

Abstract:

This paper reviews how the OSIsoft RtPM Platform (RtPM™) supports the specific Blackout Task Force recommendations. We demonstrate how the underlying OSIsoft system components provide the interface for real-time data access to multiple enterprise applications; and specifically, how other key features of the RtPM Platform meet the requirements specified in the recommendations.

Introduction: Consolidation of Task Force recommendations

The task force recommendations fall under four broad themes:

Group 1. Strict adherence to high reliability standards. Market mechanisms should be considered, but reliability should take precedence over market concerns.

Group 2. Regulated companies will not invest in improved infrastructure without

assurances that the costs will be recoverable, while unregulated companies will not make such outlays unless investments are profitable.

Group 3. Implementation of the recommendations is critical.

Group 4. IT security-related actions are needed to enhance reliability.

We will initially outline the four major components of the RtPM Platform, then describe how they apply to the recommendations

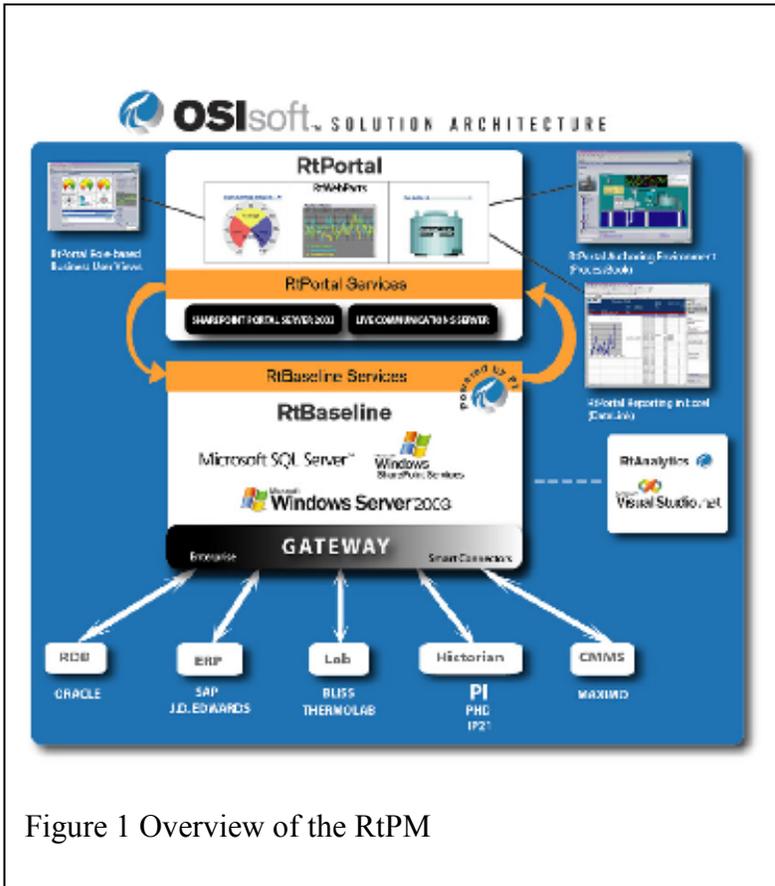


Figure 1 Overview of the RtPM

define a frame of reference or context for data, and based on some event or specific request, to gather all the relevant data from disparate sources for presentation to individuals based on their roles. RtBaseline™ is a virtual, real-time data warehouse that

- Collects data from across the enterprise

RtPM handles Blackout Task Force Recommendations

- Stores it in a time series database
- Cross-correlates data into useful information for business users based on their roles.

RtBaseline can be rapidly installed and deployed to enable your enterprise to begin collecting real-time data and events quickly into this enterprise-wide, scaleable infrastructure.

RtAnalytics

This set of applications alerts you to business opportunities or issues requiring your attention. RtAnalytics™ has the process and business analytic functionality that integrate your existing knowledge management and business intelligence tools. A wizard-based Visual Studio.NET integration, an advanced calculation engine, batch Analysis, event analysis, and integration with Microsoft's .NET XML Web Services, RtAnalytics delivers all the analyses that are key to your enterprise.

RtPortal

RtPortal™ is a set of configurable, role-based portal and smart-client tools used to display processes, documents and information for effective team collaboration based on either Microsoft SharePoint Portal Server or SAP Enterprise Portal.

RtPortal crosses application, platform, and organizational boundaries to provide real-time visibility into your critical processes, providing a holistic view of your entire operation. With RtPortal, you can automate, manage and monitor processes from end to end in real-time, and provide your team with an organizational framework where they can interact and collaborate effectively.

RtPortal extends the portal environment with pre-packaged iViews or SharePoint Web parts (called RtWebParts) so users can build personalized pages in both SAP Enterprise Portal and Microsoft SharePoint environments.

RtStudio

RtStudio™ provides an application-building environment that plugs into Microsoft Visual Studio.NET. Users wishing to develop custom applications use this integrated software development tool.

In the following sections, we outline specific applications of RtPM on a task-by-task basis. We have omitted tasks that have no relevance RtPM applications. A complete list of Task Force Recommendations may be found in the Appendix.

Group I. Institutional Issues Related to Reliability

1. Make reliability standards mandatory and enforceable, with penalties for noncompliance.

The language to enforce mandatory standards is in the current Energy Bill pending in Congress. When passed, EROs (Electric Reliability Organizations) will have the legal right and obligation to set enforceable reliability standards with financial and civil penalties for non-compliance. FERC, in the absence of legislation, is ramping up to handle grid reliability issues with its new “Vigilant Oversight” group of thirty additional staff members in the Office of Market Tariffs and Rates (OMTR).

Reliability standards include both contingency energy sources and defined ranges for critical variables in the grid, such as frequency and voltage. Each standard has a “persistence” limit, typically no longer than 30 minutes. For example, a voltage should not exceed its threshold for more than 10 minutes; if it does, the RTO/ISO is required to report this violation, and is then subject to fines for exceeding this limit.

In order to implement this type of standard, “history” values must be available. The Totalizer function in RtAnalytics is an ideal tool to implement automatic detection of standards violations. Totalizer comprises more than 1200 built-in functions to automatically compute complex events dependent on multiple values and persistence. For example, “alarm when voltage greater than X for Y minutes and frequency less than Z for M minutes, or if reactive power less than R for 15 minutes.” This condition can be implemented in the RtAnalytics package by simply filling in the conditions to be tested in an Excel spreadsheet.

Violations must be reported and audited. The RtAnalytics toolbox includes the RtReports package, enabling users to create auditable reports automatically as required under 21 CFR Part 11 regulations of the Food and Drug and Environmental Protection Agencies. Given that a reliability standard is violated, this must be auditable by the ERO (or redefined NERC) and/or FERC. This tool would be used to quantitatively determine violations, forming the basis for fines and penalties.

2. Develop a regulator-approved mechanism for funding NERC and the regional reliability councils, to ensure their independence from the parties they oversee.

Transmission owners, generators, and other market participants pay into the funds of ten regional Reliability Councils, supporting the annual NERC budget. This arrangement makes NERC subject to the influence of the reliability councils, which are in turn subject to the influence of their control areas and other members. This arrangement compromises the independence of both NERC and the councils, making it difficult for these agencies to act forcefully and objectively.

The Task Force recommendations involve a substantial increase in NERC’s functions and responsibilities, as well as a budget increase.

RtPM handles Blackout Task Force Recommendations

The RtPM Platform, capable of handling millions of datastreams of real-time information, is an ideal tool for the new NERC/ERO. Continuous streams of live data from the Reliability Councils provide critical information on grid behavior—particularly in the “seams” between control areas and Regional Councils. We discuss this in more detail in the following sections.

3. Strengthen the institutional framework for reliability management in North America.

Item 3D of the recommendations includes a detailed discussion of the current NERC function model. This model consists of the following 16 functions:

- **Operating reliability**
- **Planning reliability**
- **Balancing (generation and demand)**
- **Interchange**
- Transmission service
- Transmission ownership
- Transmission operations
- Transmission planning
- Resource planning
- Distribution
- Generator ownership
- Generator operations
- Load serving
- Purchasing and selling
- Standards development
- Compliance monitoring

The top four in boldface type are considered critical in reliability operations. Within these four categories, the Task Force considers the following areas to be key success factors:

1. Fully operational backup control rooms.
2. System-wide (or wider) electronic map boards or functional equivalents, with data feeds that are independent of the area’s main energy management system (EMS).
3. Real-time tools that are to be available to the operator, with backups.
4. SCADA and EMS requirements, including backup capabilities.
5. Training programs for all personnel who have access to a control room or supervisory responsibilities for control room operations.
6. Certification requirements for control room managers and staff.

In many ISOs today, RtPM is used for all six areas.

5. Track implementation of recommended actions to improve reliability.

NERC intends to initiate a reliability performance monitoring function that will evaluate and report on trends in bulk electric system reliability performance.

RtReports is an ideal tool for this function. The reports can be created with no programming and are fully auditable. This means that no changes can be made to the reports unless made and electronically signed by the authorized individual making the changes.

10. Establish an independent source of reliability performance information.

Those responsible for making energy policy and a wide range of economic decisions need objective, factual information about basic trends in reliability performance. The Energy Information Agency (EIA) and other organizations should identify information gaps in federal data collections covering reliability performance, and physical characteristics. Plans to fill those gaps should be developed and associated resource requirements determined. After acquiring those resources, EIA should publish information on trends, patterns, costs, and other issues related to reliability performance.

Today's EIA databases do not include high-resolution, time-sensitive information. Generally, the smallest time interval reflected is one month. However, true understanding of both the market and grid reliability requires much finer time resolution. Even now, spot markets, hourly markets, and day-ahead markets are in effect and can have a significant effect on grid reliability.

Using RtPM as the repository and deliverer of real-time and historical information to users is one means of meeting the recommendations of the Task Force. The RtBaseline component is the only time series archive system that supports millions of data streams on a single server. RtBaseline is capable of handling over 200,000 events per second and storing up to 4 Petabytes (1000 Terabytes or 1,000,000 Gigabytes) of information.

These capabilities allow the EIA or designated organization to store critical grid transactions to a very fine level of granularity and make these data available online for many years. With RtPortal, users should be able to access data in much the same manner as they currently do. RtPortal supports a common set of Webparts, allowing individuals to create Webpages that best suit their needs.

11. Establish requirements for collection and reporting of data needed for post-blackout analyses.

Some of the data needed to analyze the August 14 blackout fully was not collected at the time of the events; other reported data was based on incompatible definitions and formats. Consequently, there are aspects of the blackout— particularly those concerning the evolution of the cascade—that may never be fully explained. FERC, EIA and appropriate authorities in Canada should consult with NERC, with key members of the

RtPM handles Blackout Task Force Recommendations

investigation team, and with the industry to identify information gaps, adopt common definitions, and establish filing requirements.

RtBaseline (formerly known as PITTM database) was used by many utility companies affected by the blackout. Some were able to capture and save PI archives—the day after the blackout. This data could serve as the basis of a huge permanent archive supporting future research and development of the Digital Grid.

Though not widely known, the PI system has an interface developed by SISCO that automatically collects digital fault recorder files and automatically stores them in a PI data archive. This capability was offered to the Blackout Task Force.

13. DOE should expand its research programs on reliability-related tools and technologies.

Important areas for reliability research include but are not limited to:

- Development of practical real-time applications for wide-area system monitoring using phasor measurements and other synchronized measuring devices, including post-disturbance applications.

OSISoft developed and supports an IEEE 1344 Synchrophasor interface for Phasor Measurement Units. The Arbiter 1133A in particular has been implemented at Entergy; that data has been shared with TVA using the OLE for Process Control (OPC) server interface method. OPC has been adopted by the Eastern Interconnection Phasor project.

- Development and use of enhanced techniques for modeling and simulation of contingencies, blackouts, and other grid-related disturbances.

OSISoft developed real-time interfaces to the Distribution Engineering Workstation product as part of the DOE-funded Distributed Generation projects.

- Investigation of protection and control alternatives to slow or stop the spread of a cascading power outage, including demand response initiatives to slow or halt voltage collapse.

Below is an example of how a utility company is using OSISoft's technology to successfully avoid cascading blackouts.

- Reevaluation of generator and customer equipment protection requirements based on voltage and frequency phenomena experienced during the August 14, 2003 cascade.
- Investigation of protection and control of generating units, including the possibility of multiple steps of over-frequency protection and possible effects on system stability during major disturbances.

RtPM handles Blackout Task Force Recommendations

- Development of practical human factor guidelines for power system control centers.
- Study of obstacles to the economic deployment of demand response capability and distributed generation.
- Study of air traffic control, the airline industry, and other relevant industries for practices and ideas that could reduce the vulnerability to human error of the electricity industry and its reliability managers. Cooperative, complementary research and funding between government and industry and among nations should be encouraged.

The key issue of graphical user interface is a strong point of RtPM, which supports both Webparts and Smart Client interfaces. This means that ProcessBook's™ power and ease of use are reflected in the Web interface, with each ProcessBook display becoming a Webpart.

Group II. Support and Strengthen NERC's Actions of February 10, 2004

15. Correct the direct causes of the August 14, 2003 blackout.

As a result of the Task Force recommendations and using OSIsoft's RtPM Platform, these systems are used more effectively than before the blackout. Several of the recommendations discuss data quality and data reconciliation before the data is used in the system state estimators. OSIsoft's Sigmafine™ is also an excellent product for data screening prior to data input.

16. Establish enforceable standards for maintenance of electrical clearances in right-of-way areas.

C. Requirement to Report Outages Due to Ground Faults in Right-of-Way Areas

Effective March 31, 2004, NERC should require each transmission owner/operator to submit quarterly reports to the regional councils of all ground-fault line trips, including causes, on lines of 115 kV and higher. Failure to report such trips should lead to an appropriate penalty. Each regional council should assemble a detailed annual report on ground fault line trips and their causes in its area to FERC, NERC, DOE, appropriate authorities in Canada, and state regulators no later than March 31 for the preceding year, with the first annual report to be filed in March 2005 for calendar year 2004.

This is a prime RtReports application, enabling all ground faults to be automatically reported. Each report meets 21 CFR Part 11 for auditability and tamperproof security.

RtPM handles Blackout Task Force Recommendations

17. Strengthen the NERC Compliance Enforcement Program.

A. Violation Reporting

Requires each regional council to report to the NERC Compliance Enforcement Program, within one month of occurrence, all “significant violations” of NERC operating policies, planning standards, and regional standards, whether verified or still under investigation by the regional council. (A “significant violation” is one that could directly reduce the integrity of, or otherwise cause unfavorable risk to the interconnected power systems.) In addition, each regional council is to report quarterly to NERC, in a format prescribed by NERC, all violations of NERC and regional reliability standards.

This is also an ideal RtReports application. The report format is user-configurable; data content is auditable and cannot be altered.

18. Support and strengthen NERC’s Reliability Readiness Audit Program.

A. Readiness Audits

In its February 10, 2004 directives, NERC indicated that it and the regional councils would jointly establish a program to audit the reliability readiness of all reliability coordinators and control areas within three years, continuing thereafter on a three-year cycle. Twenty audits of high-priority areas will be completed by June 30, 2004, with particular attention to deficiencies identified in the investigation of the August 14 blackout.

RtReports would require considerably less staff to execute this function. For example, the FERC OMTR is currently hiring 30 professional staff for that; using RtReports, staffing can be reduced considerably. In addition, 250 new FERC staff members in the OMOI (Office of Market Oversight and Investigation) have been assigned to provide real time oversight of the Energy markets.

20. Establish clear definitions for *normal*, *alert* and *emergency* operational system conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas under each condition.

The task force recommended designating three alternative system conditions (normal, alert, and emergency) to help grid managers avert and deal with emergencies through preventive action. Many difficult situations are avoidable by adhering strictly to sound procedures during normal operations. However, unanticipated difficulties short of an emergency still arise, and these must be addressed swiftly and skillfully to prevent emergencies. This requires a high level of situational awareness that is difficult to sustain indefinitely; therefore, an intermediate “alert” state between “normal” and “emergency” is needed. In some areas (e.g., NPCC) an “alert” state has already been established.

RtPM handles Blackout Task Force Recommendations

OSIsoft's RtAnalytics is well-suited for accomplishing this task. The limits on system reactive power and bus voltage can be checked automatically using a single ACE program running in RtAnalytics. The key concern is the persistence of the alarm condition. This is handled automatically for each alert by configuring the time the value exceeds the limit. For example, a high voltage bus could experience a dip in voltage for a period of up to N minutes without signaling an alert, but when the limit is exceeded by this amount, automatic alerts are triggered. Alarm calculations are often more complex, consisting of multiple independent variables, each with a different persistence. For example,

“Alarm if voltage less than 225K volts for more than 5 minutes, and if the reactive power flow is less than 200 MVAR for 10 minutes, and if the real power flow is greater than 300 MW for more than 25 minutes, or if the relative phase angle is greater than 45 degrees.” This alarm condition can be applied in RtAlarms, without programming.

The tool used to issue alerts is RtAlerts. This allows users to sign up for alerts interactively via standard web pages in RtPortal. System administrators may also configure alarms to be issued to different groups of individuals assigned to roles. Using this approach, all critical alerts would automatically be issued to the “right” individuals.

Additionally, since these alarms apply cross all buses, but with different conditions, the ACE context manager, coupled with the Module Database, supports all alarms of this type to be executed by one RtAnalytics executable module. This greatly reduces software maintenance costs.

21. Make more effective and wider use of system protection measures.

NERC will require each regional reliability council to evaluate the feasibility and benefits of under-voltage load shedding (UVLS) capability in load centers that could become unstable due to insufficient reactive power following credible multiple-contingency events. The regions should promote the installation of under-voltage load shedding capabilities within critical areas to prevent or contain an uncontrolled cascade of the power system.

Additionally, the Task Force recommended that NERC require regional study results to be provided to federal and state or provincial regulators at the same time that they are reported to NERC. NERC should require every entity with a new or existing UVLS program to have a well-documented set of guidelines for operators, specifying the conditions and triggers for UVLS use.

Load shedding algorithms in the past have been based on heuristic rules-of-thumb based on contingency analyses that use linearized network models. It is well known that these

RtPM handles Blackout Task Force Recommendations

models do not represent the grid under stressed conditions¹; hence other methods are suggested to determine when load shedding should be initiated.

One method in particular, developed by OSIsoft, uses real-time moving window FFTs. RtAlarms monitors peak heights of the spectrum to determine when those peaks grow in amplitude—clearly indicating grid instability.

22. Evaluate and adopt better real-time tools for operators and reliability coordinators.

Loss of situational awareness was a principal cause of the August 14 blackout. This was a result of inadequate reliability tools and backup capabilities. Failure of control computers and alarm systems contributed directly to the lack of situational awareness. Likewise, incomplete tool sets and the failure to supply state estimators with correct system data on August 14 contributed to the lack of situational awareness. The need for improved visualization capabilities over a wide geographic area has been a recurrent theme in blackout investigations. Some wide-area tools to aid situational awareness (e.g., real-time phasor measurement systems) have been tested in some regions but are not yet in general use. Improvements in this area will require significant new investments involving existing or emerging technologies.

A common theme in many real-time control situations is GIGO (Garbage In = Garbage Out). Multiple OSIsoft standard tool sets directly address this problem. One is called Sigmafine; another is the Statistical Quality Control package. Both are used extensively in the process control industry to determine if the data being used for both real-time and financial control are valid representations. Using Sigmafine, the system continually evaluates measurements relative to “material and energy balances”. Clearly these tools address the power grid, where Kirchoff’s laws directly apply. At buses, these tools can reveal whether measurements are compliant with these laws.

Sigmafine is especially good at determining the best estimate of measurements when: a) there are multiple measurements of the same variable; and b) measurements are missing and must be estimated.

The grid may be viewed using PowerWorld Viewer and data archived in the PI database. A utility company uses this system in their control room to show multidimensional information to their reliability coordinators. Such information provides coordinators and operators with real-time insight into the quality of the grid. It displays voltage, real or reactive power, or phase angles across the grid.

¹ Ilic, Marija and John Zaborszky, Dynamics and Control of Large Electric Power Systems, Wiley Interscience, New York, 2000, chapter 7.

23. Strengthen reactive power and voltage control practices in all NERC regions.

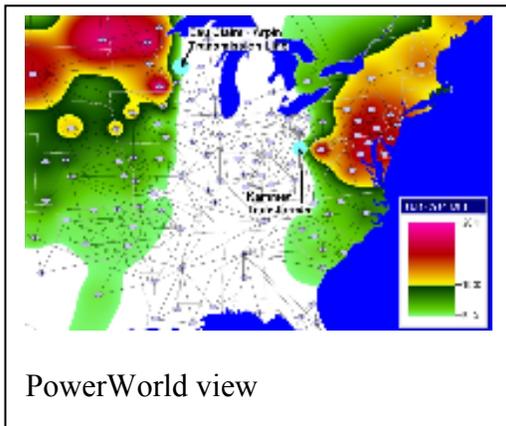
Reactive power problems were a significant factor in the August 14 outage, as well as in previous blackouts. Accordingly, the Task Force agreed that a comprehensive review is needed of North American practices with respect to managing reactive power requirements and maintaining appropriate balance among alternative types of reactive resources.

OSIsoft provides a number of standard interfaces to transmission grid monitoring devices. Such fully supported interfaces read data from primary instrumentation and send it to the PI archives.

24. Improve quality of system modeling data and data exchange practices.

The after-the-fact models developed to simulate August 14 conditions found that the dynamic modeling assumptions for generator and load power factors in regional planning and operating models are frequently inaccurate. In particular, assumptions of load power factor were overly optimistic; i.e., loads actually absorbed much more reactive power than indicated by pre-August 14 models. Another suspected problem concerns modeling of shunt capacitors under depressed voltage conditions.

Power flow and transient stability simulations should be periodically benchmarked with actual system events to validate model data. Viable load (including load power factor) and generator testing programs are necessary to improve agreement between power flows and dynamic simulations, and actual system performance. During the data collection phase of the blackout investigation, when control areas were asked for information pertaining to merchant generation within their area, the requested data was frequently not available. This was because the control area had not recorded the status or output of the generator at a given point in time. Some control area operators noted that existing data might be commercially sensitive or confidential. To correct such problems, the Task Force recommends that FERC and authorities in Canada require all generators, regardless



of ownership, to collect and submit generator data according to a regulator-approved template.

OSIsoft is a strong supporter of standards. We recommend that OPC-XML be adopted as the standard interface for generators to offer data. The IEC 61850 communications standards have been shown unable to handle more than 10,000 data points. With more than 16,000 generators in the US, each should be required to send angle, frequency, real power, reactive power,

voltage, and current on all three phases. This is far more than IEC 61850 can handle: hence our recommendation for OPC-XML In order to evaluate the models, accurate data from bus

measurements must be used. We suggest using Sigmafine as a tool to ensure data consistency.

25. NERC should reevaluate its existing reliability standards development process and accelerate the adoption of enforceable standards.

NERC is currently rewriting the reliability standards, in order to define common standards to apply across all councils and control areas. These could include monitoring automatically by a common RtAnalytics module. Such an approach would be fully automatic and would consider individual areas parametrically via the Module Database Properties. This allows static data to be associated with each function executed in real time. Thus, one software module could check for standards compliance, greatly improving the effectiveness of the monitoring process.

26. Tighten communications protocols, especially for communications during alerts and emergencies. Upgrade communication system hardware where appropriate.

On August 14, 2003, communications regarding conditions in northeastern Ohio were in some cases ineffective, unprofessional, and confusing. Ineffective communications contributed to a lack of situational awareness and precluded effective actions to prevent the cascade. Consistent application of effective communications protocols, particularly during alerts and emergencies, is essential to reliability. Standing hotline networks, or a functional equivalent, should be established for use in alerts and emergencies (as opposed to one-on-one phone calls) to ensure that all key parties are able to give and receive timely, accurate information.

RtMessenger™ is an ideal solution to this issue. The Microsoft LCS with RtMessenger configuration tools allows reliability coordinators and control area operators to automatically see and detect the presence of others in the same role. Role based assignments provide an easy method for communicating all live interactions between areas and regional councils in a fully documented, auditable manner. The communications are secure over a VPN circuit connecting all parties by role to a common portal.

OSIsoft RtPortal is also well suited to this application. RtPortal supports a rich set of online collaboration functions between regions, including sharing of documents, task lists, and other information in the form of Web-parts. We discuss more of this concept in later sections of this report.

27. Develop enforceable standards for transmission line ratings.

Inadequate vegetation management can lead to the loss of transmission lines even if those lines are not overloaded according to their rated limits. After allowing for regional or geographic differences, there is still significant variation in calculating the ratings of existing lines. This variation is expressed in terms of assumed ambient temperatures, wind speeds, conductor strength, and the purposes and duration of normal, seasonal, and emergency ratings. However the ratings themselves are unclear, inconsistent, and

RtPM handles Blackout Task Force Recommendations

unreliable across a region or between regions. This situation creates unnecessary, unacceptable uncertainties about the safe carrying capacity of individual lines on the transmission networks. Further, the appropriate use of dynamic line ratings must be included in this review; adjusting the rating of a line to reflect changes in ambient conditions may enable that line to carry a larger load and still meet safety requirements.

This recommendation clearly points to the need for a common standard to compute line ratings. This could be done in a single shared RtAnalytic routine taking into account seasonal, environmental, and age characteristics of the line.

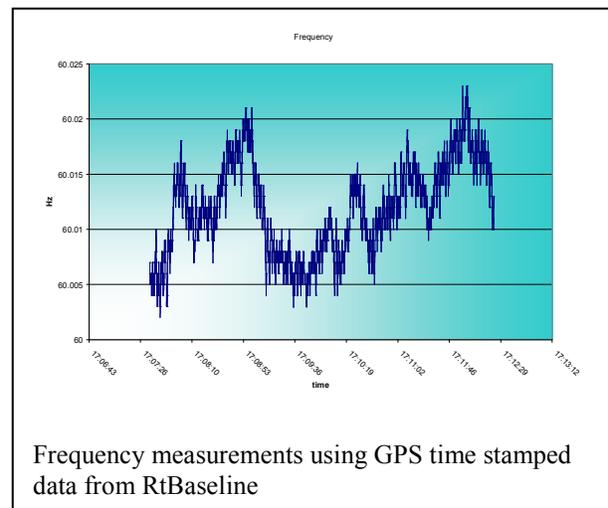
As discussed below, actual line impedance can be computed online using phasor measurements.

28. Require use of time-synchronized data recorders.

A valuable lesson from the August 14 blackout regards the importance of time-synchronized system data recorders. Task Force investigators labored over thousands of data items to determine the sequence of events, much like assembling small pieces of a very large puzzle. That process would have been significantly faster and easier had there been wider use of synchronized data-recording devices. NERC Planning Standard I., Disturbance Monitoring, requires the use of recording devices for disturbance analysis.

On August 14, time recorders were frequently used, but were not synchronized to a time standard. Today, at relatively modest cost, all digital fault recorders, digital event recorders, and power system disturbance recorders can and should be time-stamped at the point of observation using a Global Positioning System (GPS) synchronizing signal. Recording and time synchronization equipment should be monitored and calibrated to assure accuracy and reliability. It is also important that data from automation systems be retained for a minimum period for archiving, enabling analysis of particularly interesting events.

OSIsoft is the leading supplier of time-stamped data archiving systems, supporting real-time COMTRADE standard interfaces to both phasor measurement devices and digital fault recorders. The phasor measurement devices send GPS time-stamped data to standard supported OSIsoft interfaces, archiving data at rates up to 60 Hz. A common interface standard, IEEE 1344, reads data from native devices into RtBaseline. Users can then view high-rate data in real time, using standard RtWebparts or traditional smart-client applications such as ProcessBook and Datalink.



29. Evaluate and disseminate lessons learned during system restoration.

Efforts to restore the power system and customer service following the outage were generally effective, considering the massive amount of load lost and the large number of generators and transmission lines that tripped. Fortunately, restoration was aided by the ability to energize transmission from neighboring systems, thereby speeding the recovery. Despite the apparent success of the restoration effort, it is important to evaluate the results in more detail to compare them with previous blackout/restoration studies and determine opportunities for improvement. Black start and restoration plans are often developed through study of simulated conditions. Robust testing of live systems is difficult because of the risk of disturbing the system or interrupting customers. The August 14 blackout provides a valuable opportunity to review actual events and experiences to learn how to better prepare for system black start and restoration in the future. That opportunity should not be lost.

Blackstart time can be greatly reduced using on-line phasor measurement systems on the high side of the step-up transformer. This approach is currently being used by Entergy and other companies, including large manufacturing companies with internal generation.

The real-time phasor interfaces offered by OSIssoft fit this purpose. Note that the phasor measurement devices alone are not particularly useful, since it is phasor differences between the source and the loads that are critical. Thus, real-time phasor differences should be computed in RtBaseline and these values used for restoration.

30. Clarify criteria for identification of operationally critical facilities and improve dissemination of updated information on unplanned outages.

Lack of accurate, near real-time information about unplanned outages degraded the performance of state estimator and reliability assessment functions on August 14. NERC and the industry must improve the mechanisms for sharing outage information in the operating time horizon (e.g., 15 minutes or less), to ensure accurate, timely sharing of outage data needed by real-time operating tools. These include state estimators, real-time contingency analyzers, and other system-monitoring tools. Further, NERC's present operating policies do not adequately specify criteria for identifying critical facilities within reliability coordinator and control area footprints, whose operating status could affect the reliability of neighboring systems. This leads to uncertainty about which facilities should be monitored by both the reliability coordinator for the region in which the facility is located, and by one or more neighboring reliability coordinators.

RtPM is clearly of use in sharing data between reliability regions and control areas. We suggest using OPC-XML format, since it is an open, fully supported industrial-grade interface. Users could also elect to share data via PI-to-PI interfaces.

Yet another alternative is to make all critical real-time data available via secure Web services. This approach allows each reliability agency to automatically discover what real-time information is available in a different EMS data system. The agency can then

RtPM handles Blackout Task Force Recommendations

automatically request advice on all critical events, including major tie-line flows, voltages, and other real time occurrences.

31. Clarify that the transmission loading relief (TLR) process should not be used in situations involving an actual violation of an Operating Security Limit. Streamline the TLR process.

Reviews of control area and reliability coordinator transcripts from August 14 confirm that the TLR process is slow, cumbersome, and lacks predictability for situations in which an Operating Security Limit is close to or actually being violated. NERC should develop an alternative to TLRs that can quickly to address alert and emergency conditions.

This observation also pertains to tasks outlined above relating to online communications. RtMessenger™, RtAlerts, and RtAlarms™ directly address this issue. The OSLs must be known in real time by affected Regional Councils and control areas. Sharing data via RtWebparts will greatly streamline this process.

Group III. Physical and Cyber Security of North American Bulk Power Systems

32. Implement NERC IT standards.

Interviews and analyses indicate that within some of the companies interviewed, the potential exists for cyber system compromise of EMS and supporting IT infrastructure. Indications of procedural and technical IT management vulnerabilities were observed in some facilities, including unnecessary software services not denied by default, loosely controlled system access and perimeter control, poor patch and configuration management, and poor system security documentation. Analysis of prevalent policies and standards within the electricity sector revealed existing and expanding guidance on standards within the sector regarding IT and information security management. NERC issued a temporary standard (Urgent Action Standard 1200, Cyber Security) on August 14, 2003, and is developing the formal Reliability Standard 1300 for Cyber Security. Both start the industry down the correct path, but there remains a need to communicate and enforce these standards by providing the industry with implementation guidance. Such guidance regarding these sector-wide standards is especially important given that implementation procedures may differ among CAs and RCs.

OSIsoft's IT Monitor™ is very well-architected to address this recommendation, providing users with an instant footprint of the behavior of the entire IT infrastructure. This includes, data flow rates at all nodes via self-discovery of the network structure, automatic collection of performance monitors for all critical operating systems in the networks, and all traffic flow into and out of the corporate LAN/WAN.

Additionally, IT Monitor includes a number of statistical routines that determine the behavior of the IT system, including automatic recognition of deviation from expected

RtPM handles Blackout Task Force Recommendations

behavior. This is accomplished using standard RtAnalytics components, including SQC, X-Y, ProcessTemplates, and Rt-Batch™.

33. Develop and deploy IT management procedures.

In some instances, there were ill-defined and/or undefined procedures for EMS automation systems, software and hardware development, testing, deployment, and backup. In addition, there were specific instances of failures to perform system upgrade, version control, maintenance, rollback, and patch management tasks. At one CA, these procedural vulnerabilities were compounded by inadequate, out-of-date, or non-existing maintenance contracts with EMS vendors and contractors. This could lead to situations where grid operators alter EMS components without vendor notification or authorization, as well as scenarios in which grid operators are not aware of, or choose not to implement vendor-recommended patches and upgrades.

RtReports is the best tool to meet this recommendation. Today, users manage software assets much as they manage hardware assets. Many power companies use RtPM to monitor performance of power plants, substations, transmission lines, and so forth. Using RtReports to manage change control of software is a logical extension of the existing software functionality.

34. Develop corporate-level IT security governance and strategies.

In some organizations there is evidence of an inadequate security policy, governance model, strategy, or architecture for EMS automation systems. This is especially apparent with legacy EMS automation systems originally designed as stand-alone systems, but now interconnected with internal (corporate) and external (vendors, Open Access Same Time Information Systems [OASIS], RCs, Internet, and so forth) networks. For some interviewed organizations, however, this was not the case; in fact these appeared to excel in security policy, governance, strategy, and architecture. In order to address the finding described above, the Task Force recommends that CAs, RCs, and other grid-related organizations maintain a planned, documented security strategy, governance model and architecture for EMS automation systems. This should cover items such as network design, system design, security devices, access and authentication controls, and integrity management as well as backup, recovery, and contingency mechanisms.

As outlined in Task 33 recommendations, RtPM is an ideal tool for archiving time series actions related to IT security. This includes extensive use of the Module Database,, using its ability to communicate with standard relational databases via direct COM access or via Web Services.

35. Implement controls to manage system health, network monitoring, and incident management.

In some organizations there was ineffective monitoring and control over EMS supporting IT infrastructure and overall IT network health. In these cases, both grid operators and IT

RtPM handles Blackout Task Force Recommendations

support personnel did not have situational awareness of the health of the IT systems that provide grid information both globally and locally. This resulted in an inability to detect, assess, respond to, and recover from IT system-related cyber failures (failed hardware or software, malicious code, faulty configurations, and so forth) In order to address the finding described above, the Task Force recommends:

- IT and EMS support personnel implement technical controls to detect, respond to, and recover from system and network problems.
- Grid operators, dispatchers, and IT and EMS support personnel be provided with the tools and training to ensure that the health of IT systems is monitored and maintained.
- Systems incorporate the capability to be repaired and restored quickly, with minimum loss of time and/or access to global and internal grid information.
- Contingency and disaster recovery procedures be created and implemented where necessary to temporarily substitute during systems and communications failures when EMS automation system health is unknown or unreliable.
- Adequate verbal communication protocols and procedures exist between operators and IT and EMS support personnel, so that operators are aware of IT-related problems that may affect their situational awareness of the power grid.

This task can also be performed using the standard OSIsoft IT Monitor.

36. Initiate U.S.-Canada risk management study.

Effective risk management is a key element in assuring the reliability of our critical infrastructures. It is widely recognized that growing reliance on IT by critical infrastructure sectors, including the energy sector, has increased the vulnerability of these systems to cyber disruption. These joint assessments will serve to identify critical vulnerabilities, strengths and weaknesses, while promoting the sharing and transfer of knowledge and technology to the energy sector for self-assessment purposes.

A team of Canadian and American technical experts, using methodology developed by the Argonne National Laboratory in Chicago, Illinois, began conducting the pilot phase of this work in January 2004. The work involves a series of joint Canada-U.S. assessments of selected shared critical energy infrastructure along the Canada-U.S. border, including the electrical transmission lines and dams at Niagara Falls-Ontario and New York. The pilot phase was planned for completion by March 31, 2004. It was suggested that among the companies directly involved in the power outage, vulnerabilities and interdependencies of the electric system were not well understood, making for ineffective risk management. In some cases, risk assessments did not exist or were inadequate to support risk management and mitigation plans

OSIsoft demonstrated how to detect vulnerabilities of the grid based on real-time moving window FFTs. This approach was used on actual blackout data to demonstrate that the collapse of the grid was likely by early afternoon, August 14, 2004. This RtAnalytic module is available to help determine this issue.

37. Improve IT forensic and diagnostic capabilities.

In some cases, IT support personnel responsible for EMS automation systems are unable to perform forensic and diagnostic routines on those systems. This appears to stem from a lack of tools, documentation, and technical skills. It should be noted that some of the organizations interviewed excelled in this area but that overall performance was lacking. In order to address the finding described above, the Task Force recommends:

- CAs and RCs seek to improve internal forensic and diagnostic capabilities, as well as strengthen coordination with external EMS vendors and contractors who can assist in servicing EMS automation systems;
- CAs and RCs ensure that IT support personnel who support EMS automation systems are familiar with the systems' designs and implementations; and
- CAs and RCs ensure that IT support personnel who support EMS automation systems have access to and are trained in using appropriate tools for diagnostic and forensic analysis and remediation.

IT Monitor is the RtPM tool that ideally meets this requirement.

38. Assess IT risk and vulnerability at scheduled intervals.

Most of the organizations interviewed had some type of wireless and remote wireline intrusion and surveillance detection protocols as a standard security policy. Nevertheless, there is a need to improve and strengthen current capabilities regarding wireless and remote wireline intrusion and surveillance detection. Successful detection and monitoring of wireless and remote wireline access points and transmissions are critical to securing grid operations from a cyber security perspective. There is also evidence that although many of the organizations interviewed had strict policies against allowing wireless network access, they did not undertake periodic reviews to ensure compliance with these policies. IT Monitor is capable of implementing this recommendation.

40. Control access to operationally sensitive equipment.

The operationally sensitive computer equipment of some CAs and RCs was accessible to nonessential personnel. Although most of these personnel were escorted through sensitive areas, this procedure was not always enforced in everyday operations. In order to address the above finding, the Task Force recommended that:

- RCs and CAs develop policies and procedures to control access to sensitive equipment and/or work areas.
- Access be strictly limited to employees or contractors who utilize said equipment as part of their job responsibilities.
- Access for other staff to sensitive areas and/or equipment not directly involved in RC or CA operation (i.e., cleaning staff and other administrative personnel) is strictly controlled via escort and monitoring.

RtBaseline effectively monitors discrete events and the times they occur. Additionally, OSIsoft has an interface to mesh networking systems, known as “Dust Inc.” This uses proximity sensors as the basis node element, then automatically selects the best route back to the host computer. This technology is also used in power line carrier networks.

42. Confirm NERC ES-ISAC as the central point for sharing security information and analysis.

Currently, both private and public sector information-sharing and analysis initiatives are in place for reporting physical and cyber security incidents within the electricity sector.

In the private arena, NERC operates an Electricity Sector Information Sharing and Analysis Center (ES-ISAC) specifically to address this issue. On behalf of the U.S. Government, the Department of Homeland Security (DHS) operates the Information Analysis and Infrastructure Protection (IAIP) Directorate to collect, process, and act upon information about possible cyber and physical security threats and vulnerabilities.

In Canada, Public Safety and Emergency Preparedness Canada maintains a 24/7 operations center for reporting incidents involving or affecting critical infrastructure. In both Canada and the U.S., incidents of a criminal nature can be reported to jurisdictional law enforcement authorities. However, despite such private and public initiatives spanning physical and cyber security information sharing and analysis, an evaluation of electricity sector policies and procedures reveals uneven reporting of security incidents to internal corporate security, law enforcement, or government agencies across the sector. The fact that these existing channels for incident reporting—whether security- or electricity systems-related—are currently underutilized is an operating deficiency that can hamper the industry’s ability to address future problems in the electricity sector.

Interviews and analysis conducted by the SWG further indicate an absence of coherent, effective mechanisms for sharing of critical infrastructure information between private sector and government. Also, private sector infrastructure owners and grid operators lacked confidence that information shared with governments could be protected from disclosure under Canada’s Access to Information Act (ATIA) and the U.S. Freedom of Information Act (FOIA). In the U.S., however, the imminent implementation of the Critical Infrastructure Information (CII) Act of 2002 should mitigate almost all industry concerns about FOIA disclosure.

In Canada, Public Safety and Emergency Preparedness Canada relies on a range of mechanisms to protect sensitive information related to critical infrastructure that it receives from private sector stakeholders, including exemptions for third party information that currently exist in the ATIA and other instruments. At the same time, Public Safety and Emergency Preparedness Canada is reviewing options for stronger protection of CI information, including potential changes in legislation. Clearly, RtPM can handle this task for both NERC and the Department of Homeland Security.

43. Establish clear authority for physical and cyber security.

Some power entities did not implement best practices when organizing their security staff. In several organizations, Information System (IS) security staff reported to IT support personnel such as the Chief Information Officer (CIO). Best practices across the IT industry, including most large automated businesses, indicate that the ideal way to balance security requirements with IT and operational requirements is to place security at a comparable level within the organizational structure. By allowing the security staff a certain level of autonomy, management can balance the facility's risks and operational requirements. Clearly RtPM and IT Monitor represent the best practices in this area.

44. Develop procedures to prevent or mitigate inappropriate disclosure of information.

There was no evidence of the use of open source collection, elicitation or surveillance against CAs or RCs leading up to the August 14, 2003, power outage. However, such activities may be used by malicious individuals, groups, or nation states engaged in intelligence collection in order to gain insights or proprietary information on electric power system functions and capabilities. Open source collection is difficult to detect and thus is best countered through careful consideration by industry stakeholders of the extent and nature of publicly available information. Methods of elicitation and surveillance, by comparison, are more detectable activities and may be addressed through increased awareness and security training. In addition to prevention and detection, it is equally important that suspected or actual incidents of these intelligence collection activities be reported to government authorities. RtPM is an ideal tool to perform this function.

Group IV. Canadian Nuclear Power Sector

45. The Task Force recommends that the Canadian Nuclear Safety Commission request Ontario Power Generation and Bruce Power to review operating procedures and operator training associated with the use of adjuster rods.

Current operating procedures require independent checks of a reactor's systems by the reactor operator and control room supervisor before the reactor can be put in automatic mode, allowing reactors to operate at 60% power levels. Alternative procedures to allow reactors to run at 60% of power while waiting for the grid to be re-established may reduce other risks to the health and safety of Ontarians arising from loss of a key electricity source. CNSC oversight and approval of any changes in operating procedures would ensure that health and safety, security, or the environment are not compromised. The CNSC would assess the outcome of the proposed review to ensure that health and safety, security, and the environment would not be diminished as a result of any proposed action. Real-time monitoring of the adjuster rods by the use of RtPM and RtAnalytics will meet the requirements of this task.

46. The Task Force recommends that the Canadian Nuclear Safety Commission purchase and install backup generation equipment.

RtPM handles Blackout Task Force Recommendations

In order to ensure that the CNSC's Emergency Operations Center (EOC) is available and fully functional during an emergency situation—whether nuclear-related or otherwise—to support the safety of staff responders, the CNSC should maintain backup electrical generation equipment. This should have sufficient capacity to provide power to the EOC, telecommunications and Information Technology (IT) systems and accommodations for responding CNSC staff.

The U.S. and Canada's critical infrastructure sectors, including the energy industry, are increasingly vulnerable to computer attacks. Of particular concern are the supervisory control and data acquisition (SCADA) computer networks. In the power industry, these include status and control telemetry and energy management systems (EMS) handling protective relaying and automatic generation control. “These systems, many of which were intended to be isolated, now find themselves, for a variety of business and operation reasons, either directly or indirectly connected to the global Internet,” the task force report said. Tying the systems into the Internet to allow, for example, remote monitoring, presents security risks, including the “compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms,” the report added.

The task force's Security Working Group, which reviewed cyber security, found “indications of procedural and technical information technology management vulnerabilities, “including unnecessary software services, loosely controlled system access and perimeter control, poor patch and configuration management and poor system and security documentation.” The findings were based on interviews with a number of utilities.

The task force issued four recommendations. These include the development of industry-wide information technology standards; development and deployment of IT management procedures; development of corporate-level IT security governance and strategies; and the implementation of controls to manage system health, network monitoring, and incident management.

Appendix

Overview of Task Force Recommendations: Titles Only

Group I. Institutional Issues Related to Reliability

1. Make reliability standards mandatory and enforceable, with penalties for noncompliance.
2. Develop a regulator-approved funding mechanism for NERC and the regional reliability councils, to ensure their independence from the parties they oversee.
3. Strengthen the institutional framework for reliability management in North America.
4. Clarify that prudent expenditures and investments for bulk system reliability (including investments in new technologies) will be recoverable through transmission rates.
5. Track implementation of recommended actions to improve reliability.
6. FERC should not approve the operation of new RTOs or ISOs until they have met minimum functional requirements.
7. Require any entity operating as part of the bulk power system to be a member of a regional reliability council if it operates within the council's footprint.
8. Shield operators who initiate load shedding pursuant to approved guidelines from liability or retaliation.
9. Integrate a "reliability impact" consideration into the regulatory decision-making process.
10. Establish an independent source of reliability performance information.
11. Establish requirements for collection and reporting of data needed for post-blackout analyses.
12. Commission an independent study of the relationships among industry restructuring, competition, and reliability.
13. DOE should expand its research programs on reliability-related tools and technologies.
14. Establish a standing framework for the conduct of future blackout and disturbance investigations.

Group II. Support and Strengthen NERC's Actions of February 10, 2004

15. Correct the direct causes of the August 14, 2003 blackout.
16. Establish enforceable standards for maintenance of electrical clearances in right-of-way areas.
17. Strengthen the NERC Compliance Enforcement Program.
18. Support and strengthen NERC's Reliability Readiness Audit Program.
19. Improve near-term and long-term training and certification requirements for operators, reliability coordinators, and operator support staff.
20. Establish clear definitions for *normal*, *alert* and *emergency* operational system conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas under each condition.
21. Make more effective and wider use of system protection measures.
22. Evaluate and adopt better real-time tools for operators and reliability coordinators.
23. Strengthen reactive power and voltage control practices in all NERC regions.
24. Improve quality of system modeling data and data exchange practices.
25. NERC should reevaluate its existing reliability standards development process and accelerate the adoption of enforceable standards.
26. Tighten communications protocols, especially for communications during alerts and emergencies. Upgrade communication system hardware where appropriate.
27. Develop enforceable standards for transmission line ratings.
28. Require use of time-synchronized data recorders.
29. Evaluate and disseminate lessons learned during system restoration.

RtPM handles Blackout Task Force Recommendations

30. Clarify criteria for identification of operationally critical facilities, and improve dissemination of updated information on unplanned outages.
31. Clarify that the transmission loading relief (TLR) process should not be used in situations involving an actual violation of an Operating Security Limit. Streamline the TLR process.

Group III. Physical and Cyber Security of North American Bulk Power Systems

32. Implement NERC IT standards.
33. Develop and deploy IT management procedures.
34. Develop corporate-level IT security governance and strategies.
35. Implement controls to manage system health, network monitoring, and incident management.
36. Initiate U.S.-Canada risk management study.
37. Improve IT forensic and diagnostic capabilities.
38. Assess IT risk and vulnerability at scheduled intervals.
39. Develop capability to detect wireless and remote wireline intrusion and surveillance.
40. Control access to operationally sensitive equipment.
41. NERC should provide guidance on employee background checks.
42. Confirm NERC ES-ISAC as the central point for sharing security information and analysis.
43. Establish clear authority for physical and cyber security.
44. Develop procedures to prevent or mitigate inappropriate disclosure of information.

Group IV. Canadian Nuclear Power Sector

45. The Task Force recommends that the Canadian Nuclear Safety Commission request Ontario Power Generation and Bruce Power to review operating procedures and operator training associated with the use of adjuster rods.
46. The Task Force recommends that the Canadian Nuclear Safety Commission purchase and install backup generation equipment.