

Opportunities and Perils in Ubiquitous Data Availability for the Open Access Environment

Panel: Grand Challenges in
Electric Power Engineering
Christopher L. DeMarco
University of Wisconsin-Madison

IEEE Power Engineering Society
Winter Meeting
Wednesday, January 30, 2002



PSERC

History: FERC Orders 888/889

- Order 889's title coined OASIS for "Open Access Same-time Information System."
- To many, OASIS goals seem far from fully realized today, raising natural questions:
- Is it a technical challenge to be overcome, to efficiently communicate & efficiently compute summary of available transmission capability?
- Or are there valid institutional/policy reasons to question timely release of relevant data?



Today: Pose Questions...



⌘ What if maximally feasible amount of transmission/distribution data were truly made universally available?



Today: Pose Questions...



- ⌘ Would this create beneficial opportunities, and realize goals envisioned in OASIS?
- ⌘ Or would it be too perilous, endangering consumer privacy and infrastructure security?



Specific Scenario

Suppose: all control centers posted to universally accessible site the raw measurements typically fed to state estimator.



Speculate - Potential Benefits

- ⌘ Create true competitive market for special purpose state estimators, culling useful information from data;
- ⌘ Decentralized & specialized ATC calculations;
- ⌘ Create more effective load management;
- ⌘ Open door to cost effective integration of micro-grids to large distribution/transmission system
- ⌘ Facilitate move to cost effective real time pricing.
- ⌘ General premise - observing example of GPS data - once useful data is made widely accessible, entrepreneurial opportunities to exploit data abound.



Speculate - Potential Perils

- ⌘ Unacceptably compromise privacy, proprietary data of customers;
- ⌘ Ability to extract detailed individual consumption production patterns seems inevitable (isn't it?);
- ⌘ Broadcast knowledge of grid's Achilles heels;
- ⌘ Aid ill-intentioned players in design of "maximal disturbances" & malicious controllers



Details - Potential Perils

Author's previous work on malicious control:
Given power flow network data, and
"reasonably accurate" ($\pm 20\%$) knowledge
of generator dynamic parameters, one
can design local generator controls to
intentionally destabilize *other* machines.



Details - Potential Perils

Concern: earlier malicious control work postulated “only” over-aggressive, unethical competitor in the power market;

How much worse if agent implementing control is unconstrained by concerns of remaining in the market after the event?



Is There a Silver Lining (and a Grand Challenge?)

(and a potential tie-in to state estimation
grand challenges to follow... ?)

Hypothesis - hope for acceptable trade-off
in data opportunity vs. privacy/security
lies in distributed, scalable, monitoring &
data query systems.



... Is There a Silver Lining (and a Grand Challenge?)

- ⌘ View extraction of raw data from power system as database queries;
- ⌘ Local “managers” of portions of the database perform automated negotiation for releases of data;
- ⌘ Queries could be legitimated by “tipping one’s own cards;” I get data only if I have useful data or computations to share.



Conclusions

- ⌘ Strong reasons to believe that wide spread availability of transmission/distribution data *is* a prerequisite for benefits of open access.
- ⌘ But ... genuine security/privacy concerns make unfettered, universal release of data dangerous.
- ⌘ Challenge - can concepts from database security and query protocols be adapted to offer *relatively* open data, with decentralized verification and validation?

