Section 2, Chapter 6

CONFIGURATION & SYSTEM AVAILABILITY

6. 0 General

This chapter describes the requirement of monitoring and managing the SCADA/DMS system with regard to its configuration and availability under normal conditions and under hardware and software failure conditions.

6.1 System Redundancy

The SCADA/DMS system envisages some functions as critical functions and others as non-critical functions as defined in Chapters 1 and 2.The critical functions shall have sufficient hardware and software redundancy to take care of hardware or software failure condition whereas non-critical functions may not be provided with hardware and software redundancy.

The redundancy requirement for hardware of SCADA/DMS system shall be as follows:

(a) Servers: The servers for SCADA/DMS,ICCP, Communication servers, ISR application, servers for DMZ/ security system systems, DR and shall be configured as redundant system. (Except for DTS , development server)

(b) LAN and device interface: LAN shall be configured as redundant . All equipment, except DTS, development system shall have single LAN)

(c) Printers: All Printers shall be non- redundant devices.

(d) Operator workstations: These shall be configured as non-redundant devices.

(e) Time and frequency system: The GPS receiver of time and frequency system shall be configured as a redundant device at SCADA/DMS control centre.

(f) Communication front end (CFE): Communication front end shall be configured as redundant system.

(g) WAN Router: The WAN router connected to dual LAN shall have channel redundancy.

(h) DAT Magnetic tape autoloader shall be non redundant drive

(i) Video Projection System (VPS) shall be non redundant

Every critical function must be supported by sufficient hardware redundancy to ensure that no single hardware failure will interrupt the availability of the functions for a period exceeding the automatic transfer time.

Non-critical functions are those that support maintenance and development of database, application software and training of users. No hardware redundancy is envisaged for these functions.

6.2 Server and Peripheral Device States

Server and peripheral device states represent the operating condition, of each server and peripheral device. The various states have been defined below: The system's reaction to restart/failover operations shall be governed by the state. Server and peripheral device states shall be assigned by the function restart, server and device failover functions, and by user command.

6.3 Server States

Each server shall be assigned to one of the following states:

(a) Primary State: In primary state, a server performs any or all of the on-line functions described in this specification and is referred as primary server. A primary server shall concurrently perform maintenance functions (e.g. update of database, display and reports).

(b) Backup State: A server in backup state is referred as backup server. A backup server replaces a primary server/primary server group in the event of primary server/primary server group failure or upon user command. It shall communicate with the primary server(s) to maintain backup databases and monitor the state of the primary server(s). A backup server shall concurrently perform maintenance functions.

(c) Down State: A server in down state shall not communicate with the computer system and is not capable of participating in any system activity

6.4 Peripheral Device States

Each peripheral device shall be assigned to one of the following states:

(a) Primary state: A device in primary state is referred as primary device. The primary device is logically attached to a primary server or primary server group. If the primary server or primary server group fails and its functions are reassigned to a backup server or backup server group, the device shall follow the reassigned functions.

(b) Backup state: A device in backup state is referred as backup device. A backup device is used to replace a primary device in the event of primary device failure. It shall communicate with the primary server or primary server group to inform its readiness for it's assignment as a primary device. A device may be assigned to the backup state by the server function and by user action.

A backup device may participate in on-line activity alongwith the primary device as can be the case with LAN s. For such cases, failure of any one device shall cause other device to take up the role of both devices.

(c) Down state: A device in down state is referred as down device. A down device cannot be accessed by the computer system.

6.5 Functional Redundancy

Every critical function must be supported by sufficient hardware redundancy to ensure that no single hardware failure will interrupt the availability of the functions for a period exceeding the automatic transfer time.

Non-critical functions are those that support maintenance and development of database, application software and training of users. No hardware redundancy is envisaged for these functions.

6.6 Backup Databases

Copies of all databases shall be maintained on the Backup server so that system operations may continue in the event of Primary server, peripheral device or software failure. The backup databases shall be updated with the current contents of the primary databases such that all changes to a primary database are reflected in the backup database within 60 seconds of the change. The backup databases shall be maintained in such a manner as to be protected from corruption due to server and device failure. Backup databases shall be preserved for system input power disruptions of any duration. The information maintained in the backup databases shall include:

(a) Telemetered, calculated, and manually-entered values and their attributes, including quality codes, control inhibit state, and tag data

(b) Data and associated attributes maintained by the Information Storage and Retrieval function

(c) Alarm, event, and summary displays (such as off-normal, control inhibit, and alarm inhibit displays) or sufficient information to rebuild the displays in their entirety (including the time and date of the original data entries, not the time and date the display is newly created)

(d) Application function execution, control, and adaptive parameters and input and output data, including DMS functions savecases.

(e) Changes resulting from the addition or deletion of items and restructuring of databases in an existing database shall be automatically accommodated in the backup database.

6.7 Error Detection and Failure Determination

All servers, peripheral devices, on-line software functions, and maintenance functions in SCADA/DMS system shall be monitored for fatal error and recoverable errors. All errors shall be recorded for review by maintenance personnel. Each type of error (e.g., server failure, memory access violation, device reply time-out, or message checksum error) shall be recorded separately with a date and time tag.

6.8 Server and peripheral device Errors

The Server/Device shall be declared as failed in case of fatal error. Server and peripheral device failure shall be detected and annunciated to the user within 10 seconds of the failure. For each type of recoverable error the programmer shall assign a threshold. When the count of consecutive recoverable errors exceeds this threshold, a warning message shall be issued to the operator.

6.9 Software Errors

Execution errors in on-line and maintenance functions that are not resolved by program logic internal to the function shall be considered fatal software errors. Examples of errors that may be resolved by internal program logic include failure of a study function to achieve a solution due to violation of an iteration limit or arithmetic errors (such as division by zero) which are caused by inconsistent input parameters or data. These errors shall produce an alarm informing the user of the error but shall not be considered fatal software errors. Fatal software errors shall result either in termination of the function or shall be handled as a fatal Server error. The action to be performed shall be defined by the programmer for each on-line function and each maintenance function. If the function is to be terminated, future executions of the function shall also be inhibited until the function is again initiated by the programmer.

On the occurrence of each fatal software error, Server and operating system error codes and messages shall be recorded in the SCADA/DMS system.

6.10 Server Redundancy and Configuration Management

Each server or server group supporting the CRITICAL functions described in the specifications, shall include at least one redundant server. The redundant server shall normally be assigned to the backup state and shall take the role of a primary server in the event of failure or upon user command.

When a failure of a primary server in a redundant group is detected, the SCADA/DMS computer system shall invoke the appropriate failover and restart actions so that on-line functions assigned to the failed server are preserved. The on-line functions of the failed primary server shall be assigned to the backup server by execution of a function restart within 30 seconds after detection of server failure, except for ISR function. For ISR_server function the corresponding time shall be within 120 seconds after detection of server failure_In case of failure of ISR sever, the ISR data shall be stored in the SCADA/DMS system till the failover of ISR server is completed to avoid data loss. This stored data shall be transferred to the ISR server automatically after restoration of ISR server.

If on-line functions are restarted in a backup server, the server's state shall be changed to primary. If backup servers are not available to perform the required functions, the SCADA/DMS computer system shall attempt to restart the failed primary server. A complete restart of the System, including full update from the field, shall not more than the stipulated time as specified above. No data shall be lost during the transfer of operation

A failover (transfer of critical functions) to an alternate Server shall occur, as a minimum, under any one of the following situations:

- Non-recoverable failure of a server performing a critical function
- User request for a transfer of servers
- Failure of a periodic / scheduled function to execute on schedule.
- Violation of a configurable hardware device error counter threshold.

Failure of non-critical function shall not cause server failover. Functions assigned to a failed server in a non-redundant group may be lost until the failed server is restored to service. Failure of server operating in the backup state shall not initiate failover action.

Failed server shall be switched from down to any other state by user command only. All server reinstatement actions shall result in operator message. The messages shall identify the server(s) affected, all server state changes, and the success or failure of any restart operations.

6.11 Server Startup

Server startup shall be performed when commanded by a user, when server input power is interrupted and restored such that the operating environment of the server is established prior to restarting the on-line functions. Establishment of the operating environment may include execution of self-diagnostics, reloading the operating system and system services, and connection to and verification of communications with all nodes on the SCADA/DMS computer system LAN. Subsequent to server startup, a function restart shall bring the server(s) to the appropriate server state.

Server Startup requirements are as follows:

Cold Start: In which default values are used for entire database. A cold start would be used only to build the initial SCADA/DMS and to recover from extraordinary failure conditions. Server startup shall be completed within 15 minutes and all applications shall be operational within 20 minutes of applying power except for ISR server and its database initialisation, which can be up to 60 minutes.

Warm Start: In which a previously saved version of the database shall be used to initialise all real time data values. Server startup shall be completed within 10 minutes and all applications shall be operational within 15 minutes of application of power.

Hot Start: In which the memory resident version of database shall be used for continued operation. No reload of saved data shall be performed, although application software restarts. The intent is that after hot restart, only the operations being performed at the time of failure may be lost. All on line applications shall be operational not more than failover time.

6.12 Peripheral Device Redundancy and Configuration Management

The device failover shall result in an orderly transfer of operations to a backup device in the event of failure of primary device. The device failover function may replace a failed device with an identical backup device or with a backup device that is different from the normal device.

Device failover actions shall be completed and the backup device shall be operating within 30 seconds of detection of the device failure. All device failures shall be annunciated by alarms.

6.13 System Configuration Monitoring and Control

Required displays shall be provided for the user to review the system configuration and to control the state of the equipment. The following operations shall be possible:

- Fail-over, switching of states and monitoring of Servers and peripheral devices.
- Control of the resource usage monitoring function and display of server resource utilization
- The user shall be provided with the capability to interact with all functions using displays. It shall be possible to atleast Stop, Start, inhibit /enable and Restart any of the functions.
- Displays to view and control the status of backup databases shall also be provided.

End of Section 2, Chapter 6