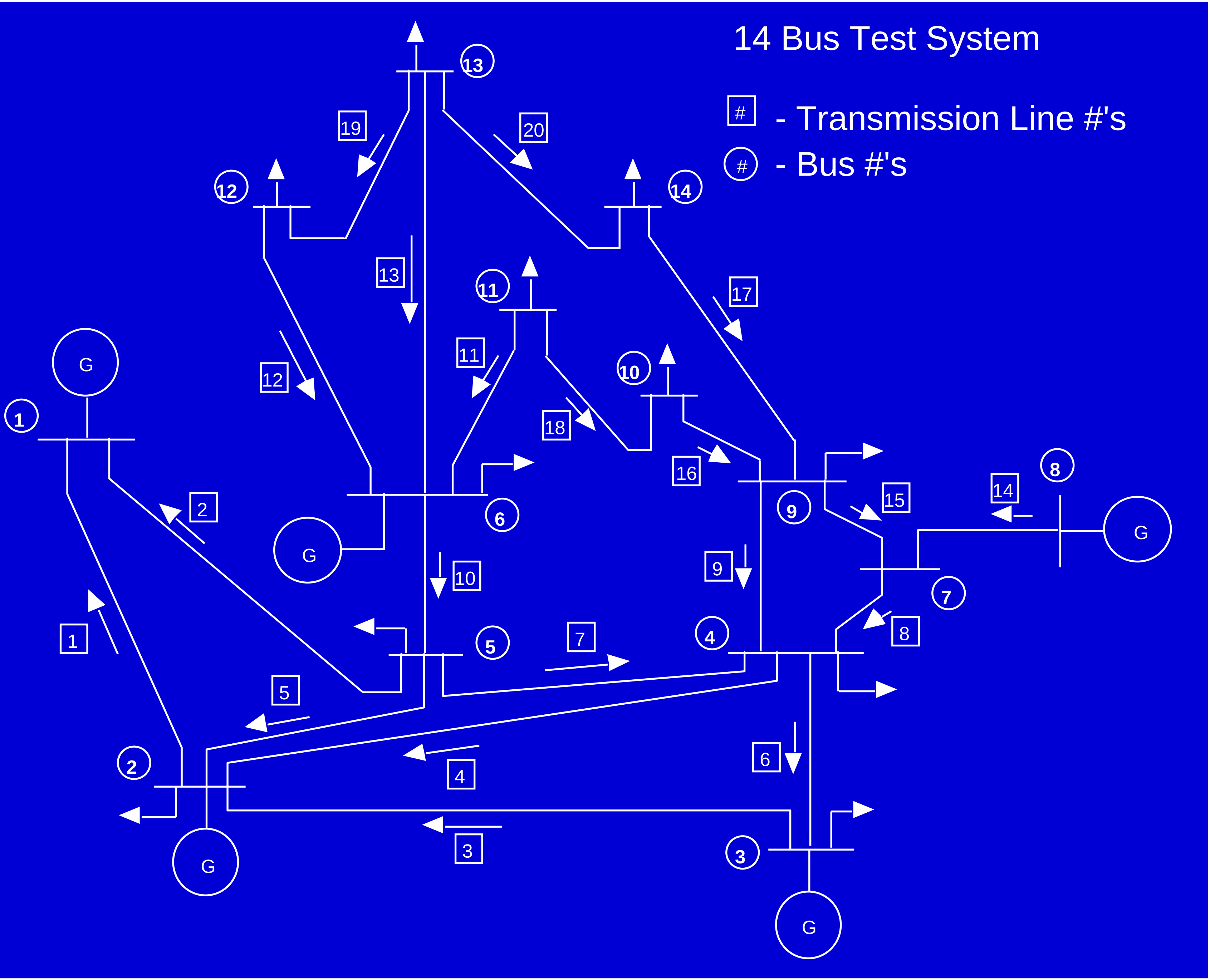
Little Case Study

- Based on modified form of IEEE 14 bus test system; 5 generators, one set as infinite bus here (note that presence of an infinite bus makes job of designing predatory control more challenging!)

14 Bus Test System

- Transmission Line #'s

# - Bus #'s



Predatory Control Design

- Predatory group – gens at buses 2 &3.
- Control is designed such that (“ideally”): gen@3 experiences no oscillations;

  gen@8 2.4x larger oscillation than gen@2;

  gen@8 1.9x larger oscillation than gen@2

Predatory Control Design

- Each controller acts as a strictly local governor feedback, from local frequency error measurement to commanded prime mover ΔMech_Power.

Predatory Control Design

$$G_1(s) = \frac{-(0.0982s + 0.5306)}{s^2 - 0.68s + 25.62}$$

poles at -0.34 ± j5.05, zero at -5.403;

$$G_2(s) = \frac{0.0474s + 0.6139}{s^2 - 0.68s + 25.62}$$

poles at -0.34 ± j5.05, zero at - 12.95 .

Simulation Results

- Simulation here is simple swing dynamics only, classical model (admittedly, a rough cut…)

- However - it tests efficacy of linear predatory control design in a model reflecting nonlinear power flow coupling.

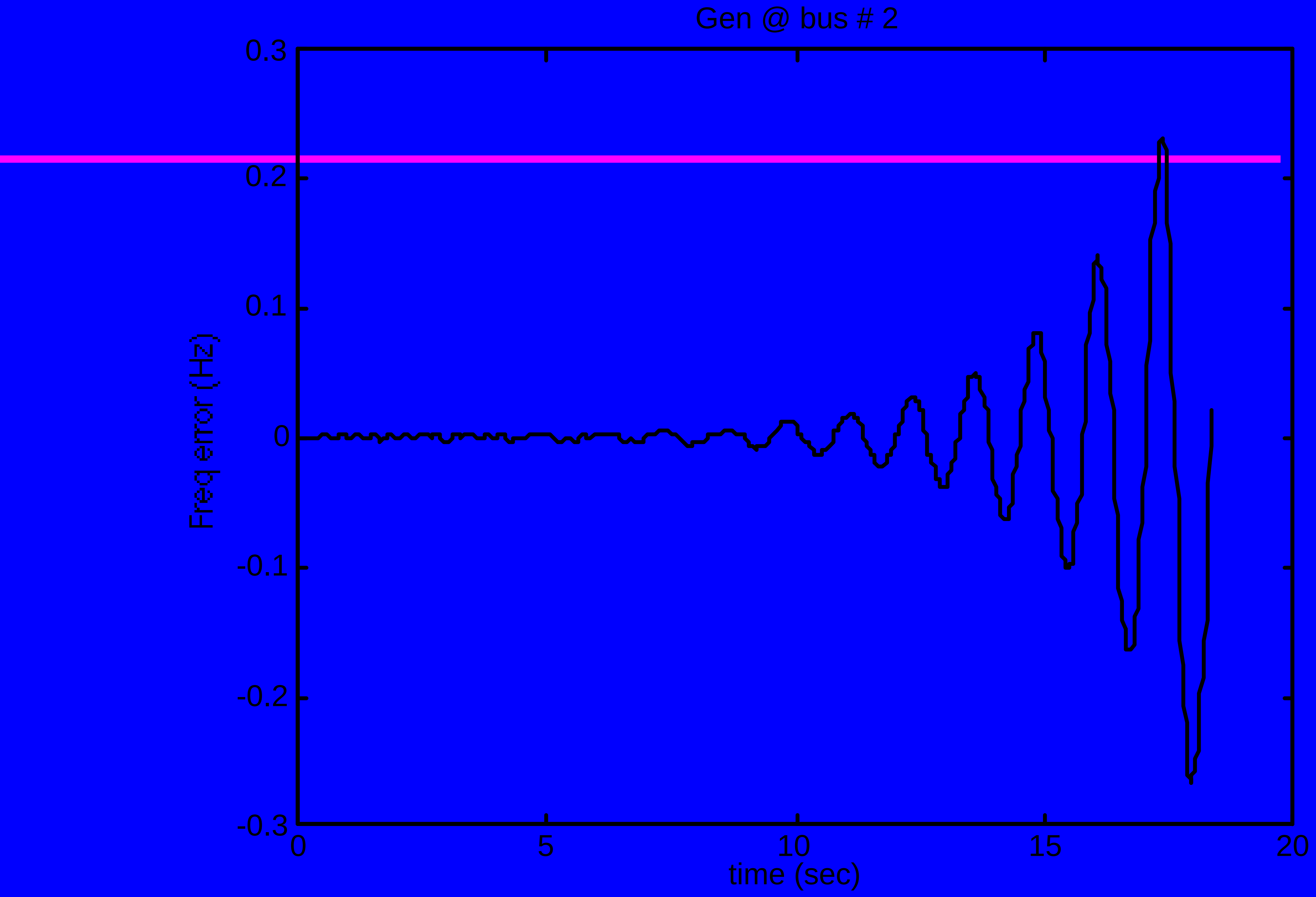


Figure 2: Generator@2 Frequency Trajectory

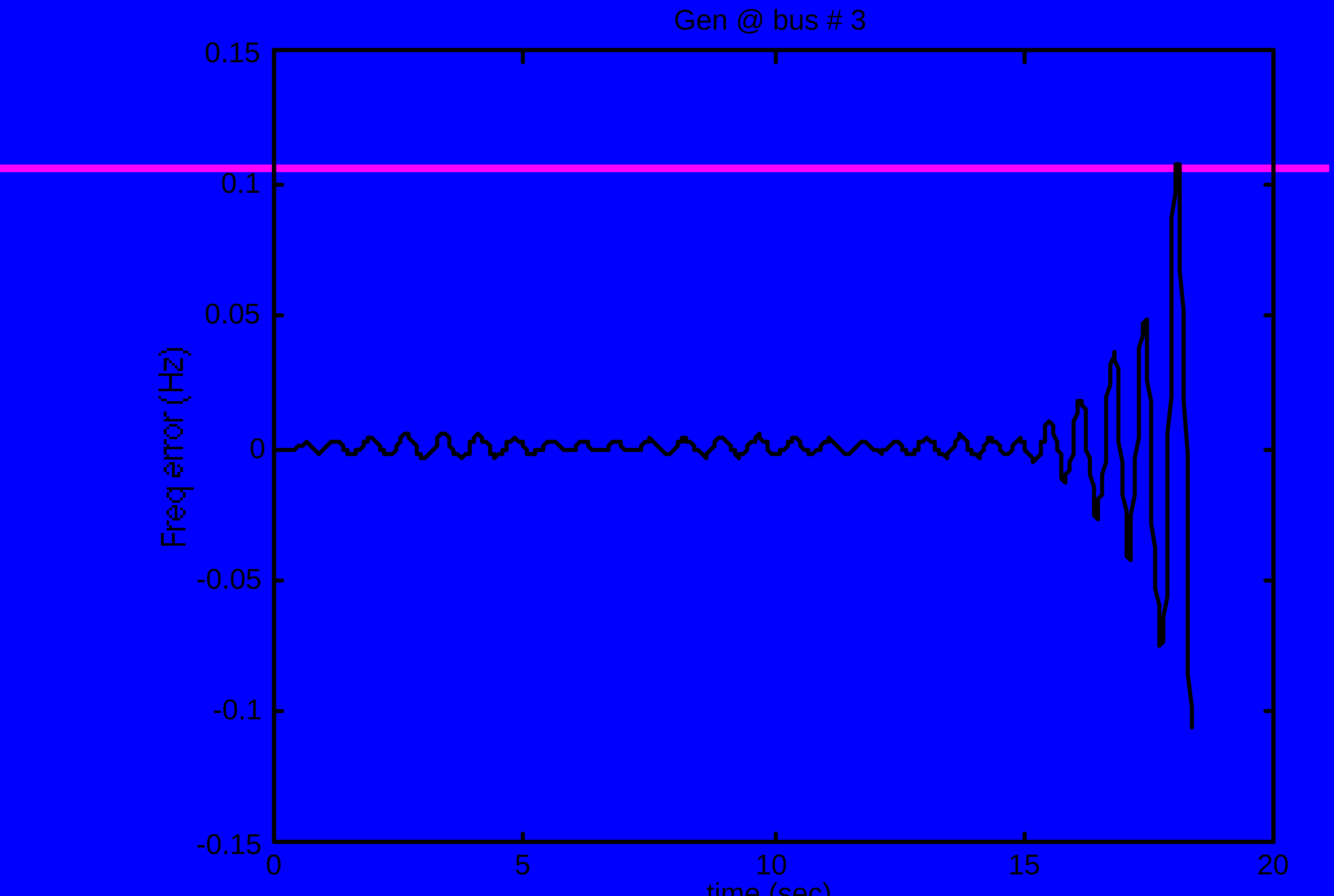


Figure 3: Generator@3 Frequency Trajectory

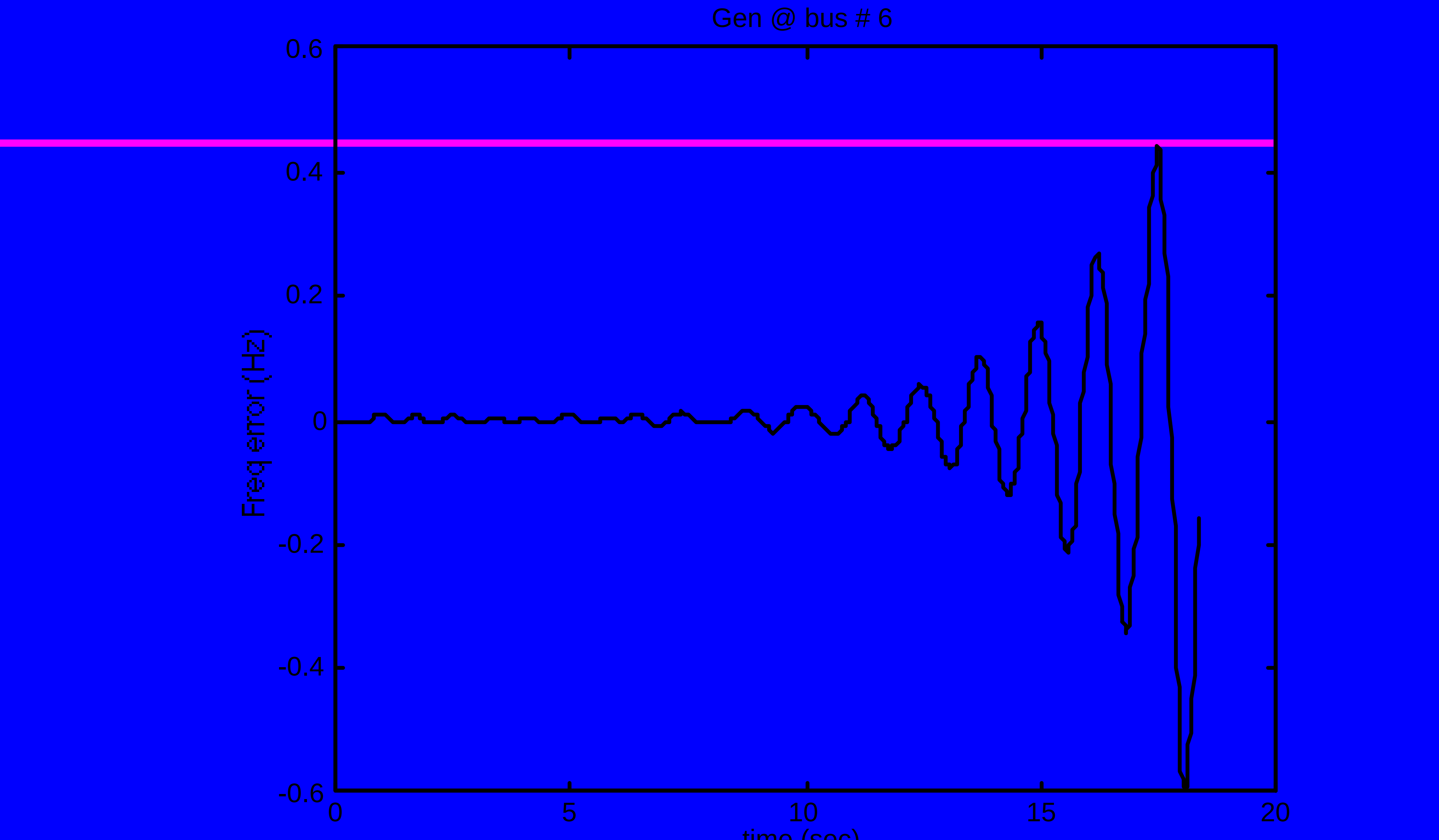


Figure 4: Generator@6 Frequency Trajectory

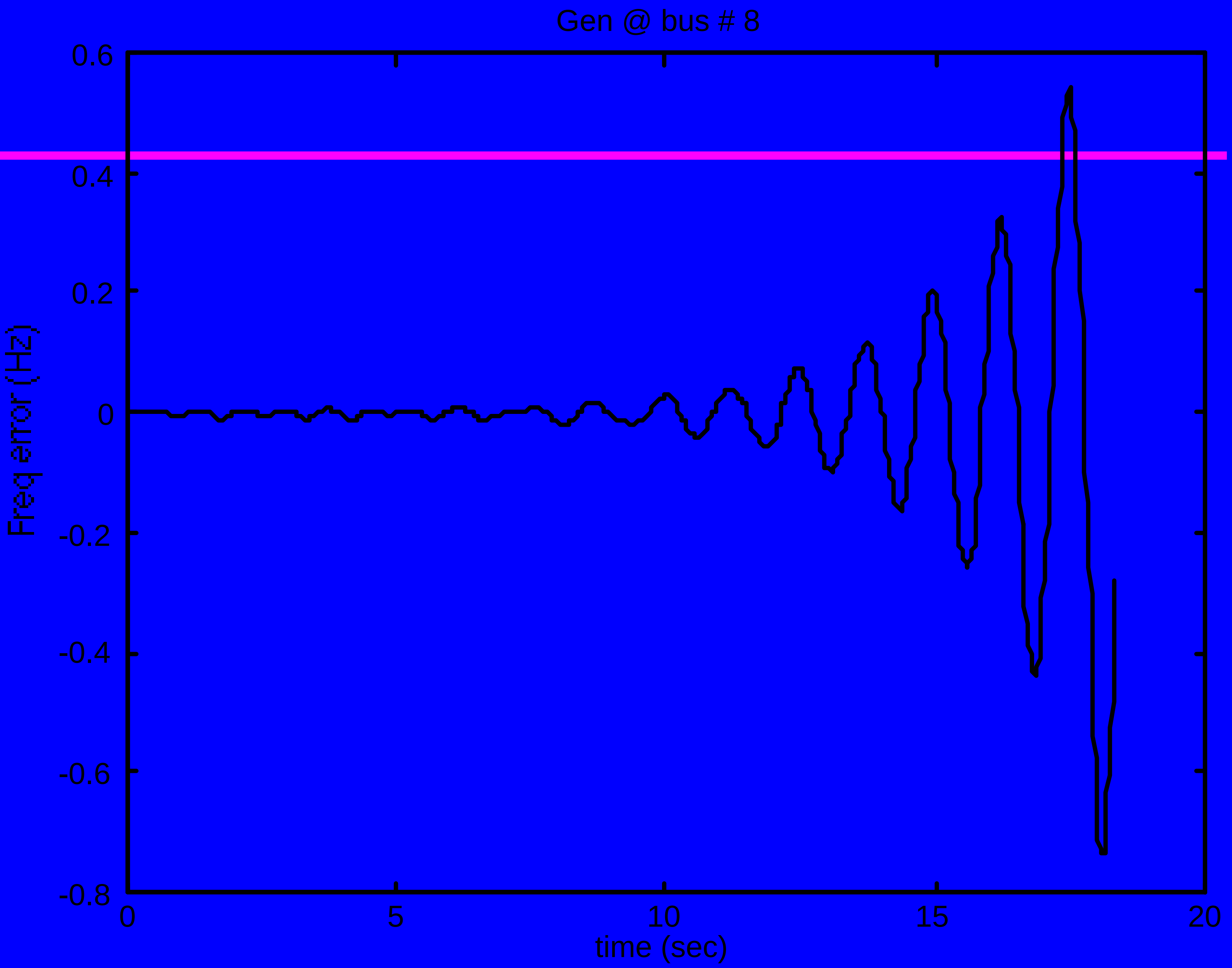


Figure 5: Generator@8 Frequency Trajectory

Observations

- Recall that common form of protective relay on generators is disconnect on detection of excessive df/dt = rate of change of frequency.

- Predatory design successfully subjects target machines to much higher df/dt than machines exercising the predatory control.

Observations

- Key point: generators experiencing the “worst instability” are NOT those machines causing it!

Conclusions

- New algebraic observation indicates predatory control very easy to implement.
- Only second order transfer function added in governor control loop at each participating machine (example here – just 2 machines)
- With remote internet access to gen controller parameters, intruder could turn these on/off selectively.

Conclusions

- Implications: suggests predatory control might be difficult to police against.
- In particular, detecting “point of intrusion” into system would be very challenging without real-time monitoring of internal control parameters –to best knowledge of this author, no regulations/ authority for such monitoring currently exist!

Conclusions

Decision for today’s audience: is this a ridiculous red-herring or a Cassandra’s warning:

That seduced by attractiveness of advanced internet technology for remote controller updates, insufficient attention will be paid to severe SYSTEM-WIDE vulnerabilities created if intruders gain access to controllers of even a small number of low output generators.