Texas Nodal:

High-level Architecture

April 14, 2006

Table of Contents

1. Document Goals and Intended Audience

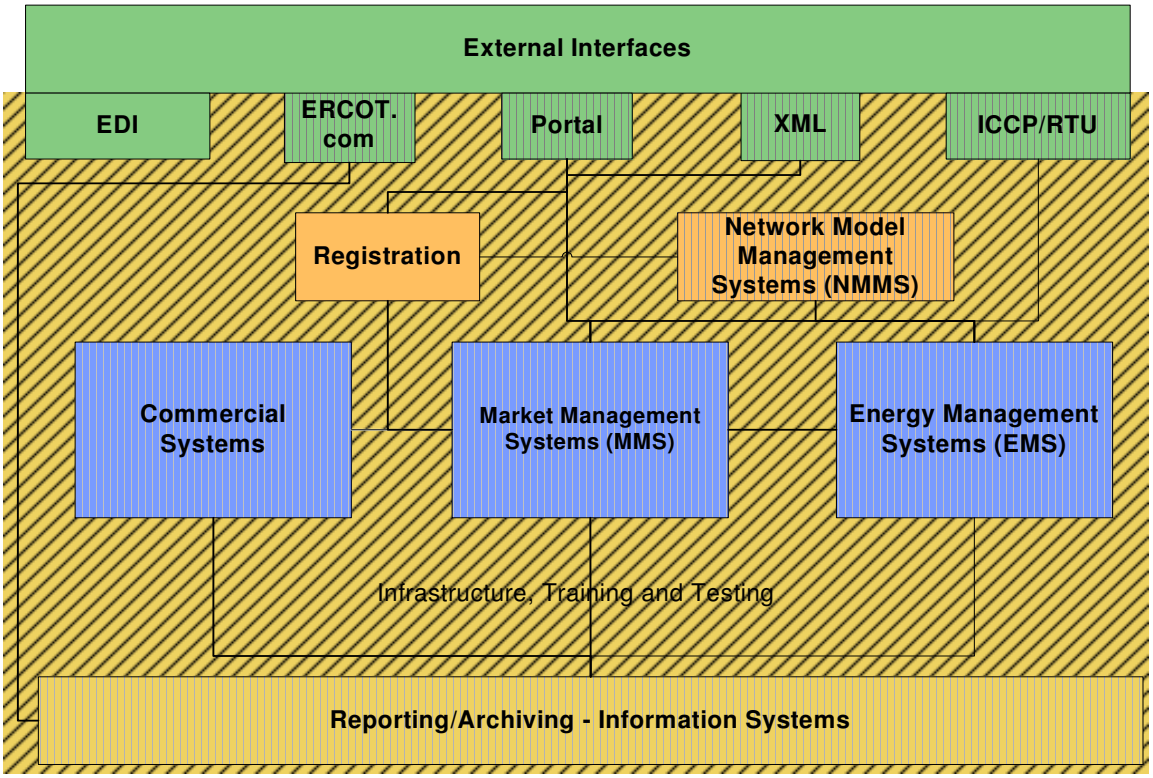
The goal of this document is to describe the major components of ERCOT systems in the Texas Nodal system and its interrelationships. This helps to frame discussions relating to system design.

The intended audiences are ERCOT Information Technology departments, relevant Market Participants and Texas Nodal Bidders.

2. System Overview

The Public Utilities Commission of Texas (PUCT) has determined that ERCOT will design and implement a transition from the current zonal market to the nodal market. The fundamental change is that Qualified Scheduling Entities (QSE) will submit bids and offers at the resource level instead of the portfolio level, and that market clearing prices will be calculated at the nodal level instead of the zonal level.

The main components of the wholesale market and grid operations are illustrated below:



In the diagram above, certain functionalities such as Load Forecast, Renewable Production Potential (RPP) Forecast, Security Constrained Economic Dispatch (SCED), Congestion Revenue Rights (CRR) Auction and Outage Scheduler may be procured from different vendors irrespective of the system that they are represented in (e.g. EMS, MMS).

The external interfaces communicate with the following groups of people: Market Participants (including Operators, Schedule/Tracker, Accounting/Finance, Support), PUCT and the public.

ERCOT provides infrastructure support to Compliance and Market Monitoring. Compliance refers to activities that monitor ERCOT and Market Participants' compliance to North American Electric Reliability Council (NERC), ERCOT Protocols, security standards and guidelines. Market Monitoring monitors the ERCOT markets.

3. Major Components of the System

Market participant entity relationships are defined in the registration process and propagated to the rest of the system. The NMMS serves as the repository of all power system network data from this process and this data is used in EMS, MMS and the Commercial Systems. The EMS is a mission-critical system designed to monitor and operate the electric power grid in a reliable manner. The MMS, also a real time mission-critical system, has a set of market clearing engines and a relational database housing the set of market rules (defined in the ERCOT protocols) to be used in operating and managing the ERCOT markets: Day Ahead Market (DAM), Real Time SCED/Locational Marginal Price Calculator, Supplementary Ancillary Services Market (SASM), Reliability Unit Commitment (RUC, both Day Ahead and Hour Ahead) and Congestion Revenue Rights (CRR) Auction. All the market clearing engines that use the network model in their calculations derive the model from the NMMS and EMS. The Outage Scheduler is also part of the MMS.

The Commercial systems include the Settlement and Billing system, that settles all the billing determinants (as defined in the ERCOT protocols) using data from MMS, Load Profiling & Aggregation, Metering and Renewable credit applications. The Credit Monitoring application within the Commercial systems evaluates the credit exposure for all participants and validates their credit against their limit to decide if the participant is qualified to participate in the market.

The EDW/EIS is the repository of all the archived data and provides extracts/reports for market participants, compliance reporting as well as market monitoring and market analysis.

The purpose of this document is to describe these components more in detail and identify the architectural requirements for each of them and their interfaces for data flow in the Texas Nodal Market. The following sections detail high-level components of the wholesale market and grid operations:

3.1. Registration

The registration system maintains the market participant information, including relational data between market participants. In the Nodal environment, asset registration (generators, controllable loads, interruptible loads, and high-set under frequency relay enabled loads) and data registration (breakers, transmission lines, etc) is managed by NMMS. Interfaces between NMMS and registration will facilitate the required cross-validation (ownership, etc.) and information transfer.

This system is the source of all the identified market drivers influencing the Texas market from players to assets. Data residing in this system will establish what has been verified and approved for market participation, and will feed into the NMMS, MMS and the Commercial Systems.

3.2. Network Model Management System (NMMS)

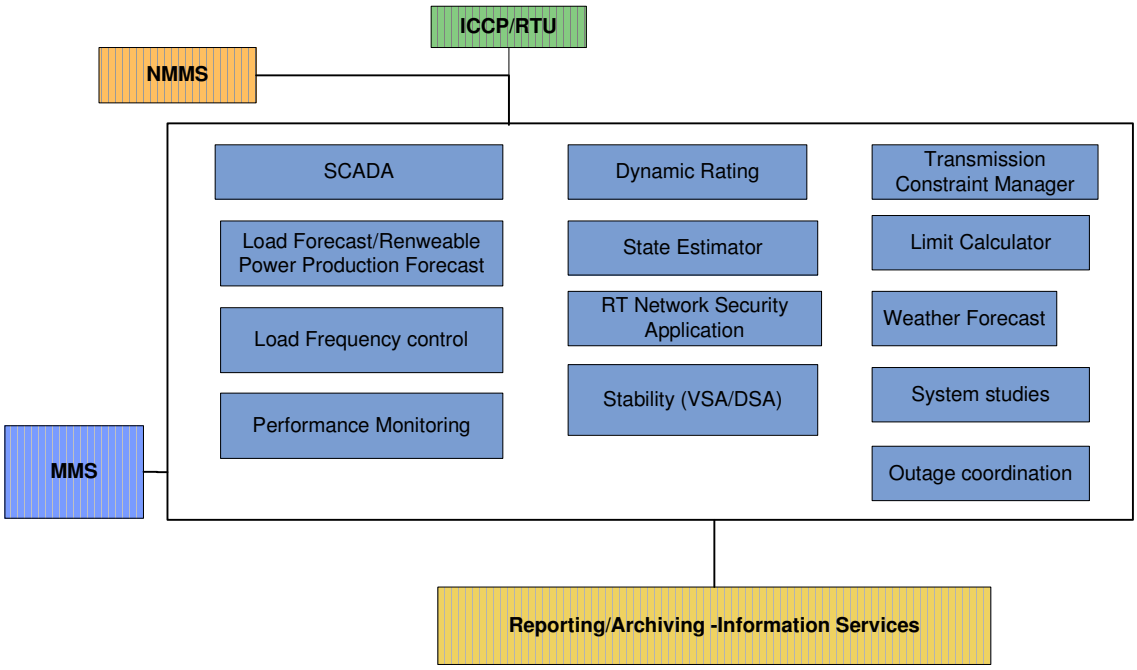
The purpose of the NMMS is to provide capabilities to input, edit network model data and validate the data for use in numerous applications as well as create network model cases to be used for annual planning, Congestion Revenue Rights auctions, Dynamic Simulation and Network Operations models; deploying these network cases to the production system so the model data can be used in the respective applications when the corresponding equipment is operational in the field.

The NMMS receives some Market Participant data from the Registration system and the network model is fed into the EMS for use in the respective applications and also posted on the Portal web site.

As previously mentioned, in the Nodal environment, asset and data registration is managed by NMMS and the interfaces between registration and NMMS will facilitate the required validation and information transfer.

3.3. Energy Management System (EMS)

The EMS supports two major application suites – 1) Real Time Applications, which are run as part of a Real Time Sequence that could be triggered either by a periodic or an event trigger and include Supervisory Control And Data Acquisition (SCADA), Load Forecast, Renewable Production Potential Forecast, Load Frequency Control, Performance Monitoring, State Estimator, Network Security Application, Stability Analysis; and 2) Study applications are run on demand by the operator/engineer to study certain specific system conditions and include Dispatcher Power Flow, Contingency Analysis, Transient Stability Analysis, Voltage Security Analysis, Transmission Outage Approval Study tool.



The major subcomponents of EMS are described below:

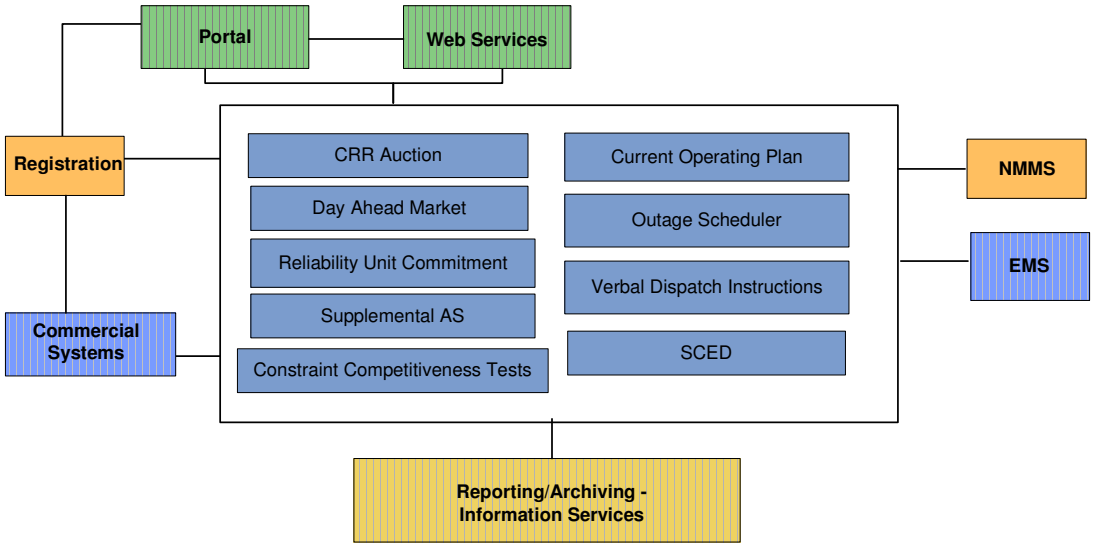
EMS Sub-Component	Functionality
Supervisory Control And Data Acquisition (SCADA)	The SCADA application periodically communicates with Market Participant systems either through the Inter-control Center Communication Protocol (ICCP) or Remote Terminal Units (RTU) directly. The SCADA performs the following functions: data collection, conversion, validation, alarm generation and event notification. Data received/sent includes Generation MW, MVAR; Load MW, MVAR; Flows on Transmission line and transformers; Close/Open status of breakers and switches etc.
Load Forecast	Load forecasts are provided with different levels of granularity for the next 2 years. The mid-term load forecast will predict hourly loads for the next 168 hours based on weather forecasts and historical loads. The long-term load forecast will predict minimum and maximum daily Load for the next 2 years. Both mid-term and long-term load forecast applications must have self-training mode to review historical load data and retrain the algorithms.
RPP Forecast	RPP Forecasts for Wind-powered Generation Resources (WGR) are used as an input into the Day-Ahead Reliability Unit Commitment (DRUC) and Hour-Ahead Reliability Unit Commitment (HRUC) through information provided by WGR Entities, meteorological information, and SCADA.
Load Frequency Control (LFC)	In the nodal environment, SCED runs every 5 minutes and calculates the unit Base points that are then telemetered to QSEs. Every 4 seconds, LFC calculates Area Control Error (ACE) based on the frequency error and comes up with regulation signals for the units participating in regulation (with bids). In accordance to ERCOT protocols, aggregated regulation signals will be sent to QSEs, which will then determine the relative participation of their units and communicate that information back to ERCOT.
Performance Monitoring	This measures the performance of ERCOT in terms of frequency control by calculating the L10 and Control Performance Standard 1 (CPS1) as per North America Electric Reliability Council (NERC) specifications. In addition, the performance of QSEs will be measured based on its providence of obligated ancillary services as agreed to support the frequency.

Dynamic Rating	This is used to calculate the transmission elements ratings based on temperature. There are two ways the ratings are established: a) Transmission Service Providers (TSP) provide them through SCADA to be used in the Real Time Sequence and b) TSPs provide look-up tables that are used in Study Applications.
State Estimator (SE)	The SE is used to filter redundant real time data, eliminate incorrect measurements, produce a reliable system state and contributes to the determination of power flows in parts of the system that are not directly metered. The functionality includes system-state estimation, state tracking, measurement anomaly detection/identification and network model validation.
Real Time Network Security Application	The Network Security Application identifies a set of transmission constraints (thermal, voltage, stability) that need to be included in the respective market clearing process. This includes using the Voltage Scheduler for real-time purposes.
Stability Analysis /Limit Calculator	Determine transfer capabilities along major transmission corridors subject to system voltage and angle stability as well as contingency and scheduled outage considerations. The Limit Calculator performs the same functions as the Voltage Stability Analysis tool (VSA) but has a look-ahead capability.
Weather Forecast	ERCOT procures weather information – actual and forecast values for a number of weather stations across Texas. This information is used in the load forecasting models and is made available to the Market Participants.
System Studies	System studies involve ERCOT engineers/operators performing various power flow/contingency analysis type studies for analysis purposes. This includes the use of Voltage Scheduler function.
Outage Coordination	Outage coordination involves ERCOT coordinators analyzing the impact of proposed outages and using the results to approve/disapprove outages.
Transmission Constraint Manager	The Transmission Constraint Manager performs the business function of the "gating" network – constraints from the Network Security Analysis application to SCED. ERCOT protocols require that operators examine each constraint prior to "gating" the constraint into the SCED.

3.4. Market Management System (MMS)

The Market Management System (MMS) primarily resides on a relational database with an Operator Interface and a Market Interface using a combination of Web browser and a XML interface. Day Ahead Market, Supplemental Ancillary service Market, Reliability Unit Commitment, Security Constrained Economic Dispatch and CRR Auction are the primary set of Market Analytical Functions used to perform market clearing. Current Operating Plan reflects anticipated operation conditions of each of the resources. The Outage Scheduler is a scheduling application used to coordinate scheduling of outages.

The MMS exchanges data with the Commercial Applications Systems for Registration and Settlements and the Enterprise Data Warehouse for archiving, and the MIS for data extract/report. All processes within MMS are highly fault-tolerant.

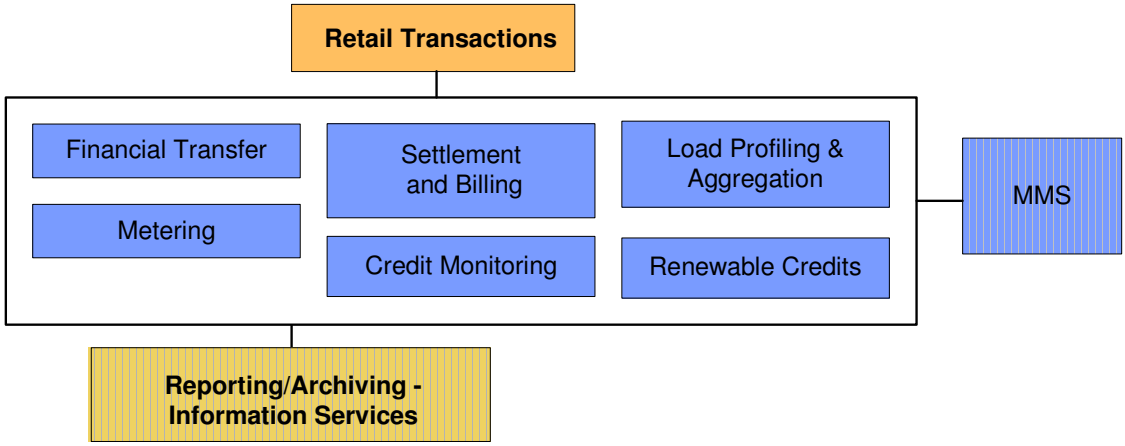


The major subcomponents of MMS are described below:

MMS Sub-Component	Functionality
Outage Scheduler	This facilitates submission and maintenance of transmission and resource outages. The market participants submit details of outage equipment through the XML/Portal interface.
Day Ahead Market (DAM)	The Day-Ahead Market (DAM) is a daily, co-optimized market in the Day-Ahead for Ancillary Service capacity, certain Congestion Revenue Rights, and forward financial energy transactions. Bids/offers are submitted through the market interfaces (programmatic and web-based). The awarded quantity and the prices from the market clearing engines are sent through the market interfaces back to the participants, and also to the Settlement and Billing system as well.
Supplementary Ancillary Service Market (SASM)	This market for supplementary ancillary service is run during the adjustment period and the creation of this market is based on the sole discretion of ERCOT under certain conditions that ERCOT deems necessary to create a SASM. Bids/offers are submitted through the XML/Portal interface. The awarded quantity and the prices from the market clearing engines are sent through the market interfaces to the participants and also sent to the Settlement system.
Reliability Unit Commitment (RUC)	The purpose of Reliability Unit Commitment (RUC) is to ensure that enough Resource capacity, in addition to Ancillary Service capacity, is committed in the right locations to reliably serve the forecasted Load. The Day-Ahead RUC (DRUC) is conducted at least once a day and the Hourly RUC (HRUC) is run at least once before each hour of the Operating Day. ERCOT, in its sole discretion, may conduct a RUC at any time to evaluate and resolve reliability issues. The DRUC must be run after the close of the Day-Ahead Market (DAM). The Bids/offers are submitted through the market interface. The awarded quantity and the prices from the market clearing engines are sent through the market interface to the participants and also sent to the Settlement system. RUC considers network constraints.
Current Operating Plan	The Current Operating Plan (COP) is primarily a data repository of the resource data provided by the QSEs on the various statuses of their resources. This data covers a time range of 7 days for each resource and is continuously updated.
Security Constrained Economic Dispatch (SCED)	The Security Constrained Economic Dispatch (SCED) process is designed to simultaneously manage energy balance and congestion through calculation of Resource Base Points and the Locational Marginal Prices (LMP) every five minutes. SCED process uses a two-step methodology that applies mitigation prospectively to resolve Non-Competitive Constraints. The SCED process evaluates Energy Offer Curves and Output Schedules to produce a least cost dispatch of On-Line Generation Resources to the total current generation output level, subject to transmission constraints.
Verbal Dispatch Instructions (VDI) & Emergency and Short Supply Operation	One of ERCOT's responsibilities is to maintain the reliability of the ERCOT grid. ERCOT shall utilize the market processes to the fullest extent to maintain the reliability of the grid. Under certain conditions when this is not possible, ERCOT shall utilize manual overrides to ensure grid reliability. Verbal Dispatch Instructions (VDI) is one of the methods used. Emergency and Short Supply Operations are procedural steps to be followed when Emergency and Short Supply conditions exist.
Congestion Revenue Rights Auction (CRR Auction)	The two main functions of the Congestion Revenue Rights (CRR) component is to auction the available network capacity of the ERCOT Transmission System that is not allocated to NOIE's, wind generation resources (WGR) or sold in previous auctions and to facilitate bilateral trading on the MIS. This component will use information from the CRR Network Model, offers and bids from market participates and auction rights. The auction must be a single-round, simultaneous auction and SFT's are run during the determination of the winning bids and offers. Credit limits are also considered by the auction system. The CRR component will need to be able to conduct annual auctions (for two year terms), monthly auctions and possibly a balance of the year auction. For each auction the CRR component provides CRR statements to the market participants and information to the Financial Transfer component.
Constraint Competitiveness Tests	This "tags" network constraints as "competitive" or not. These constraints are the contingency/limiting transmission element pairs that represent the Commercially Significant Constraints (CSCs) and Closely Related Elements (CREs) and will be defined immediately prior to the Texas Nodal Market Implementation date. The tests are to be performed annually, monthly, and daily. Any transmission element that passes the annual Competitiveness Test for every month of a particular year will be designated a Competitive Constraint. However, a Competitive Constraint may be temporarily treated as a Non-competitive Constraint for a particular month or day if it fails the Monthly or Daily Competitive Test. The reverse is true for a transmission element not designated as a Competitive Constraint in the Annual Competitive Test. The inputs to the Constraints Competitiveness Tests include CSCs, CREs and the monthly peak case. Planned Transmission and generation outages should also be included. The outputs for the Constraints Competitiveness Tests go to SCED and the MIS. Annual, monthly, and daily competitive tests are performed offline. The daily test is performed in the day ahead period and the final determination of Competitiveness Constraints is used in SCED in the operating day.

3.5. Commercial Systems

The main function of the Commercial Systems component is to calculate the payment and charges as well as generate the Settlement Statements and Invoices as prescribed by the protocols for both the DAM and RTM. The three main subcomponents with significant changes for the implementation of the Nodal market are Settlement and Billing, Financial Transfer and Credit Monitoring, as detailed below.

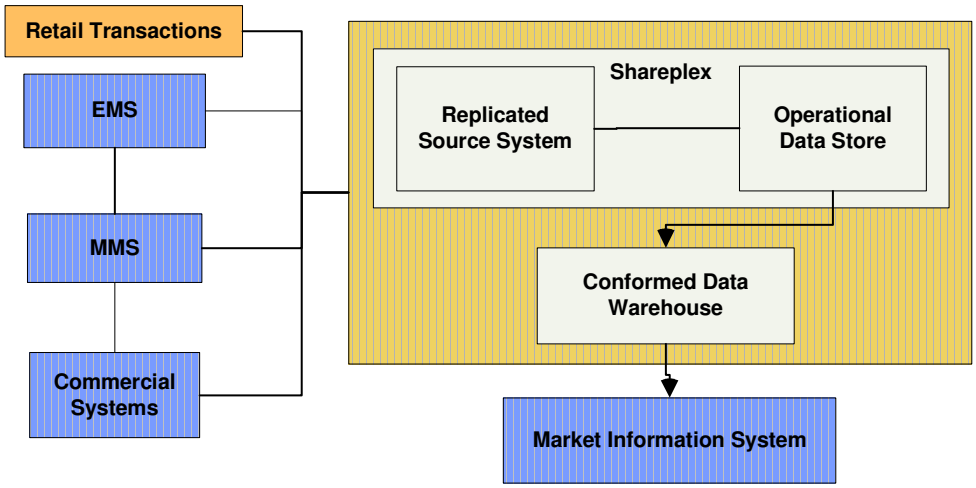


Commercial Systems Sub-Component	Functionality
Settlement and Billing	These Settlement Statements include payments and charges for CRR holders. The Settlement Statements and Invoices for the DAM are posted more or less the day after the operating day. In general, there is a DAM Statement and Invoice for each operating day and resettlement of the DAM should be very rare but can occur. Posting requirements for the Settlement Statements and Invoices for the RTM are similar to the current ERCOT zonal market. (i.e. initials, finals, true-ups and ad-hocs are expected and weekly invoicing is also specified in the Nodal Protocols) For each operating day about 80 different calculations will need to be executed in a batch process that runs each night. These calculations cover all the charges and payments for both the DAM and RTM including payments and charges to CRR holders and the end of month CRR balancing accounts. The charges and payments in the DAM and RTM include those for day-ahead energy, ancillary services, day-ahead RUC, hourly RUC, real-time energy, RMR, black start, supplemental ancillary services, and others. The Commercial Systems component includes a Financial Transfer component, which provides functions such as tracking payments, calculating short payments and late fees, as well as some data and calculations for Credit Monitoring.
Financial Transfer	The main function of the Financial Transfer component is to facilitate the financial transfers associated with the DAM Settlement Invoices, the RTM Settlement Invoices, the Settlement Late Fee invoices, CRR Auction invoices and other invoices. This component tracks the amounts due from market participants and applies their payments as they are received. It also, calculates late fees and generates Late Fee invoices. It also calculates the amounts that should be paid out to market participants incorporating the logic required in the event of short payments.
Credit Monitoring	The main functions of the Credit Monitoring and Management component are to determine and monitor Counter-Party Credit Exposure, issue real-time alerts to market participants who exceed credit limits (that impact participation in CRR/DAM markets) and perform credit analysis and generate credit reports.

3.6. Enterprise Information Services (EIS)

Enterprise Information Services (EIS) is the component that receives information from systems such as EMS and MMS and prepares the information for the Conformed Data Warehouse archiving. The information is then available for use in generating reports and extracts by the Market Information System. The changes in the definition of the information received will require modifications to the data structures.

EIS uses Oracle DataGuard and Quest SharePlex as its technology infrastructure and involves a large number of read and write transactions as the information flows and is processed:

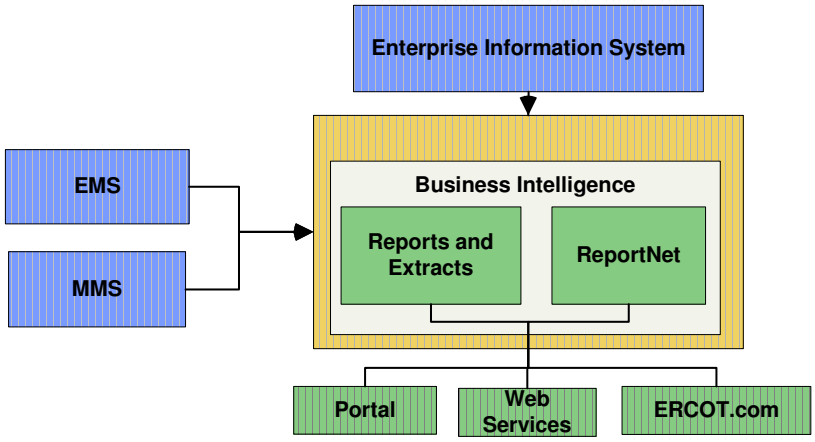


EIS Sub-Component	Description
Source System Replication (SSR)	Near real-time replication of source side systems, capturing required intra-day transactions (inserts, updates, and deletes)
Operational Data Store (ODS)	This system is used as a source archive, an integration environment for data warehouse data marts and an integrated environment for reporting on historical source information.
Conformed Data Warehouse	A conformed data warehouse is the union of all data marts. A data mart is a flexible set of data, ideally based on the most atomic data possible to extract from an operational source, and presented in a symmetric (dimensional) model that is most resilient when faced with unexpected user queries. Data marts can be tied together using drill-across techniques when their dimensions are conformed. In its simplistic form, a data mart represents data from a single business process.

3.7. Market Information System

The Market Information System (MIS) retrieves information from the data warehouse, operational data store, and when required, deliver information to the public and Market Participants.

MIS uses a variety of technology platforms including: Cognos ReportNet, Oracle custom code, internal and vendor developed report builders, for example. It also makes use of the Market Information Delivery system and the Market Information Repository.



MIS Sub-Component	Description
Business Intelligence	A standardized layer of business logic used to answer business questions about information in the source systems.
Data Extraction	Based on both Protocol and Market expectations, information from our source systems is transferred directly to them, typically as it is stored in its relational format. This allows the Market to simulate ERCOT systems and study information locally within their systems.
Reporting	Reporting environment for internal, the PUCT, and the Market (under review). The Reports and Extracts sub component refers to the preprogrammed information feeds that go to the Market Participants, PUCT, and the public. This subcomponent encompasses a wide range of tools.

4. Hardware Conceptual Design

This section provides a list of Server Processor types (Application, Web and Database), performance, scalability, capacity and Disaster Recovery details for the components.

For estimating purposes three different server levels have been defined:

Characteristics	Server A	Server B	Server C
I/O Bandwidth (Internal)	High	Medium	Low
I/O Bandwidth (External)	High	Medium	Low
Transactional Load	High	High	Medium
Analytical Load	High	Medium	Low
Floating Point	High	High	Low
Examples of Processor Types	IA64 (Itanium2), RISC	EM64T, Opteron, Virtual	EM64T, Opteron, Virtual
Max Processing Sockets	64	4	2
Max Processing Cores	128	8	4
Logical Configuration	Multi-Node Clusters	Multi-Node Clusters Distributed Parallel Processing Standalone	Multi-Node Clusters Distributed Parallel Processing Standalone
Node Types	Cells	Standalone Virtual Machines	Standalone Virtual Machines

5. Information Security

The purpose of this section is to describe the high-level security architecture of the ERCOT IT systems and their interrelationships. This is to help frame the development of a secure design for the IT systems as ERCOT migrates to the Texas nodal market through the market redesign process.

5.1. Definition

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected environment of ERCOT, the Market Participants, and the Texas Public Utilities Commission. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail.

The regulatory and industry standards for ERCOT's market redesign effort are the North America Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards (CSS) and the ISO 17799 Information Technology — Security Techniques — Code of Practice For Information Security Management.

The security design must address the following aspects:

- Robust Security Architecture – The increased data volume and computational performance expectation of the Nodal Market will require an approach that includes systems robust enough to accomplish the protection without negatively impacting the necessary data processing and delivery.
- Increased User complexity – The increased scope of the Nodal Market will result in an increased demand for user and system level access to data. This increased access will incur the need for additional controls for networks, systems, applications and information.

5.2. Information Security Process

The information security process consists of four stages: risk assessment, establishing security requirements, selecting controls, and implementing controls.

5.2.1. Risk Assessment

All systems will require a security risk assessment. From the risk assessment, the necessary controls can be identified to ensure that the systems are adequately protected from violation of confidentiality, integrity and availability requirements.

5.2.2. Establish Security Requirements

ERCOT must review all planned information system implementations for the Texas Nodal Market Redesign effort to identify the security requirements that must be met by all components of that system. Therefore, all systems will need to be carefully assessed for risk, threat environment and appropriate controls to ensure that the most effective

use of limited resources is applied to the Security effort. Certain security requirements have been and are being developed as ERCOT policies and standards, notably, CP-6 Information Protection Policy, Information Classification (in draft), and Application Security Standard (in draft) and requirements.

5.2.3. Select Controls

Upon determination of risk and identification of security requirements, the most appropriate controls must be selected to ensure that the risk is mitigated to the maximum possible level without impairment of functionality or required access. Some examples of controls are:

- Security Policies – All controls begin with policies that document the responsibilities of various entities to accomplish the specific control or groups of controls.
- Authentication – the identification of a user (defined as either a person or an application) that requires access to data.
- Access Control – the limitation of data or control access to that necessary to accomplishment of the required function (again applies to both persons or applications), the required regular review of such access by the approver, and the audit trail documenting the granting and reviews of the access.
- Separation of Duties – the requirement that no one person has authority over a control. As an example, the approval of access will not be granted by the same person, one person is an approver and there must be a different person to actually configure that access.
- Documentation and Audit Trails – the enumeration of the design and implementation of all systems showing logical progression from initial idea to decommissioning of the system and all modifications of that system over its life. This documentation is necessary for security audit compliance and is a component of a Systems Development Life Cycle Methodology that is, in and of itself, a necessary control.
- Information Classification – determination of the relative value, and therefore the risk to the enterprise, of data from which the appropriate security control systems can be identified an applied.

5.2.4. Implement Controls

Policies

The policy that drives the ERCOT Information Security Architecture is the Information Protection Policy and is the guiding principle for this and all follow-on documents. Standards which are derived from the requirements of this policy (primarily the protection of and controls over the granting access to information entrusted to ERCOT), the NERC CIP Cyber Security Standards and ISO 17799.

At present, there are several standards being developed that will apply to ERCOT and, thus, the Market Redesign effort, The Data Classification, Application Security and Network Security Standards. Additional standards will be applied as they are developed and approved. It is expected that there will be a WAN Security Standard, an Internet Security Standard, an Email Standard and an Encryption Standard developed in the next few months and all will be applied to both the present ERCOT IT infrastructure and the Market Redesign effort. The associated requirements documents for each of these standards will identify the appropriate controls.

These Standard documents, their associated requirements, procedures and guideline documents will act as the guiding principles for security of the Market Redesign effort.

Asset Management

All information technology systems consist of assets (for example the IT Network can be classified as an asset that is defined by all of its components) such as software, hardware and data. All assets will be identified in a system of record (prior to implementation), owned by an individual responsible for the appropriate acquisition, implementation, maintenance and decommissioning of that asset. All events (security or otherwise) that involve that asset will be documented.

Network Security

As the network is the primary conduit of all data conveyance and processing, security is of paramount importance. All systems designed, implemented and operated at ERCOT will be developed to ensure that security, consistent with proper functionality and performance is, inherently, a component of that system.

Information Protection
The IT Infrastructure will implement all necessary procedures to ensure that information, in transit, at rest, stored on and off site is protected to the level necessary to ensure that potential damage to either ERCOT or the Market Participants is prevented to the extent possible with well designed technology, processes and procedures.

Access Controls
Access control rules and rights for each user or group of users must be clearly defined as part of the market redesign effort. Access controls are both logical and physical and these will be considered together. Access contains the inherent risk that it can be abused and the use of appropriate controls limits the potential damage that can result from granting of inappropriate access.

User Access Management
User access management covers all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. A functional and reliable system of user access management is critical to ensuring a secure and manageable IT infrastructure.

Technical Vulnerability Management
Technical vulnerability management will be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations will include network components, operating systems, and all applications in use.

5.3. Applicable Security Standards

Industry security standards:

1. North America Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards: NERC website details
2. ISO 17799: Details on ISO website

ERCOT security policies and standards:

1. Information Protection Policy
2. Information Classification Standard
3. Application Security Standard (in approval)
4. Network Security Standard (in approval)
5. Email Standard (in development)
6. Encryption Standard (in development)