Bellcore Practice
BR 007-240-100
Issue 2, December 1984

Remote Diagnostic Access Facilities Centrally Developed Systems

Prepared by the Information Management Services Division,
December 1984.

For further information, please contact:

D. R. Heitert
Organization 25810
PYA 1J-277
(201) 981-3486

REMOTE DIAGNOSTIC ACCESS FACILITIES
CENTRALLY DEVELOPED SYSTEMS

CONTENTS

1. GENERAL

1.01 Purpose

Users of Centrally Developed Systems (CDS) need timely, efficient resolution of high priority problems in CDSs. In addressing this need, Bell Communications Research (Bellcore) CDS developers must occasionally have read-only access to Operating Telephone Company (OTC) data to expedite the analysis of problems brought to their attention. The OTCs have prime responsibility for security of their data and computer systems. The purpose of this practice is to define the rules and procedures for approval and use of Remote Diagnostic Access (RDA) techniques.

1.02 Reasons For Reissue

This practice is reissued to convert it from a predivestiture Bell System Practice to a Bellcore Practice and also to make minor additions, deletions, and changes.

1.03 Applicability

This practice applies to central developers, all OTCs, and to both test and production CDSs at the OTCs. At this time, this standard applies to centrally developed information systems for large mainframe computers that are intended to be maintained by a central developer or a release agent.

1.04 References

The facilities and procedures for RDA must be consistent with existing documentation, notably 007-203-101, Standard Operating Environment - MVS.

2. DEFINITIONS

2.01 Centrally Developed System (CDS)

Within the context of this practice, a CDS is an information system developed and supported centrally by Bellcore and/or a vendor for use on-site at multiple OTCs.

2.02 Information Systems Rules Panel (ISRP)

The panel responsible for defining and administering rules for CDSs. Voting members are from each of the regional companies.

2.03 Remote Diagnostic Access (RDA)

The ability for maintainers of CDSs to read data contained within an OTC CDS via a communications link for the purpose of diagnosing a high priority CDS failure. The objective in using RDA is to expedite analysis of reported failures through direct investigation of problem conditions.

2.04 RDA Session

The performance of a remote data gathering and analysis procedure via RDA to resolve a problem. The specific problem is reflected in an OTC-initiated trouble report, and the ensuing session is coordinated by authorized CDS and OTC personnel.

2.05 Remote Diagnostic Port (RDP)

The communications facility installed at an OTC to enable RDA activity.

2.06 Remote Diagnostic Terminal (RDT)

The terminal specified by the central developers/maintainers for use in RDA.

2.07 Remote Diagnostic Facility (RDF)

Includes the RDT, communications equipment, administrative personnel, and procedures established by central developers/maintainers at the central site to implement RDA.

2.08 Maintenance Control Center (MCC)

A generalization which may refer to either an actual physical facility existing at developer and OTC sites or merely a set of functions. As a facility, it is a 24-hour central point of contact for all OTC maintenance problems. It may also handle the processing of new software releases.

2.09 Session Log

A manually generated detail record of each RDA session.

2.10 System Journal

A computer generated record, produced at the OTC computer, of all RDT activity.

3. REQUEST AND AUTHORIZATION OF RDA

3.01 Requests To Use RDA

Requests for authorization of an RDA capability for a CDS, or for major modifications of a previously approved RDA implementation (paragraph 4.02), shall follow these procedures.

(a) The central developer presents a description of the proposed RDA implementation, or modification of an existing RDA implementation, to the ISRP for their review. Subsequent uses of an ISRP-approved RDA implementation may be authorized by the ISRP on a written request from a central developer. Central developer responsibilities are defined in paragraph 4 of this practice.

(b) The compliance of the proposed RDA implementation, or modification, with paragraph 4 of this practice is jointly evaluated by the ISRP support staff — the Computer Technology Support Division (CTSD) of the Bellcore Computing Technology Laboratory — and the central developer.

(c) If the RDA implementation, or modification, is found to be in compliance with paragraph 4 of this practice, the CTSD shall so advise the ISRP. The ISRP will authorize the central developer to include the RDA capability and OTC user documentation as a part of the CDS release package.

(d) When discrepancies exist, the CTSD shall so advise the ISRP and the central developer that the RDA facility is not in compliance with this practice. The discrepancies are documented by the CTSD.

(e) When this procedure results in differences that cannot be resolved between the parties involved, the ISRP decides the points in question.

3.02 Notification of Approved RDA Facilities

The ISRP shall notify the OTCs and the central developer by Bellcore letter whenever an RDA implementation or modification has been authorized (paragraph 3.01).

3.03 Requests For Changes

Changes to ISRP-approved RDA facilities or procedures must be resubmitted for review and approval.

4. CENTRAL DEVELOPER RESPONSIBILITIES

4.01 Request For RDA Authorization

The central developer must present a description of a proposed RDA implementation to the ISRP. A separate request must be made for each CDS. The presentation must include the following:

(a) A demonstrated need for RDA such as a requirement for enhanced response to high priority reported CDS failures.

(b) Full documentation to the ISRP including, as a minimum, the following:

- A list of transactions, programs, and commands to be executed from the RDT.
- A set of program listings (on paper or microfiche) for all RDA support software distributed with the CDS. These listings are for the use of only the ISRP and the CTSD.
- Documentation and examples of data recorded on the recommended system journal.
- A description of how the RDA capability is used, including CDS administrative procedures.
- Outline of suggested OTC administrative procedures.

4.02 Single Remote Diagnostic Access

For a given host software system — e.g., Information Management System (IMS) — one set of terminal specifications and administrative procedures is authorized by the ISRP. All central developers utilizing the same host software system and desiring RDA must adopt the same standard terminal specifications and administrative procedures.

4.03 Dedicated Remote Diagnostic Terminals

Central developers must specifically identify the RDTs. The RDTs must be located in a Maintenance Control Center (MCC) or similar facility dedicated to the management of CDS software maintenance. Access to the RDTs must be restricted by the MCC administrator to those approved to use RDA and who have received OTC authorization to conduct a session.

4.04 Autocall Capability

The ability to dial up the MCC to initiate an RDA session is a present possibility, though not necessarily implemented. Until this capability becomes available, terminal connections should be made by dialing the OTC from the RDT at the central developer's MCC. Autocall should be used when available.

4.05 System Journal

The OTC must have the capability to record all RDA activity. The record of RDA activity may be generated in hard copy or machine-readable form. The ability to post-process a machine-readable journal must be available for routine analysis of such journals if it is used to record RDA activity. These capabilities may be part of the CDS-released software in support of RDA or part of the host system software. When these capabilities are part of the host system software, the central developers must advise the OTC of the specific host system software required.

4.06 Data Security

To protect OTC data and operating systems, RDA specifications must reflect the following requirements:

(a) The RDA software will be restricted to OTC-authorized operation within the CDS's host software subsystem — e.g., IMS or Time-Sharing Option (TSO). Modification of the CDS's host software subsystem is prohibited. Modification of, or unauthorized access to, the operating system — e.g., Multiple Virtual Storage (MVS) - or to other host software subsystems is prohibited.

(b) There will be read-only access to OTC data by central developers. The central developer shall not have the ability to modify or add to OTC data, files or programs. This does not apply to temporary data files created by the OTC for use by the central developer during an RDA session.

(c) Transactions, programs, and CDS commands for RDA use must be delivered with the CDS release package and must be fully documented. Source code listings must be available for authorized OTC security review at the location of the central developer.

(d) All hardcopy printouts generated at the RDF via RDA must be kept on file for at least 3 months. OTC data of a proprietary nature printed at the RDF must be stored in a protected area in accordance with prescribed holding and destruction procedures.

(e) All RDA software must comply with normal system software security. The OTC-installed software security systems should be compatible with the host software system (e.g., IMS and TSO) and should not require RDA software changes.

4.07 Data Base Maintenance Fixes

All fixes must be applied to OTC data files by OTC personnel. Under no circumstances will RDA be used to modify any OTC or CDS data files.

4.08 CDS Program Maintenance Fixes

All program fixes must be complete new load modules, and must be sent to the OTC using established release procedures. Under no circumstances will RDA be used to modify any OTC or CDS software.

4.09 Administrative Procedures - General

The central developer's MCC must establish and document administrative procedures which control access to and use of the RDF. The following items must be included:

(a) A procedure for selection and approval of CDS personnel who can use RDFs.

(b) A procedure for requesting central developer MCC approval of an RDA session.

(c) Specifications for an RDA session log.

4.10 Approved Personnel

The central developer must establish procedures for identifying personnel who will be authorized to use RDA facilities. The procedures must provide for identification of approved personnel to the OTCs and must provide for prompt notification to the OTCs of any changes.

4.11 Session Approval

The central developer must establish procedures for approving RDA sessions, both OTC and central developer-initiated. Session approval responsibility at the CDS should be in the central developer's MCC.

Approval procedures should address the following:

(a) Identifying MCC personnel authorized to approve an RDA session.

(b) Verification of central developer personnel requesting an RDA session.

(c) Obtaining OTC approval for a CDS-requested RDA session.

(d) Initiation of the session log and synchronization with the OTC log and maintenance modification request (i.e., trouble report).

(e) Procedure alternatives, as necessary, for off-tour periods.

(f) Simplicity to avoid delays and improve compliance.

4.12 Logs

All RDA sessions must be manually recorded in the CDS session log. This log should correlate the RDA session with the related trouble report and with the OTC session log. At a minimum, it should identify the date, start and end time, session activity, and personnel involved. The MCC administrator should be responsible for maintaining the central developer's session log.

4.13 Basis For Initiating RDA Session

An open trouble report, following the procedures for the specific CDS, must exist for every central developer-initiated RDA session. However, several RDA sessions in a short time period may all be related to the same trouble report.

5. OTC RESPONSIBILITIES

5.01 Remote Diagnostic Port

Each OTC must install and make available a dial-up port as specified by the central developers for those CDSs with RDA approval. A single dial port can be used for multiple CDSs, on one or more processors, if appropriate switching is provided.

5.02 Technical Support Personnel

The OTC must provide technical support personnel to assist the central developers in completing an RDA session, monitoring the RDA session activity, and restoring system security following the RDA session. The technical support personnel must have sufficient skill and authority to respond accurately and effectively to problems encountered by the central developers (e.g., to correct operational problems such as line trouble during an RDA session).

5.03 Access Security

All components of an approved RDA must be protected from unauthorized use. Such protection must include available technical protection plus appropriate administrative procedures. As a minimum, the following technical protection and administrative controls are required:

(a) An RDA session, once (logically) terminated, should not be restartable. Where available, RDP facilities should be equipped with automatic disconnect. However, this feature should not prevent the reconnection of RDA facilities disconnected by equipment failures.

(b) Terminal names and/or user identification must be disabled/inactivated under normal conditions and also following an RDA session.

(c) Logon password protection should be used where available; passwords should be changed after each RDA session.

5.04 Administrative Procedures - General

The OTC must establish and document procedures which control access to and use of the RDP and which define the data available for RDA. The following items must be included:

(a) Centralized control of all RDPs in the OTC's MCC.

(b) Procedures for MCC approval of an RDA session.

(c) Procedures for selecting and approving the data to be made available for RDA.

(d) Procedures for approving requests for access to additional data during an RDA session.

(e) Specifications for an OTC RDA session log.

(f) Requirements and procedures for system journal post-processing.

(g) Training procedures

(h) Procedures for identifying approved personnel to the central developers and for prompt notification to the central developers of any changes.

5.05 Session Approval and Control

The OTC must establish procedures for approving an RDA session, both internally (OTC) requested and developer-requested. Session approval should be under the jurisdiction of the OTC MCC; the procedures must be approved by the OTC Data Security Administrator. Approval procedures should address the following:

(a) Selection and identification of OTC personnel authorized to approve an RDA session.

(b) Verification of session approval from the central developer.

(c) Verification of central developer personnel using RDA for this session.

(d) Initiation of OTC RDA session log and synchronization with central developer RDA session log and OTC trouble report.

(e) Procedure alternatives, as necessary, for off-tour periods.

(f) Simplicity (to avoid delays and improve compliance).

(g) The ability to monitor an RDA session and to control any line activity.

(h) Correlation of all RDA sessions with a trouble report.

5.06 Logs

All RDA sessions must be manually recorded in an OTC session log. This log should correlate each RDA session with the trouble report and the central developer's session log for the problem under investigation.

5.07 Basis For An RDA Session

A trouble report, following the procedures for the specific CDS, must be submitted by the OTC to the central developer's MCC for each RDA session. However, several RDA sessions in a short time period may all be related to the same trouble report.

5.08 Journals

All activity via the RDP must be captured on appropriate system journals.

5.09 Management Trail Reports

Each OTC should establish procedures to generate management trail reports for routine review of system journal reports, for validating the reported activity, and for investigating variations or discrepancies.

5.10 Training

The OTC must establish training programs to educate all involved personnel in the established procedures and security requirements of RDA.