# Comments to the U.S.-Canada Power System Outage Task Force Regarding the Interim Report

**Carl Hauser**

**Technical Report EECS-GS-004**

**School of Electrical Engineering and Computer Science**
**Washington State University**
**Pullman, Washington 99163**

**November 2003**

Comments to the U.S.-Canada Power System Outage Task Force
Regarding the Interim Report, November 2003

Carl Hauser
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington 99163

hauser@eecs.wsu.edu

## Introduction

These comments raise questions, not addressed in the November 2003 Interim Report, which I believe to be important for understanding what happened on August 14 and for reducing the likelihood of such occurrences in the future. Because I am a computer scientist, not a power engineer, my concerns address exclusively the performance of the information technology (IT) systems before, during, and after the outage. These comments reflect what is said in the Interim Report (IR) as well as the MISO telephone transcripts submitted to the House Committee on Energy and Commerce at their hearing on September 4, 2003 (http://www.2003blackout.info/hearingdocs/grid_transcript.pdf).

The IR emphasizes the importance in this kind of investigation of establishing root causes for the outage. As in almost all major incidents involving highly complex systems, the root causes for this outage are manifold. The report identifies causes in three categories: inadequate situational awareness, inadequate tree trimming and inadequate reliability-coordinator diagnostic support as principal causes of the August 14 outage.

In the first and third categories, information technology systems play crucial roles. The IR's treatment of the problems in those systems on Aug. 14 does not begin to approach the detail of analysis that is shown for the behavior of the power aspects of the system. The comments below address in turn IT systems at FirstEnergy, at MISO, and the IDC.

## FirstEnergy Alarm System and EMS

The IR details the failure of the alarm system at FirstEnergy and the unawareness of the failure by FirstEnergy personnel (pp. 28 ff). In summarizing the causes the IR concludes that the root causes were "FE lacked procedures to ensure that their operators were continually aware of the functional state of the critical monitoring tools" (p. 23, Group 1, C) and "FE lacked procedures to test effectively the functional state of these tools after repairs were made." (p. 23 Group 1, D). What is missing here is any questioning or analysis of the *design* of these tools that allowed them to fail as they did.

There are several indications in the IR that worrisome flaws exist in the FE EMS.

1. The IR notes (p. 30) that beginning between 14:20 and 14:25 EDT FE's remote control terminals in remote substations began failing due to "queueing" and "overloading the terminals' buffers". This is a serious design or implementation flaw in the alarm system software. It should not be possible to drive the alarm system itself into failure with data loading produced by the operating power system.

2. At 14:41 EDT the FirstEnergy EMS primary server failed for reasons that are speculated to be either stalling of the alarm application or queuing backlog at the remote terminals (p. 30). Operation transferred to the hot-standby server which subsequently failed for the same reason. While well-suited for protection against *hardware* failure of the primary server, the hot-standby architecture is not sufficient protection for the kind of *software* failure apparently experienced here: failure of the backup server is to be expected in this case as both are faced with the same input data.
3. Failure of the primary and backup EMS servers also took out the AGC function, the strip chart function and ACE function as well as slowing the operators' screen update rate to "a crawl". The design of backup functionality in the system again appears to be inadequate.
4. Post-outage it was determined that the "only available course of action to correct the alarm problem was a 'cold reboot' of FE's overall XA21 system." (p.32) At 15:42 control room operators had decided not to allow IT personnel to perform a cold reboot because they "considered power system conditions precarious, were concerned about the length of time that the reboot might take to complete, and understood that a cold boot would leave them with even less EMS support until it was completed." (p. 32) Again one questions the design of the EMS: it fails at a time when the power system state is "precarious" and the *only* solution to such a failure is a cold reboot which will render it even less available over an extended period of time.

These observations from the IR strongly suggest that a line of inquiry is needed into the reliability characteristics first, of the EMS at FE, second of any other installations of the same product, and third of other EMS products in use in the North American power grid. (The IR notes that the FE EMS is scheduled for replacement and was not the latest version available. These facts do not obviate the need to investigate the cause of the EMS failures.)

The Security Working Group's report in Section 6 of the IR adequately rules out security-related concerns as the cause of these failures. But no group had the charter to find root causes for these failures: we know what *was not* the cause, but we don't know what *was* the cause.

## The MISO State Estimator

The IR discusses difficulties with the MISO state estimator (SE) between 12:15 EDT and 16:04 EDT. The fact that it was not functioning was not noted until 14:40 which is itself a major concern, as noted in the IR. However, additional questions should be asked.

The SE is not able to solve when its view of line status does not reflect reality. It is an ongoing project at MISO to automatically update line status from reports received from ECAR and direct data links. Some line status updates which are not yet automated and which had to be performed manually were missed and the SE was not able to solve the system. When the SE does not reach a solution, the system engineer must diagnose the cause – a time-consuming activity (apparently, diagnosing the Stuart-Atlanta line outage took about 20 minutes (p. 27)). The question here is whether the combined automated and

manual system constitutes an adequate analysis framework for reliable operation. The SE normally runs every 5 minutes. If it fails, manual diagnosis taking (based on the one data point) 20 minutes is required. Does this give the reliability coordinator adequate time to respond to a contingency?

## The IDC

The IR does not mention the Interchange Distribution Calculator (IDC) even in the system overview section, yet the MISO phone transcripts indicate that operators at several utilities and MISO were having difficulty performing updates to it on Aug. 14, both earlier in the day and after the outage. Those conversations and other descriptions of the IDC available to the layman (for example, http://www.memagazine.org/supparch/mepower01/computing/computing.html) suggest that the IDC plays an important role in scheduling power transactions so as to not overload the transmission system. Furthermore, the transcripts suggest that the reliability coordinators are dependent on the IDC for at least some of their situation awareness concerning operational status of transmission lines.

The conversations and published descriptions raise two concerns about the IDC. First, its slow performance was apparently a distraction to the operators during early stages of recovery from the outage. It became difficult to load line status and TLR information into the IDC. In the phone transcripts the operators comment that the updates are taking a long time. Don Hunter at MISO contacts IDC support for assistance with loading a TLR that has repeatedly failed to load (MISO Transcript 2003 08-14 CH20 Second RC 1659ahrs.wav/1702hrs.wav). Once the TLR loads successfully he remarks on how the IDC is getting slow. In addition to the distraction factor for the operators, slow performance is an obstacle to the IDC's fulfilling its apparent role as a communication channel for line outage status.

The other concern relates to the IDC design. The operators in the phone transcripts and the description of the IDC interface refer to it as a "web page" and refer to "the internet" being "slow today". (These conversations are post-outage and so would not be seen as causally related.) Later an operator says "we have no internet connection to access OATI [operator of the IDC]" (MISO 2003 08-14 CH20 Second RC 1722hrs.wav) It is not clear whether the "internet" referred to here is the public internet or a private network, however, there is nothing to discount the former interpretation. If that were the case, it would be a major concern for several reasons, including susceptibility due to power outages and overload due to internet virus and worm activity

The phone transcripts suggest that line status updates in the IDC are performed by having operators enter the updates on the IDC web page.[1] There are hints that the IDC serves as a clearinghouse for line status information between security coordinators and transmission operators, but I cannot be sure of this. If so, this appears to be an inadequate

[1] 2003 08-14 CH 25 OPS ENG 1214hrs.WAV MISO/Mihbachler and Cinergy/Spencer discuss "putting in" outages. It is not clear that they are referring to entry into the IDC or some other system requiring manual entry. If the latter, the above comments would apply to it as well. Later in the same transcript Mihbachler: "Hey Rob – have these all been applied to the IDC? MISO/Rob Benbow: I don't know that anybody has run to the IDC and updated it.

mechanism when the situation is changing rapidly, operators are distracted with more pressing local concerns, and updates take minutes. Indeed, even for performing the interchange calculations, the IDC's picture of the system state may be incorrect to the point that wrong decisions are made.

## Summary

The IR identifies inadequate situational awareness at FirstEnergy and inadequate diagnostic support at MISO as among the principal causes of the outage. However, unlike the detailed, transmission line by transmission line chronology and causal sequence it provides for the transmission system, the IR provides scant analysis of the operation of the IT systems related to these causal factors. Furthermore, the IR does not even mention the IDC and how it performed before, during and after the outage, although the MISO transcripts clearly indicate that it was not performing as well as usual.

The power grid increasingly relies on IT systems to operate more efficiently and in a more market-oriented fashion. What the IR shows of the IT systems' performance on Aug. 14th suggests that there are important lessons to be learned about reliability of IT systems used to operate the grid. The IR does not delve deeply enough into the IT domain to make those lessons accessible to the industry. Answers to the following questions are urgently needed if future blackouts are to be prevented:

- What IT systems are critical for the RC and Control Areas to carry out their missions?
- Can the power grid be operated, perhaps in a degraded, less efficient mode, without functioning IT systems? Or have grid operations become so complex that in some scenarios control cannot be maintained without the assistance of IT systems?
- What performance standards for timely delivery of status updates are needed to ensure efficient and reliable grid operation?
- What reliability standards are needed for the IT systems? Should a failed EMS, Alarm System, State Estimator, or Contingency Analyzer itself be considered a contingency in grid operations?