City of Houston Wastewater Treatment Systems
Implementation of Hurricanes Katrina and Rita 'Lessons Learned'
SCADA Disaster Recovery Center (DRC)

Author:
Yehuda Morag
CH2M HILL
12301 Research Blvd., Bldg. 4, Suite 250
Austin, Texas 78759

Co-Author:
Hoss Forouzan
City of Houston, PW&E
4545 Groveway Drive
Houston, Texas, 77087

ABSTRACT

They are nature's fiercest storms—huge, whirling tempests that form out at sea, armed with winds in excess of 74 miles an hour, and when these hurricanes make landfall, the effects are frequently devastating. Hurricane Katrina formed in mid-August over the Bahamas, it became a tropical storm on August 24 and reached hurricane intensity before making landfall in south Florida as a minimal hurricane. A few hours later, the storm entered the Gulf of Mexico and intensified rapidly into a Category 5 hurricane while crossing the Loop Current on August 28. Katrina made landfall on August 29 near the mouth of the Mississippi River as an extremely large Category 3 hurricane. Storm surge caused catastrophic damage along the coastlines of Louisiana, Mississippi, and Alabama. Levees separating Lake Pontchartrain from New Orleans, Louisiana were breached by the surge, ultimately flooding about 80% of the city, flooding countless homes, leaving millions of people without power, and forcing the closure of many city services, including water and wastewater. Wind damage was reported well inland, impeding relief efforts. Katrina is estimated to be responsible for at least $81.2 billion in damages, making it the costliest natural disaster in U.S. history. It was the deadliest U.S. hurricane since the 1928 Okeechobee Hurricane, killing at least 1,836 people

Following behind was Hurricane Rita, the fourth-most intense Atlantic hurricane ever recorded and the most intense tropical cyclone ever observed in the Gulf of Mexico. Rita caused $10 billion in damage on the U.S. Gulf Coast in September 2005. Rita was the

seventeenth named storm, tenth hurricane, fifth major hurricane, and third Category 5 hurricane of the 2005 Atlantic hurricane season.

Rita made landfall on September 24, 2005 near the Texas-Louisiana border as a Category 3 hurricane on the Saffir-Simpson Hurricane Scale. It continued on through parts of southeast Texas. The storm surge caused extensive damage along the Louisiana and extreme southeastern Texas coasts and completely destroyed some coastal communities. The storm killed seven people directly; many others died in evacuations and from indirect effects.

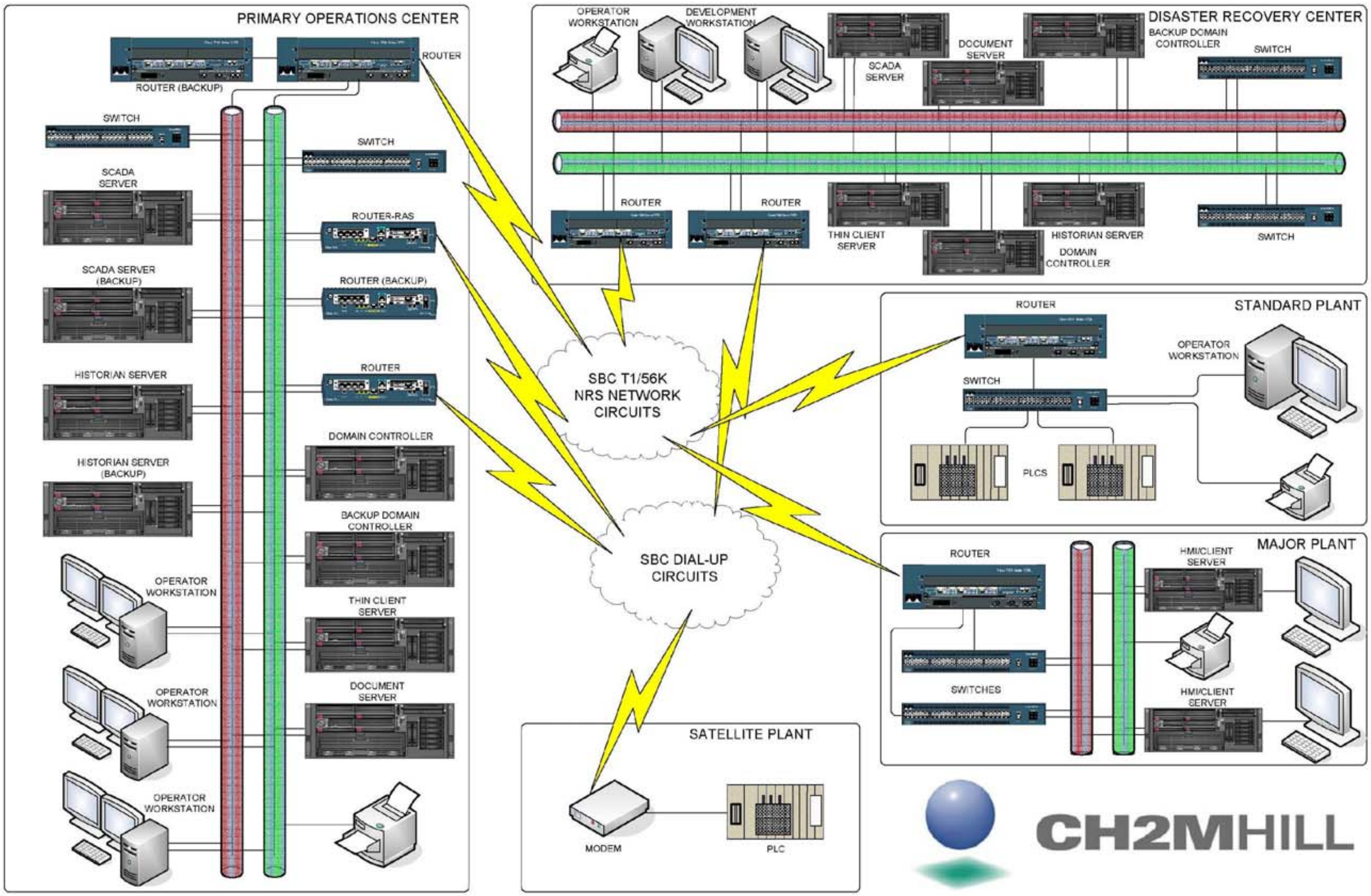
Following last year's hurricane season, the City of Houston's Public Works & Engineering, Wastewater Operations was determined to upgrade the design and implementation of the Disaster Recovery Center (DRC) system of the wastewater control center. The newly designed DRC system is intended to take-over all the necessary operations, control, and data gathering required to continue wastewater services in Houston in case of a major catastrophe such as unexpected flood, fire, or terror act that will prevent the SCADA control center from operating.

The DRC is an essential part of any small or large utility. It allows for rapid and planned recovery of vital services for the public until the failed permanent system is repaired and decommissioned.

The newly installed DRC has all the functionality of the existing SCADA control center, including the necessary hardware to access and control all of the City's WWTPs and field devices, but without the full redundancy and the enhanced functionality of the SCADA control center. The DRC configuration is intended to serve the City of Houston Wastewater Operations for a short duration (from a few hours up to six months) of full operation.

The DRC design and implementation includes the instructions and planning of routine switch-over exercises to ensure that the wastewater operations control and data acquisition systems work and that involved personnel are familiar with the pertaining switch-over SOP's.

To reduce the cost of the DRC system, certain City of Houston existing computer hardware such as servers, workstations, and software applications have been re-utilized, however a sophisticated communication system (routers, networking circuits, and configuration) were added for higher reliability and better cyber security.


PRIMARY OPERATIONS CENTER
ROUTER (BACKUP)
ROUTER
SWITCH
SWITCH
SCADA SERVER
ROUTER-RAS
SCADA SERVER (BACKUP)
ROUTER (BACKUP)
HISTORIAN SERVER
ROUTER
DOMAIN CONTROLLER
HISTORIAN SERVER (BACKUP)
BACKUP DOMAIN CONTROLLER
OPERATOR WORKSTATION
THIN CLIENT SERVER
OPERATOR WORKSTATION
DOCUMENT SERVER
OPERATOR WORKSTATION
DISASTER RECOVERY CENTER
OPERATOR WORKSTATION
DEVELOPMENT WORKSTATION
SCADA SERVER
DOCUMENT SERVER
BACKUP DOMAIN CONTROLLER
SWITCH
ROUTER
ROUTER
THIN CLIENT SERVER
HISTORIAN SERVER
DOMAIN CONTROLLER
SWITCH
SBC T1/56K NRS NETWORK CIRCUITS
SBC DIAL-UP CIRCUITS
STANDARD PLANT
ROUTER
SWITCH
OPERATOR WORKSTATION
PLCS
MAJOR PLANT
ROUTER
HMI/CLIENT SERVER
SWITCHES
HMI/CLIENT SERVER
SATELLITE PLANT
MODEM
PLC

CH2MHILL

KEYWORDS and ACRONYMS

- **BIA (Business Impact Analysis)—**An Analysis of an Information Technology or SCADA systems requirement, process, and interdependencies used to characterize system contingency requirements and priorities in the event of significant disruption.
- **CP (Contingency Plan)—**Management policy and procedures designed to maintain or restore SCADA operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- **COOP (Continuity of Operations Plan)—**A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained as a result of a disaster event before returning to normal operations.
- **DCS (Distributed Control System)—**A comprehensive hardware and software package, supplied by one single manufacturer, that encompasses the functionality required to implement control and data acquisition functions. Includes continuous and batch control software, standard hardware redundancy, operator interface terminals (OITs), communication capabilities to other digital systems, graphics screen development, alarming, historical data collection, trending, report generation packages, and more.
- **DRC (Disaster Recovery Center)—**A backup computer monitoring and control center that assumes full operation upon major failure or disruption of the primary SCADA operation center. The DRC facility can be designed as Cold site, Warm site, Hot site, mobile or fully mirrored site.
- **EOC (Emergency Operations Center)—**An alternate monitoring and control site, to be activated during disaster or major service disruption. This site might not have all the computer capabilities of the primary operations center.
- **FMCS (Facility Monitoring and Control System)—**A system that integrates one or more SCADA systems with the customer's business process and that incorporates the acquired control system data into the customer's business environment for accounting, managerial decision process, engineering studies, data publishing, and more.

- **HMI (Human Machine Interface)—**A device that allows the operator to interface with the digital control system. Includes a display unit with an interactive graphics software and keyboard, as separate or combined units.
- **IS (Information System)—**A system that uses information technology to capture, transmit, store, retrieve, manipulate, or display information used in one or more of corporate businesses, engineering, or control processes.
- **IT (Information Technology)—**The hardware and software that make the information system possible. Hardware refers to the devices, such computers, workstations, physical networks, and data storage and transmission devices, involved in processing information. Software refers to the computer programs that interpret user inputs and that commands the hardware operations.
- **OIT (Operator Interface Terminal)—**The human machine interface in a digital system that utilizes a display unit and a keyboard or similar input device for the operator’s display and control.
- **PDD-63 (Presidential Decision Directive 63)** - Critical Infrastructure Protection to achieve and maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of state and local governments to maintain order and to deliver minimum essential public services.
- **PLC (Programmable Logic Controller)—**The hardware and software combination that encompasses both control and data acquisition functions. A typical PLC architecture consists of a processor or processors and an I/O system, in most cases on common rack. In many ways, the PLC is similar to the controller module of a DCS; however, it is designed as a stand-alone device.
- **SCADA (Supervisory Control and Data Acquisition)—**A system that gathers, acquires, and sends information to remote sites. It is supervisory in nature because it is not solely responsible for the primary control functions. In most instances, some other system is implementing the primary control, and the SCADA system monitors and logs activity and interfaces with the primary controllers by sending set-points or calculated values.

- **SI (System Integrator)—**A person or a group of people responsible for the interconnection and the interaction of multiple hardware and software modules to form a single common system. The hardware and the software are usually from variety of different manufacturers.
- **SIDG (System Integration Design Guide)—**The guidance for the design and implementation of the SCADA system. Focused on the seamless systems integration, automation, and scalability. The SIDG sets the project's standards for tag naming, file naming, and equipment and nodes domain name conventions; HMI graphic STD definitions; and PLC and HMI programming templates for lower programming and troubleshooting costs.

INTRODUCTION

SCADA systems monitoring and controlling the City Water and Wastewater systems are expected to function without any disruptions, however several planned (preventive maintenance) or unplanned (short term power outage, equipment failure) system shutdowns might occur periodically, and in most cases those system's operations are restored in a short time.

While many SCADA system vulnerabilities can be reduced or eliminated using the proper engineering design, technical, and operational procedures, some severe disruptions caused by natural disasters, terrorist attack, or large accident (fire, toxic gas evaporation, train derailment, etc) require the City to prepare an effective contingency plan. The execution of this plan includes SCADA Disaster Recovery Centers (DRC) / Emergency Operation Centers (EOC), testing and exercising, training, and auditing and updating the contingency plan and policy.

This paper will discuss the steps taken by the City of Houston to design, construct, and maintain the Wastewater SCADA Disaster Recovery Center to respond to future severe system disruptions caused by natural disasters, terrorist attack, or large accidents, and the lessons learned following the 2005 Atlantic hurricane season.

Several steps were taken to accomplish this task:

1. **Develop SCADA Emergency Plan Policy:** Provide the guidance necessary to develop the required DRC design and operation planning.
2. **Conduct Business Impact Analysis:** Identify and prioritize the critical SCADA systems and components to take part of the DRC. Make sure that the DRC responds to the City's needs and that it is being executed in a cost effective manner.
3. **Develop Recovery Strategy and Operation Procedures:** To ensure that the designed DRC systems are capable of switching over when required, that the DRC is ready to assume full operation when needed, and that detailed guidance and procedures to run the DRC are in place.
4. **DRC Testing, Personnel Training and Plan Exercise:** Periodic DRC testing can identify systems' preparedness. Training will have DRC personnel ready for

immediate activation and switchover. Both activities improve the City's effectiveness to respond during severe wastewater systems disruptions.

5. **DRC Plan Maintenance:** Both the DRC SCADA systems and the operations procedures should be updated regularly to stay current with system enhancements.

CITY OF HOUSTON DRC

1. Develop SCADA Emergency Plan Policy

City of Houston Wastewater SCADA contingency planning included the tasks to identify threats and vulnerabilities that might shut down the SCADA system and prevent the City from operating the wastewater system securely and effectively. Those threats were classified as:

- Natural – Hurricane, tornado, flood, and fire.
- Human – Operator error, implant of malicious code (computer virus), sabotage, and terrorist attacks.
- Environmental – Power failure, SCADA system failure (hardware or software), and telecommunication network failure.

The City felt that the current SCADA system design and the procedures in place can respond to the environmental listed threats and most of the human errors; however the City was very concerned with the natural disasters affects and the ramification of any terrorist attack on the central SCADA system.

Various types of contingency plans were studied; however the COOP (Continuity of Operation Plan) was adapted, customized for the City's wastewater operations, and developed to match the currently operating SCADA system.

The COOP was selected, as it focuses on restoring the wastewater SCADA essential functions at alternate sites and performs the necessary functions for a certain period of time before returning to normal operations. The COOP was also chosen because it addresses the City Center of Operations model requirements on one hand, and is developed and executed independently from the BCP (Business Continuity Plan) that applies to general City services and the IT system on the other. Because the COOP emphasizes the recovery of the SCADA operational capability at an alternate site, the plan intentionally does not include the City's IT operations. In addition, minor disruptions such as short term power failure or local communication failure that do not require relocation to an alternate site were taken into consideration, and therefore were not addressed.

In accordance with PDD-63, Critical Infrastructure Protection, COOP plans for systems that are critical to supporting the nation's infrastructure are to be in place by May 2003.

Once it was established that the DRC design would follow the COOP standards, the System Development Life Cycle (SDLC) was examined to reduce the overall contingency planning costs, to enhance contingency capabilities, and to reduce the impacts to system operations when the contingency plan is implemented.

- **Initiation Phase.** During the initiation phase, DRC system requirements were identified and matched to the City wastewater SCADA operational processes. The DRC system requires very high availability therefore redundant, real-time mirroring at an alternate site and fail-over capabilities were built into the system design. During this phase, the new DRC system was also evaluated against other existing and planned SCADA and communications systems to determine its appropriate switch over and recovery procedures.
- **Development/Acquisition Phase.** During the design phase significant emphasis was given to the redundancy and robustness of the DRC system architecture to optimize reliability, maintainability, and availability during the operation/maintenance phase. By incorporating those factors into the early stages of the DRC design, implementation costs were reduced and issues relating to future planned system upgrades (mainly replacing the current OS from Unix-based to an MS-based SCADA open architecture system) were dealt with as well. Continuous data replication and mirroring was planned to take place to ensure that the DRC was ready to take over when needed. DRC data communication system reliability and availability were one of the major concerns during the design phase, as the City wastewater SCADA communications components, services and paths had to be carefully examined. SCADA power supply systems (regular feed and UPS) had to be reviewed and appropriately sized for load balancing.
- **Implementation Phase.** The City of Houston Wastewater SCADA DRC system implementation was actually planned to be accomplished in two steps. The initial implementation phase included the installation of the DRC with new and upgraded

communication components but utilized mostly spare City SCADA equipment currently installed at various wastewater treatment plants. By doing so, the initial cost of the DRC was reduced substantially when the target of fully tested and operational DRC were achieved. The second and final DRC implementation phase included the replacement of the outdated wastewater SCADA system hardware and software, and the addition of network security devices and software. Test procedures and forms were developed to ensure that the DRC contingency plan technical features and recovery procedures are fully functional and respond to the City requirements. Once the DRC system was tested and approved for operation, the developed procedures were documented and distributed to the dedicated DRC team.

- **Operation/Maintenance Phase.** During the operational phase, the City of Houston DRC team, administrators, and managers are required to maintain training and awareness of the DRC plan procedures. The SCADA team exercises and periodically tests the system to ensure that the system functions per the DRC procedures. It is also the DRC team's responsibility to update the procedures and DRC documentation to reflect changes based on hardware or software changes but also on lessons learned.
- **Disposal Phase.** As the City of Houston DRC project was carried out in two consecutive steps, considerations were given to the process of retiring the currently installed computer system and the installation of the system replacing it. Until the new, MS Windows-based system is operational and fully tested (including its contingency procedures), the original system's contingency plan should be in place.

2. <u>Conduct Business Impact Analysis</u>

The BIA objective is to verify the City of Houston wastewater SCADA system components with the critical services that they provide, and based on that information, to determine the impact and consequences of the disruption of that system in case of a component failure. The results from the BIA analysis were then incorporated into the development of the COOP and the DRC design and implementation.

The City of Houston SCADA system is very complex. The system monitors and controls a large number of wastewater facilities dispersed over a large geographic area, with numerous components, interfaces, and processes. The first step taken to evaluate the SCADA system was to determine the critical functions performed by the system and to identify the specific system resources required to perform them.

The City of Houston and Engineer's DRC team had identified and coordinated with the City and SBC/AT&T personnel the system dependency on various communications links, and external support in case of disruption and the need to switch over to the DRC. This coordination supplied the DRC design team with the needed information to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

While performing the Business Impact Analysis, the DRC team followed the contingency plan policy requiring the City of Houston wastewater SCADA system to be recovered immediately (within 15 minutes, but not more than 8 hours in case of a major catastrophe in the Houston metro area). By documenting and reviewing the recovery strategies, the DRC design team could make well informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs. Based on the BIA, it was defined that:

- The DRC system is to have all the functionality of the existing Groveway SCADA system, excluding the backup redundancy, and to have at the minimum, necessary hardware, software and communication equipment to access the current WWTPs and field sites.
- The DRC system is to be designed based on the current SCADA system, including the necessary hardware, software and configuration for a fully functional and operational system. To save the City of Houston cost, it was decided that several of the currently installed but not used servers be utilized for the DRC, following a hardware upgrade. Database tags and graphic screens were to be identical to both sites, when new LCD wide display screens will be installed at the DRC to complete mirroring of the Groveway SCADA control system.
- It is anticipated that during normal operation, database values collected by the Groveway system will be exported to the DRC via the existing City of Houston communication system, and will be stored at the local DRC servers as well for future use.

- In the case of a Groveway SCADA system failure, the switch-over to the DRC is to be performed manually by SBC/AT&T or by the dedicated City of Houston DRC designated and authorized personnel utilizing the SBC-supplied Network Management Console / Workstation with the appropriate software, for communication system configuration, testing and switch-over capabilities.
- Per the developed BIA it was also defined that the switchover is not to be considered "hot transfer" however SBC/AT&T is guaranteeing that such transfer will take place within 15 minutes but not more than 1 to 8 hours in a worst case scenario (major disaster in metropolitan Houston).
- The Groveway SCADA communication and WAN/LAN hardware components were also upgraded per the BIA, in a manner to make the Groveway communication system compatible with the DRC-SBC/AT&T communication system.

3. <u>Develop Recovery Strategy and Operation Procedures</u>

Recovery strategies provide the required means to restore the SCADA operations quickly and effectively following a service disruption, in the allowable outage times identified in the BIA. Several alternatives were considered when developing the City of Houston wastewater SCADA strategy, including cost, allowable outage time, required systems' security, but initially without the integration with the larger, City- level contingency plans.

The selected DRC strategy addressed the potential impacts identified in the BIA and therefore was integrated into the system architecture during the design and implementation phases of the system life cycle. The DRC design included a combination of methods to provide wastewater SCADA monitoring and control recovery capabilities over a full spectrum of incidents.

One of the major tasks was to select the offsite DRC facility, where the following criteria were considered:

- **Geographic Area:** Distance from the City of Houston SCADA center at Groveway, mainly trying to avoid the probability of the DRC site being affected by the same disaster as the Groveway center (flood, terrorist attack, long term power or communication outage).

- **Accessibility:** Length of time necessary to have the DRC operating team access this facility, have the communications switched over from Groveway to DRC, and have the DRC facility fully operational.
- **Security: S**ecurity capabilities of the designated DRC facility and employee confidentiality, which must meet the data's sensitivity and security requirements.
- **Environment:** Structural and environmental conditions of the DRC facility (i.e., temperature, humidity, fire prevention, and power management controls).
- **Cost:** Design, construction, and operation and maintenance costs to have the disaster response and recovery services.

Searching for the appropriate site to support the DRC system operations as defined in the plan and following the BIA, several site types were studied during the DRC design:

- **Cold Sites** typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the SCADA system. The space may have raised floors and other attributes suited for computer operations. This site does not contain SCADA equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. Should the cold site alternative be selected, the City has to provide and install the necessary SCADA equipment and telecommunications capabilities.

- **Warm Sites** are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated SCADA DRC system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

- **Hot Sites** are office spaces appropriately sized to support the SCADA DRC system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system switchover as soon as they are notified that the contingency plan has been activated.

- **Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and SCADA equipment necessary to meet the DRC system requirements. Usually the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the DRC system's allowable outage time.
- **Mirrored Sites** are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

In analyzing the above options, it became obvious that the mirrored site was the most expensive choice, but ensured a virtual 100 percent availability. Cold sites were the least expensive to maintain; however, they require substantial time to transport and install the necessary DRC equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours. However, the time necessary for installation can increase this response time.

The City of Houston DRC team selection was for the fixed-site location, taking into consideration that it is operational with City employees 24/7 and the time to transport the dedicated DRC personnel there is minimal. In addition, the selected fixed site is located in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the Groveway SCADA center. As sites were evaluated, the City of Houston and the Engineer team reviewed that the system's security, management, operational, and technical controls were compatible with the required plan and responded to the BIA.

However following the devastating 2005 Atlantic storms Katrina and Rita, it became obvious that only one DRC site might not respond to the City of Houston wastewater SCADA emergency plan policy as Houston metropolitan traffic became a significant gridlock with many people trying to evacuate, and the DRC managers and operators simply could not commute to the dedicated DRC site and operate the system. It then became clear that to effectively operate the wastewater SCADA system more sites would be needed.

The Business Impact Analysis was reviewed and revised to include additional EOC sites geographically dispersed in various areas, accessible to the DRC team. To keep the cost low for those EOC sites, it was decided to have several City services commonly share the DRC equipment and operations.

4. DRC Testing, Personnel Training and Plan Exercise

The DRC intensive testing plan, which was a critical element to ensure that the system is ready to operate per the design and the policy set forth by the City of Houston, was carried out initially by the contractor installing the DRC system and periodically by the DRC team. The thorough testing enabled the DRC technical and operational deficiencies to be identified, addressed and corrected. The performed tests also assisted in evaluating the ability of the recovery staff to implement the plan quickly and effectively. The following areas were addressed during the tests:

- System switchover to the DRC with alternate methods (by the DRC team and SBC)
- Coordination among DRC team members
- SCADA system performance following the DRC switchover
- Notification procedures
- Restoration of normal operations after testing

Prior to DRC system delivery to the City of Houston, the contractor was required to perform the following tests:

- Failure mode and backup procedures including power failure, AUTO restart, and disk backup and reload.
- Dual Computer Operation: Processor transfer modes, peripheral switching, and communications switching.
- Message logging and alarm handling.
- Communication with field interface units.
- Data acquisition.
- Human-Machine Interface: Database and display configuration and use of all types of displays.
- Data collection and data retrieval.

- Report Generation: Creation of a typical report and production of specified reports.
- Operational Readiness Test.
- Performance Acceptance Test.
- Reliability Acceptance Test.

Training for the City of Houston DRC team with the contingency plan responsibilities came to complement testing. Training took place during system construction and is planned to be provided at least annually to ensure that the DRC operations are able to execute their respective DRC procedures without the aid of actual documents or the assistance of the DRC management team. This is an important goal to achieve to ensure that the team is ready to operate the DRC even if documentation is not available due to the extent of the disaster. DRC personnel are to be trained as follows:

- **Classroom Exercises**. Walk through the procedures without actual DRC switch over and operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing the functional exercises.
- **Functional Exercises.** Functional exercises require the event to be simulated and the DRC switchover and operation to take place. The functional exercise is to be coordinated with the City of Houston EOC management, with the SBC/AT&T team and the wastewater SCADA operations. This exercise includes the actual switchover to the DRC site, thorough communication testing and SCADA system recovery following the successful testing.

5. <u>DRC Plan Maintenance</u>

To keep the DRC fully functional and to maintain its readiness, the plan procedures and policies must be kept. However, as the City of Houston SCADA systems undergo frequent changes because of technology upgrades, or new internal or external policies, the DRC operational plan is being reviewed and updated periodically as part of the City of Houston change management process. Certain elements are required to be taken into consideration:

- Operational requirements
- Security requirements
- Technical procedures

- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of DRC team members
- Names and contact information of SBC/AT&T
- Vital records (electronic and hardcopy)

A copy of the DRC procedures is kept in both places (Groveway and the DRC); however, additional copies are stored at the DRC team sites and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of the disaster.

Changes made to the DRC plan, strategies, and policies are coordinated through the City of Houston DRC planning coordinator, who then communicates the changes to the DRC team members as necessary.

The DRC coordinator also evaluates the supporting information to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

- DRC team contacts
- Hardware and software requirements and licenses
- System network communications
- Security requirements
- Recovery strategy
- Contingency policies
- Training and awareness materials
- Testing scope, and required testing schedule

CONCLUSION

In this age of highly computerized control and monitoring systems, much of the information received is available only via computer and digital network systems. Regularly backing up the information stored on the SCADA system computers is a very important step that might protect the loss of information due to computer failure. However the SCADA system itself could be destroyed or damaged due to flood, earthquake, terror attack, or other natural disaster or man-made problem. Furthermore those actions might prevent access to the SCADA monitoring and control center and will prevent them from supplying the required wastewater services to City of Houston residents.

The City of Houston wastewater SCADA DRC system implementation project, which added a fully functional backup system to the Groveway wastewater SCADA monitoring and control system have supplied the city with the required tool to be prepared for contingencies and disasters.

The DRC project team discussed the strategies to provide continuous operation for the City of Houston wastewater SCADA operations, and identified the best means for recovering with minimum or no delay. As cost of the DRC system vary and is greatly dependent upon the systems and sites selected, the team performed a thorough Business Impact Analysis (BIA). Recovery strategies were developed and implemented to make sure that the response to the disaster would be quick and effective. The implemented plan was tested time and again to assure that procedures were in place and that the DRC personnel were well trained and the systems exercised. A disaster recovery maintenance plan was put into place with the policy to update it regularly and to remain current with systems enhancements and modifications.

The continuous and thorough project review process, followed by the implementation and testing of the SCADA systems, and the fact that the DRC contingency plan is kept as a 'live document' incorporating every necessary update, along with the team effort that included City of Houston PW&E, together with the consulting engineering firms made this DRC project successful and valuable for the years to come.

ACKNOWLEDGMENTS

The CH2M HILL SCADA team would like to thank the City of Houston PW&E teams and the Groveway and DRC Operations staff for their commitment to this important project. Also a special appreciation to the Telvent folks that worked diligently to complete the DRC system installation and testing and the SBC/AT&T Houston managers and technicians that made sure that the communications systems will function smoothly.

REFERENCES

- ISA Standards Library for Measurement and Control. InTech –SCADA Disaster Recovery. Various articles.
- CH2M HILL SCADA System Improvements Project. Disaster Recovery System (DRC-CS) Project documentation.
- National Institute of Standards and Technology – Preparing for Contingencies and Disasters. The NIST Handbook. An Introduction to Computer Security. Special Publication (800-12). July 2002.
- National Institute of Standards and Technology – Risk Management Guide for Information Technology Systems. Computer Security Division (800-30). July 2002.
- National Institute of Standards and Technology – Contingency Planning Guide for Information Technology Systems. (800-34). June 2002.
- Policy on Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD-63). May 22, 1998
- Middletown Thrall Library Special Coverage: Hurricane Katrina Information Guide
- Various Web Sites: Hurricane Rita
- Office of Community Development - Disaster Recovery
- CH2M HILL Project Delivery System: A System and Process for Benchmark Performance. 4th Edition.
- Automation of Wastewater Treatment Facilities. Water Environment Federation. Manual of Practice No. 21. Third Edition. 2006.