Design considerations for electronic funds transfer switch system development

by JOSEPH P. MAZZETTI
Technology Management Incorporated
Washington, D.C.

ABSTRACT

This paper reviews the EFTS switch concept and outlines some of the major design considerations involved in its implementation. The EFTS switch permits financial institutions to share customer terminal devices (for example, point-of-sale terminals in a supermarket) by transmitting messages generated at the terminal to the financial institutions holding the customer (and merchant) account. The switch, in addition to message routing, must maintain information for settlement among the financial institutions involved, and generate accounting, audit trial and operational reports. Specifically addressed in the paper are: the financial transactions and terminal devices involved; switch message processing and accounting functions; hardware, software, and network components and alternatives; and security and backup considerations. The material presented is based on EFTS project work performed by Technology Management Incorporated (TMI) for the Federal Home Loan Bank System.

INTRODUCTION

An Electronic Funds Transfer System involving shared terminals *—for example, financial institutions sharing point-of-sale devices in a supermarket or an automated teller machine in a shopping center—requires a computerized switch to route messages from a given device to the computer system (host computer) servicing a particular financial institution. A typical switch configuration servicing two institutions is shown in Figure 1. In addition to message routing, the EFTS switch is designed to generate information for inter-institutional settlement and to maintain accounting and audit trials.

The EFTS switch design emphasizes throughput performance while at the same time providing a high degree of message protection and system integrity. Further, a switch must be capable of handling a multiplicity of host computers with different operating characteristics, have the capability of dealing with varied terminal types, and communicate with other switch networks.

The EFTS switch will be a key element in the future of Electronic Funds Transfer because neither the public nor the merchant community will tolerate a profusion of competing terminals and because of the higher costs associated with independent facilities. The technology for switch development is well within the current state-of-the-art; what remains is the application of that technology to real-world situations. Further, a number of alternative switch and network design approaches exist providing EFTS planners in a given area the ability to configure the switch(es) which best meets the geographical, demographic, and market demand characteristics of that area.

This paper treats basic switch concepts and outlines

* Commonly called Customer Bank Communications Terminals (CBCTs) by commercial banks or Remote Service Units (RSUs) by thrift institutions.

Figure 1—EFTS switch overview
the major design considerations involved in switch development. It is based on EFTS project work performed by Technology Management Incorporated (TMI) for the Federal Home Loan Bank System.

OPERATIONAL CONCEPT

A range of plastic card transactions initiated by depositors will be processed by the switch, including:

- **cash withdrawal**—direct withdrawal from a checking or savings account;
- **check cashing/guarantee**—placing a "hold" on the customer's account in the amount of the transaction;
- **deposit**—placing funds on deposit to a customer's account;
- **funds transfer**—transfer of funds from one account to another;
- **payments**—direct submission of cash or check for loan payment (e.g., mortgage loan); and
- **balance inquiry**—determining the existing balance in an account.

Other switch-based services could include: interface with Automatic Clearing Houses (ACH); interconnection with Credit and Debit card networks; possible linkage with the FEDWIRE, BANKWIRE, and other networks; and other depositor-based services.

These transactions are generated from several types of terminal devices as shown in Figure 2, including automated teller machines and merchant-operated terminals. The automated teller machines (ATMs) dispense cash, accept deposits, accept payments, and transfer funds between customer accounts, and are activated by a combination of a plastic card and push buttons. They typically limit the total number of withdrawals a customer can make through controls built into the system (on-line operations) and on the customer's plastic card (off-line operations). The merchant-operated terminals are those devices normally operated by merchant personnel in a business establishment.

These terminals usually include the following components: plastic card, magnetic stripe reader; numeric keyboard and function keys; display; printer or imprinter; journal tape unit (ECR); and usually a terminal controller to service multiple devices.

The flow of data for a typical transaction is shown in Figure 3. In this example, a customer makes a cash withdrawal at a supermarket; the customer's and merchant's accounts are maintained at different financial institutions.

The customer submits his plastic card to the financial service window at the supermarket. The clerk enters the customer's plastic card along with merchant data (either by a second plastic card or key entry). The customer enters his Personal Identification Number (PIN) through a separate numeric key pad. The transaction data is then transmitted to the switch...
where card and account validation and security is performed through algorithmic procedures and reference to a negative file containing stolen or counterfeit card information. Assuming the validation checks are passed, an acknowledgement is sent back to the terminal. The clerk enters the transaction code and the amount, and the message is then transmitted to the switch. The switch routes the message to the customer's financial institution processor which verifies that a sufficient balance exists to cover the withdrawal and debits the customer's account. A positive acknowledgement of the action is sent to the switch which, in turn, transmits the acknowledgement to the terminal (where a receipt is printed) and also transmits a message to the merchant's financial institution processor where the merchant's account is credited.

The processing performed in each of these steps in the case of a cash withdrawal transaction may vary in alternative switch designs, depending on the division of functions between the switch and financial institution processors.

MAJOR DESIGN CONSIDERATIONS

This section describes in some detail the major design considerations involved in EFTS switch development, including: switch functions, hardware and software components, network alternatives for terminal support and degree of centralization, backup, security, and message standardization.

Switch functions

The EFTS switch must be designed with maximum emphasis on throughput performance (i.e., low message residency time as in an inquiry/response communications network) and also on the ability to provide a high level of system integrity and message protection as can be found in a store-and-forward message processing system. General switch design considerations include:

- ability to support the processing of plastic card-based financial transactions described above;
- ability to provide interconnection with a variety of host processors and terminal devices;
- modular system architecture to accommodate evolutionary transaction volume growth so that no major structural changes are required as greater levels of volume are reached;
- flexible hardware and software design to permit new terminal devices to be added in the future; and
- a high degree of system reliability.

The specific functions to be performed by the switch are listed in Figure 4 and discussed below.

- MESSAGE PROCESSING
- SETTLEMENT
- REPORT GENERATION
- AUDIT TRAIL MAINTENANCE

Figure 4—Switch functions

Message processing

The elements of common processing for each transaction message include:

- message receipt—receipt of messages transmitted from terminals and terminal subsystems (i.e., controllers and concentrators), host processors, and other switches;
- message validation—verification of the format and content of the message received;
- account verification and security—verification of customer and merchant account numbers;
- message logging—writing of all messages processed by the switch to a historical file (usually magnetic tape) for audit trail purposes;
- settlement—posting accounting data to an interinstitutional settlement file;
- message reformatting—reformatting of message as necessary to achieve the appropriate terminal/host processor interface; and
- routing—directing the output message to the appropriate endpoint.

Settlement

The settlement process provides for transferring funds between financial institutions to cover the value of interinstitutional transactions originated by the customers of those institutions. This is normally accomplished by moving the funds between the clearing accounts held by a common financial intermediary such as a Federal Reserve Bank or a commercial bank.

Settlement can be handled in a number of ways, depending primarily on the relationship between the entity that operates the switch facility and the financial intermediary which holds the clearing accounts. If the switch is operated by the financial intermediary which holds the clearing accounts, a continuous clearing process can be implemented. This allows instantaneous clearing, and each transfer can be applied, as it occurs, to the clearing accounts of both the sending and receiving institutions. Periodic cutoffs could provide for reporting, reconciliation, and analysis.

In circumstances where continuous settlement is impractical or impossible, batch settlement can be used. This involves the accumulation of transaction data between cutoffs for subsequent posting to a clearing
account. A single settlement entry can then be made for each participating institution. That entry represents the net of all deposits and withdrawals initiated by that institution's cardholders through its own terminals.

Regardless of the settlement process used, the switch operation will have to provide detailed transaction reports to enable the participating institutions to reconcile their settlement accounts. In addition to accomplishing the settlement function, the switch should provide on-line availability of net position data (among institutions) which is a continually updated balance or a beginning balance and net debits and credits. Warning levels can be established at which an institution would be notified of a need to transfer additional funds into the clearing account.

Report generation

The switch must provide data for the production of reports of four types: on-line reports, system activity reports, accounting reports, and history reports. Definitions of these reports are given in Figure 5.

Audit trail maintenance

In order to ensure the ability to restore system operation following an outage, identify patterns of terminal or network use for possible security violations, and assist in reconciliation of switch/host processor/ter-

On-Line Reports (or displays) assist in the management of the switch system during the processing day. These are usually monitored by an operator at a system control panel. They include:

- **status reports** - status of network hardware;
- **transaction traffic level and flow reports** - type and flow of transaction message traffic;
- **switch system resources utilization** - use of storage devices, core, and other system resources.

System Activity Reports (produced at end-of-day) cover a wide range of data reporting, describing the characteristics of that day's processing. They include:

- **message/transaction workload volumes and characteristics** - by terminal end point, concentrator, and communication line;
- **security** - identification of security problems;
- **error reports** - detailing hardware errors (by source);
- **peak/load reports** - showing peaking characteristics of the daily workload; and
- **file usage reports** - describing update activity against switch files.

Accounting Reports (produced at end-of-day) are directed at control of the inter-institutional settlement process, and include:

- **settlement reports** - displaying the transactions (debits and credits) affecting the various institution accounts and the net result of daily settlement activity; and
- **terminal level reconciliation reports** - reflecting the transactions generated by the terminals to the participating financial institutions.

History (Archival) Reports attempt to maintain a sufficient audit trail on daily activity for purposes of researching and reconciling transaction level questions which might arise. These may be produced daily, monthly, or on an on-request basis. These could include: transaction journals, transaction and dollar volume reports, and other statistical analyses useful to overall management of the switch system.

Figure 5—Switch reports
minal interactions, an audit trail must be maintained of each transaction processed by the switch.

All messages received by the switch must be recorded on magnetic tape or some other suitable device. The tape record should include—in addition to the incoming data—a time and date stamp, a sequential reference number, and the identification of the line and terminal or other device from which the data originated. In addition, the record should contain information relating to the disposition of the transaction, such as routing, format revisions, and error codes.

These transaction records will have to be retained for a period of time commensurate with the need for reprocessing, trouble-shooting, and analysis relating to system integrity and security matters.

The hardcopy could be in the form of microfilm, microfiche, printed listings, or another suitable media.

**Hardware and software components**

The major hardware and software components required for EFTS switch operation are described below. The mix of components will differ for each switch installation based on functions to be performed, transaction workload and performance requirements.

Hardware components will include:

- **Processors**—Several classes of computers could feasibly be used in the switch configuration, including microprocessors, minicomputers, and medium-scale processors. The medium-scale processors would have the capability to perform other financial processing functions, together with the switch functions (integrated switch). For purposes of switch reliability, multiple processors are suggested.

- **Processor Memory**—The range of processor memory sizes will vary according to the class of processor used and the functions to be performed by the switch.

- **Communications Adapters**—These are utilized for communications line control and multiplexing.

- **Input/Output Controllers and Peripheral Devices**—The specific components necessary for switch configurations include:
  - tape drives—for transaction audit log and interfacing with other outside systems;
  - disk—for program storage, switch file residence, and working storage for message processing operations;
  - printer—for production of accounting and activity reports;
  - system console—display-type device for monitoring system operations; and
  - communication “front-ends”—for network control and message handling.

All software required for the EFTS switch can be categorized as either environmental software or applications programs. Environmental software is the manufacturer-supplied packages, including:

- **Operating System**—supports the effective, shared utilization of system hardware and software resources;

- **Transaction/Message Handling Software**—supports communication of messages from terminal to computer, computer to terminal, and from one computer to another;

- **Network Support Software**—descriptive, table-driven language used by a communications processor in controlling network configuration and operation;

- **File Maintenance Software**—provides data base access and update capability;

- **Recovery Software**—provides an automated means for re-establishing operations in the event of system failure (e.g., transmit messages previously received but not yet forwarded); and

- **System Utilities**—includes language processors, data manipulation routines, and other system support software.

The application programs are usually unique to a given switch situation and include those needed to perform the functions described earlier, i.e., message processing, settlement, report generation, and audit trail maintenance.

**Network alternatives—terminal support**

Several network configurations are possible to provide terminal support for the EFTS switch. Switch performance, economics of operation, initial development cost, maintenance costs, minimization of the number of communication lines and distance, and other factors should be considered in determining the most appropriate configuration in any given situation. Three possible alternatives are depicted in Figure 6 and are discussed below.

![Figure 6—Network alternatives—Terminal support](From the collection of the Computer History Museum (www.computerhistory.org))
• **Alternative 1—Computer/Computer Switch**—This approach would require that all terminals be connected to host processing centers with those host processors, in turn, connected to the EFTS switch. The host processors would have the responsibility for terminal and network control functions, including: communication line disciplines, error recovery, polling and addressing, and message format translation. Messages would be presented to the switch in a standard format.

• **Alternative 2—Terminal/Computer Switch**—This approach is at the opposite extreme from Alternative 1 requiring that all terminals be connected either directly or through a series of concentrators to the switch, and through the switch to the host processing centers. The switch, of course, would also handle interinstitutional settlement. In this case, the switch has complete terminal and network control including message formats, interface specifications, and network configurations.

• **Alternative 3—"Hybrid" Approach**—This approach would provide for:
  - Some terminals connected directly to the switch;
  - Some terminals connected to host processing centers and the host processing centers connected to the switch; and
  - Some computer centers connected directly to each other over high-speed lines (by-passing the switch for certain types of message traffic).

In the short term, Alternative 1 appears to be the most expedient because it reduces the complexity of interfacing various terminal devices (and related standard setting) and reduces the switch software and communications costs involved. Alternative 2 presents, in the longer term, the most likely point of evolution because it provides the centralized control and flexibility needed for network expansion. With Alternative 3, several key control questions exist relating to the integrity of the network in the event of failure.

**Network alternatives—centralized vs. distributed switch**

Figure 7 presents two alternative network design philosophies which are applicable: the centralized switch and the distributed switch.

- The **centralized switch** approach uses one or more computers as the heart of the network processing all transactions. For network configuration (a), transactions generated at terminals are transmitted to the switch and routed by the switch to the appropriate host processing center (and settlement accounting is performed).

- In the **distributed switch** (b), each switching node is designed to be self-contained, operating independently of the other nodes in the network. Normally, at least two communication paths are possible to reach each switch node. Further, if the network is constructed such that specific endpoints (such as a host processor) have connections to two nodes (primary and backup), the functions of that endpoint would be available in the event of failure of a given node.

**Backup considerations**

The reliability of the switch network depends largely on the switch design itself. For most switch applications, the need for multiple processors is indicated. For the centralized switch, several backup approaches are possible as discussed below for a two processor example:

- **Foreground/Background Processors**—There are two processors; one CPU operates on-line performing all switch functions, while a backup CPU (with access to all peripheral devices) is available to perform off-line functions until the foreground processor goes down.

- **Load Sharing**—There are two processors, each of which services half of the network workload under normal conditions. In the event that one pro-
cessor fails, the second processor takes over its workload.
- **Hot Standby**—There are two processors; each processor is capable of supporting the network workload and processes each transaction separately. In the event that the main processor fails, the standby computer takes over network operation.

The distributed switch network contains inherent backup in that the overall workload is segmented; thus, only a portion is vulnerable at any particular time. Further, alternate transaction routing among nodes in the network also increases the network reliability.

Another factor affecting the reliability and integrity of the switch is the segregation (physical and logical) of switch functions. This segregation is possible at several levels:

- **Software Segmentation**—Use of modular software design to maintain the processing integrity of each of the functional segments described earlier;
- **Separate Processors**—Use of dedicated processors to perform one or more of the functions indicated; and
- **Sharing**—Assignment of one or more processors in the network to perform given functions; e.g., assigning a host processor to maintain all settlement information.

This segregation can affect the operational efficiency of the switch, its reliability, and its ability to recover in the event of an outage.

**Switch security**

The process of transferring funds between customer accounts and from one financial institution to another via depositor-activated or merchant-operated terminals is susceptible to many types of fraud. Switch designers must build security protection into the basic design. Figure 8 highlights some of the major areas of "vulnerability". Examples of possible fraud are: counterfeit, changed or duplicated cards; wire tapping; tampering with terminal devices; adjusting switch or HPC programs; modification of switch or HPC files.

Commonly considered approaches to achieving adequate security include:

- rendering the card counterfeit-proof and tamper-proof by embedding various materials on or within the card during manufacture;
- encrypting procedures, such as enciphering the characters on the magnetic stripe, and enciphering all file data;
- physical security procedures for switch and host processing center facilities; and
- systems for signature verification, voiceprint, and fingerprint identification.

**Message standardization**

The issue of message standardization has a direct bearing on the cost of development and on-going maintenance of an EFTS switch, its operational performance, and the degree of cooperation among those institutions participating in the use of the switch. Consider two opposite approaches:

- **Standard formats**—This approach would require that all messages (i.e., terminal/switch and switch/host processor) be standardized. This would provide considerable ease of administration and control, as well as a lower base of development and operating costs. On the other hand, practical experience has proven that agreement on standards is very difficult to obtain and, during an interim period, the changeover to standard formats would require maintenance of dual formats with the attendant operational and control problems.
- **No standard formats**—This approach would require that the switch have available a set of terminal-specific and host processor-specific programs which are used whenever a given terminal (or host processor) interaction is initiated. It would permit any new terminal or host processor to be brought "on stream" with minimum switch-imposed restrictions or modifications. It would, however, involve a large investment in software devel-
opment and maintenance and could increase overall transaction processing time.

Between the two extremes, there exists the possibility of standardizing portions of message processing: such as between the terminal and the switch or between the host processor and the switch. Over the long term, as EFTS networks expand, standardization of message formats will become more important. As the number of host processors and other switch nodes increases, control and maintenance problems will also increase.

RECAP

The technology to support EFTS switch development in a range of alternative design configurations as described above is generally available today. EFTS development work is currently under way in pilot projects throughout the country and hardware and software vendors offer a variety of relevant product lines. More detailed investigation is still required in several areas, specifically:

- Security—There is a need to determine the degree of security (over terminal devices, communications network, and switch operation) which is required to ensure against violations of privacy and fraud; and how that level of security can be delivered at a price which does not render switch operation prohibitive expensive.

- Standards—A lack of standardization will, in the long run, lead both to unnecessary duplication of effort and the intercommunication problems both within and outside of a given switch area. Standards will be required in message formats, communication line protocols, terminal device characteristics, and error detection and correction mechanisms.

- Other Considerations—Further definition is required in areas relating to settlement and audit trail including: float implications of switch operation (e.g., direct debiting of an account versus value dating of the transaction for future debiting); clearing arrangements for the financial institutions participating in the switch; and historical audit trail requirements for transaction, terminal, and store level reconciliation of customer and merchant accounts.