Supplementary Materials on Information Security

Multi-Functional Products with GW Architecture

Version 1.0

Contents

Prepared: Feb. 4, 2004
Ricoh Company, Ltd

Overview

This document describes the structural layout and functional operations of the hardware and software for multi-functional (MFP) products with GW architecture designed and developed by Ricoh Co. Ltd (see below), as well as the security of image data and related information handled by MFP internal and peripheral devices.

The explanations will primarily focus on the following, with particular attention to demonstrating how unauthorized access is not possible via the CSS and FAX telecommunications lines to local network environments and to data stored in the machine.

- Operational summaries
- Data flow
- Data security considerations

Products to which This Document Applies

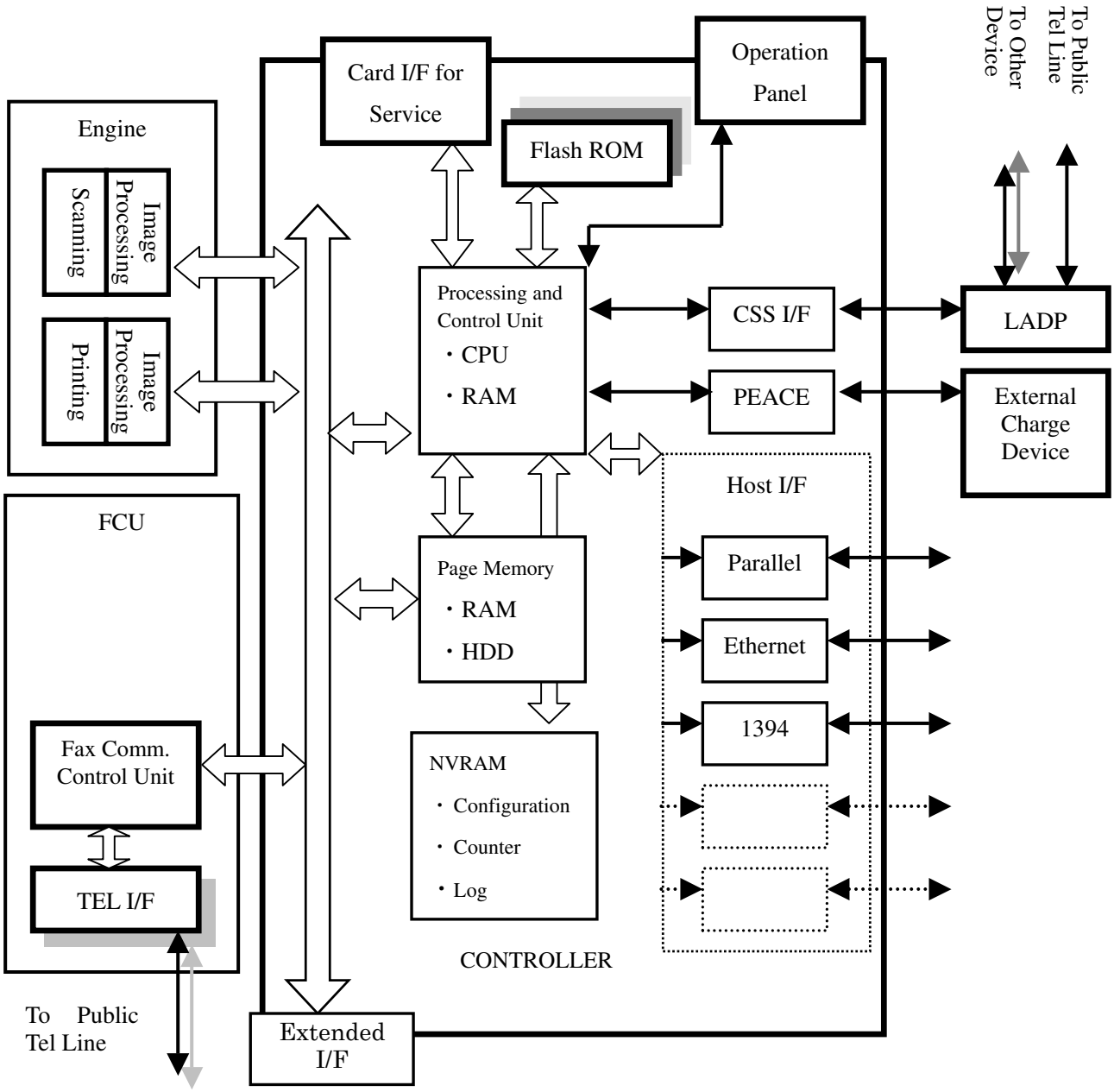
This document applies to the following MFP products with GW architecture, designed and developed by Ricoh Company Limited:

Bellini-C2 (Aficio 2090/2105), Adonis-C3V1 (Aficio 1535/1545), Adonis-C3V2 (Aficio 2035e/2045e),
Russian-C3 (Aficio 2022/2027), Jupiter-C1 (Aficio 2232c/2238c), Kir-C2 (Aficio 2015/2018).

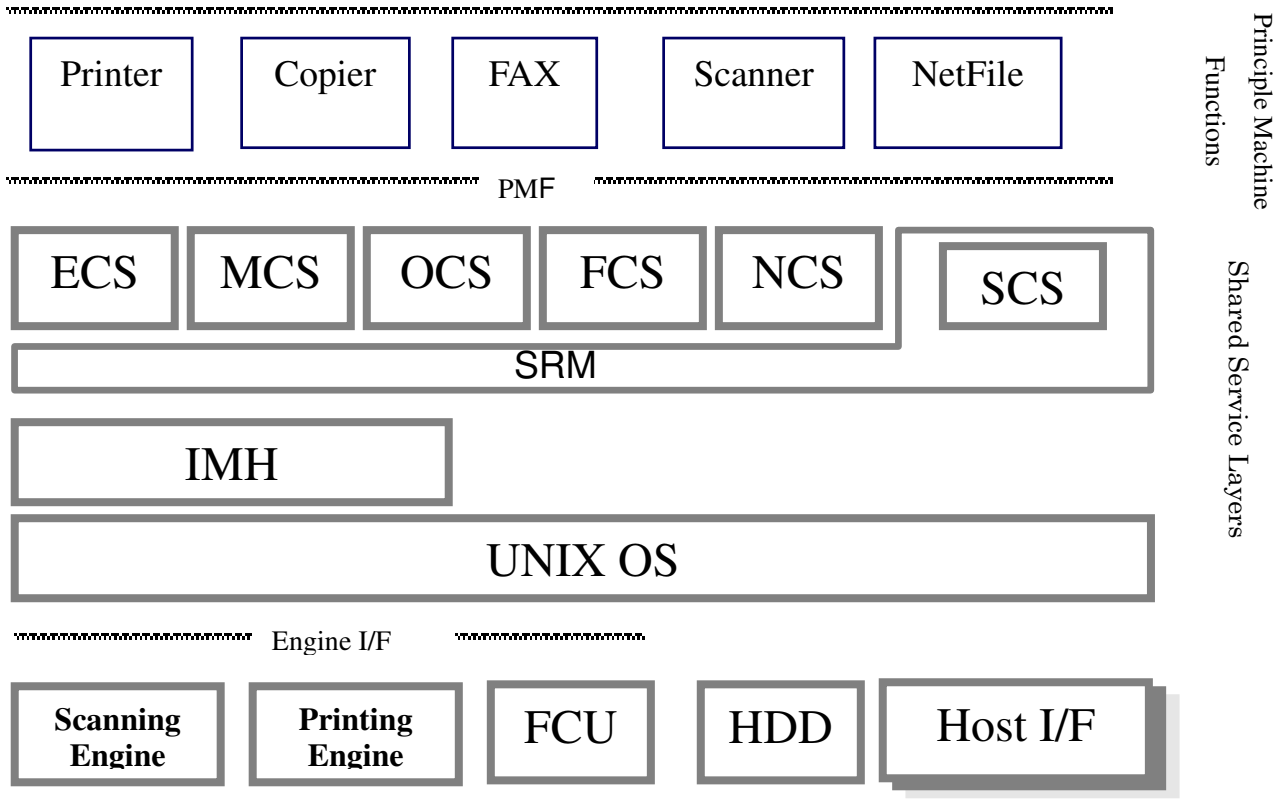
1. Internal System Configuration

1.1 Hardware Configuration

- Scanner Image Memory: Memory buffer for scanned data.
- Image Memory: Consisting of RAM (part of which is used for Page Memory) and memory in the HDD, this area performs image processing functions such as data compression and de-compression.
- Card I/F: Dedicated interface for service maintenance cards.
- Serial communication between the CSS (Customer Support System) I/F and LADP (Line Adapter).
- Serial communication between PEACE (coin/card-operated device I/F) and external coin/card-operated devices.



1.2 Software Configuration



1.2.1 Shared Service Layers

ECS (Engine Control Service)	Controls engine operation for scanning, printing.
MCS (Memory Control Service)	Manages the memory in the Image Memory area (incl. the HDD), as well as compression/decompression.
IMH (Image Memory Handler)	Transfers data between the controller and engine.
OCS (Operation Panel Control Service)	Controls the panel LEDs, monitors panel keys and manages panel objects and display messages.
NCS (Network Control Service)	Controls host I/F and protocol control (transport, session).
SCS/SRM (System Control Service/ System Resource Manager)	Manages machine settings and counter/log data.

1.2.2 Principle Machine Functions

①	Copier	Activates the scanning engine, which reads the original and then sends the data on to the controller to be printed out from the printing unit. Secondary data, such as that used for access control, is handled from the operation panel.
②	Printer	Receives image data through the host interface, which then sends the data to the controller. Also contains a printer language processing subsystem (e.g. RPCS) that converts the printer language into image data, which is then printed out from the printing unit. Secondary data is handled via the connection protocols between the driver UI and the host I/F.
③	Scanner	Activates the scanning engine, which reads the original and then sends the data to a PC via the host I/F. Scanning can be initiated from both the operation panel and from a PC via a TWAIN driver.
④	FAX	Activates the scanning engine, which reads the original and then sends the data to the FCU to be sent as a FAX via a telecommunications line. Also receives FAX data and prints it out from the printer engine.
⑤	NetFile	Accesses and performs operations on documents stored on the Document Server through the 3 functions above via a PC utility or server software.

1.3 Data Security

1.3.1 External I/F

The MFP is equipped with the following interfaces for connection with external devices:

- Serial I/F for LADP connection.
- Serial I/F for connection of external coin/card-operated devices.
- Serial I/F for connection of peripheral devices (e.g. DF, Finisher, LCT).
- Standard IEEE 1284 parallel I/F, Standard IEEE 1394 I/F.
- USB 2.0 I/F
- 100BASE-TX and 10BASE-T compatible network I/F
- Standard IEEE802.11b wireless LAN (option) network I/F

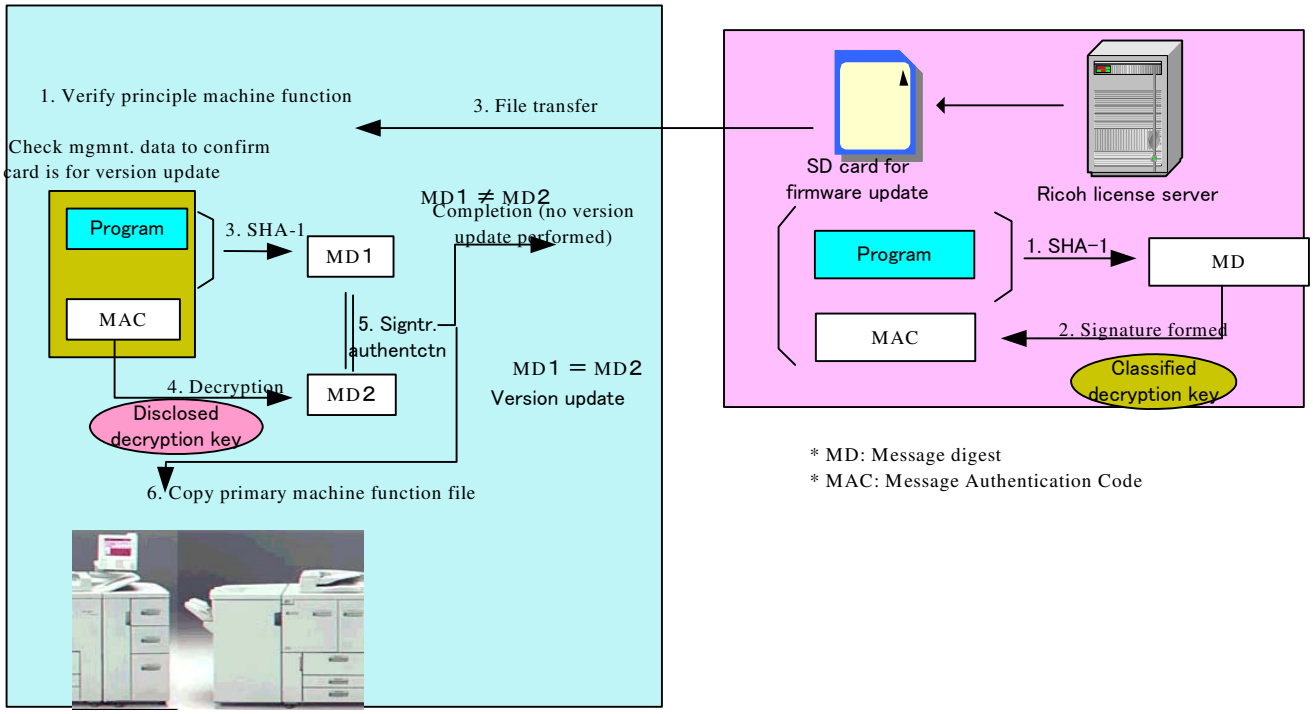
Note: Regarding the Standard IEEE 1394 I/F, USB 2.0 I/F and wireless LAN network I/F, only one can be used at any given time.

1.3.2 Protection of Program Data from Illegal Access via an External Device

1. All of the above principle machine functions, as well as software for all shared service layers, run on the UNIX operating system as independent processes (data/program modules). Memory space is allocated specifically for each module, which makes it impossible for one module to directly access the memory space of any other module.
2. Data transfer between modules is Unix socket-based, whereby each communication path has a specified ID that ensures an exclusive connection, preventing access by other modules. Each module may only conduct data communication with other predetermined modules. For example, incoming CSS data will only be sent to those modules designed to conduct CSS data operations. This arrangement prevents illegal access to networks and internal programs from an outside line.
3. All image data stored on the HDD or stored temporarily in the Image Memory is managed by a memory control module called the MCS (Memory Control Service), which ensures that the data can only be accessed by specified machine function(s). In addition, this arrangement prevents illegal access to this data from an outside line.
4. Communication between the MFP and its peripherals via the peripheral I/F is conduced through Ricoh-unique protocols. These exchanges are limited to pre-determined commands and data, and only take place after the MFP has recognized the peripheral device. If the MFP receives illegal data from the peripheral, it will judge that a perhiperal device failure has occurred or that the device is not connected.
5. The MFP communicates with external coin/card-operated devices through the PEACE I/F in accordance with the same protocols used for its peripherals described in #4 above. It is possible to enable user restrictions on machine operation through such devices, in which case the device and mainframe may exchange the relevant information (e.g. user code data).

1.3.3 Firmware Updates

Machine software is updated via the SD cards commonly available in the field. To prevent the introduction of illegal data or software, each program is marked with its own unique electronic signature. This signature is created by a license server and then stored on the SD card. When a firmware update is then performed, the machine checks for the presence of any illegal or corrupted data through the process shown in the illustration below.



2. Principle Machine Functions

2.1 Copier

2.1.1 Overview of Copier Operations

- When a copy job is initiated, the scanning engine scans the original and forwards this data to the controller to be printed out from the printing unit. If the Document Server function is selected at this time, the image data is also stored in the Image Memory.

- The Document Server function can also be used to scan images directly into Image Memory without copying, and to print out documents already stored in the Image Memory. In addition, a password can also be assigned when scanning a document into memory, requiring the operator to input the correct password to print out the document. Further, user codes can be enabled to restrict access to the Copier function.

2.1.2 Data Flow

- A copy job is initiated from the Copier function, which sends a job start command to the ECS. In turn, the ECS instructs the scanner engine to begin scanning and the MCS to secure the necessary amount of memory in the volatile RAM (Image Memory RAM). The scanned image data is then temporarily stored in the Image Memory by the IMH, after which the ECS instructs the IMH to retrieve the data and send it on to the printing engine. The data is printed out according to the specified number of pages, after which the ECS erases the image data via the MCS.

- When using the Document Server function, either to store documents being scanned for copying or to scan documents directly into storage, the data is sent via the MCS and saved to HDD memory. When using the Document Server function to print out documents already stored in memory, the operator selects from among the documents displayed, i.e. only those MCS-managed documents stored in the HDD using the Copier function. The start command is then sent to the ECS and the document is printed out.

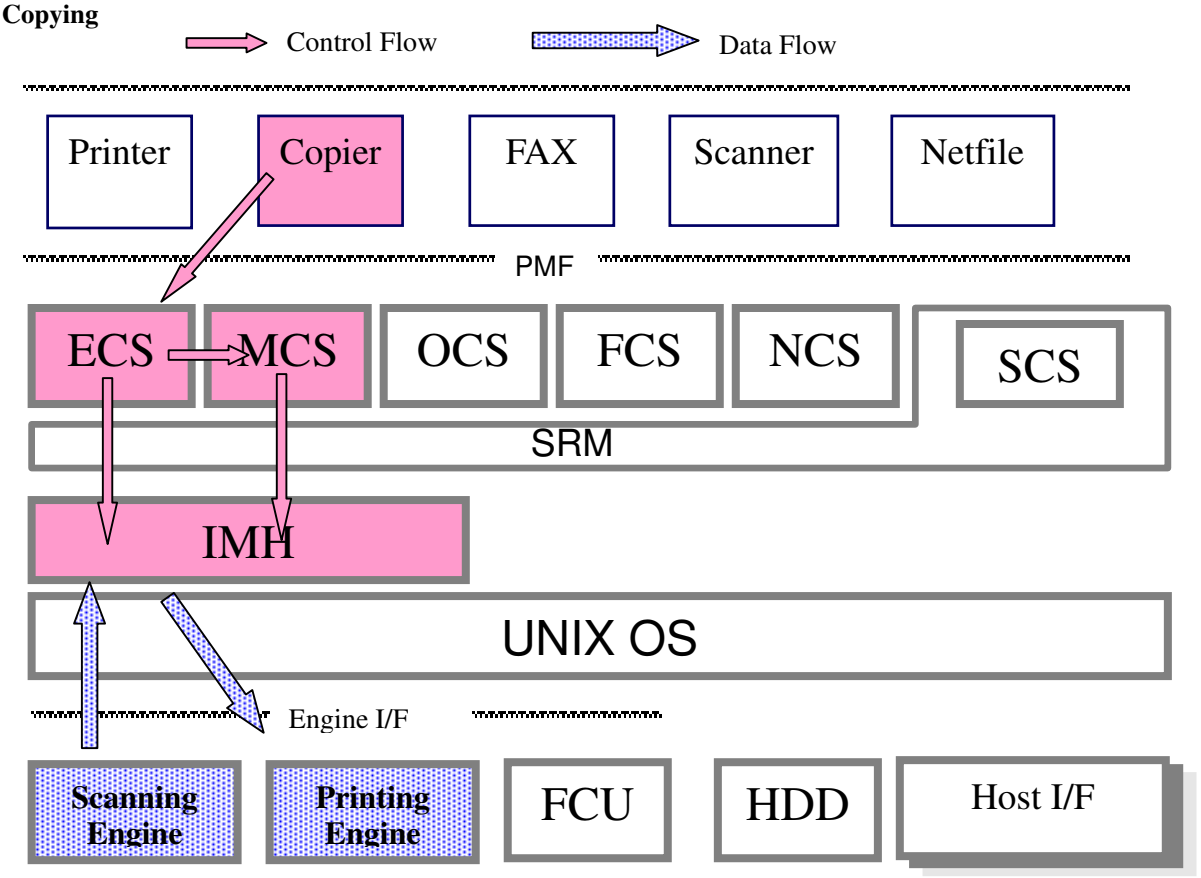
- The Copier function keeps track of how many copies have been made in each copy mode by storing these values in the non-volatile RAM (NV-RAM). These counters are incremented after each page is printed and at the conclusion of every job. These values can be viewed on the operation panel from inside Service Program Mode (SP Mode) and also on machine service reports.

2.1.3 Data Security Considerations

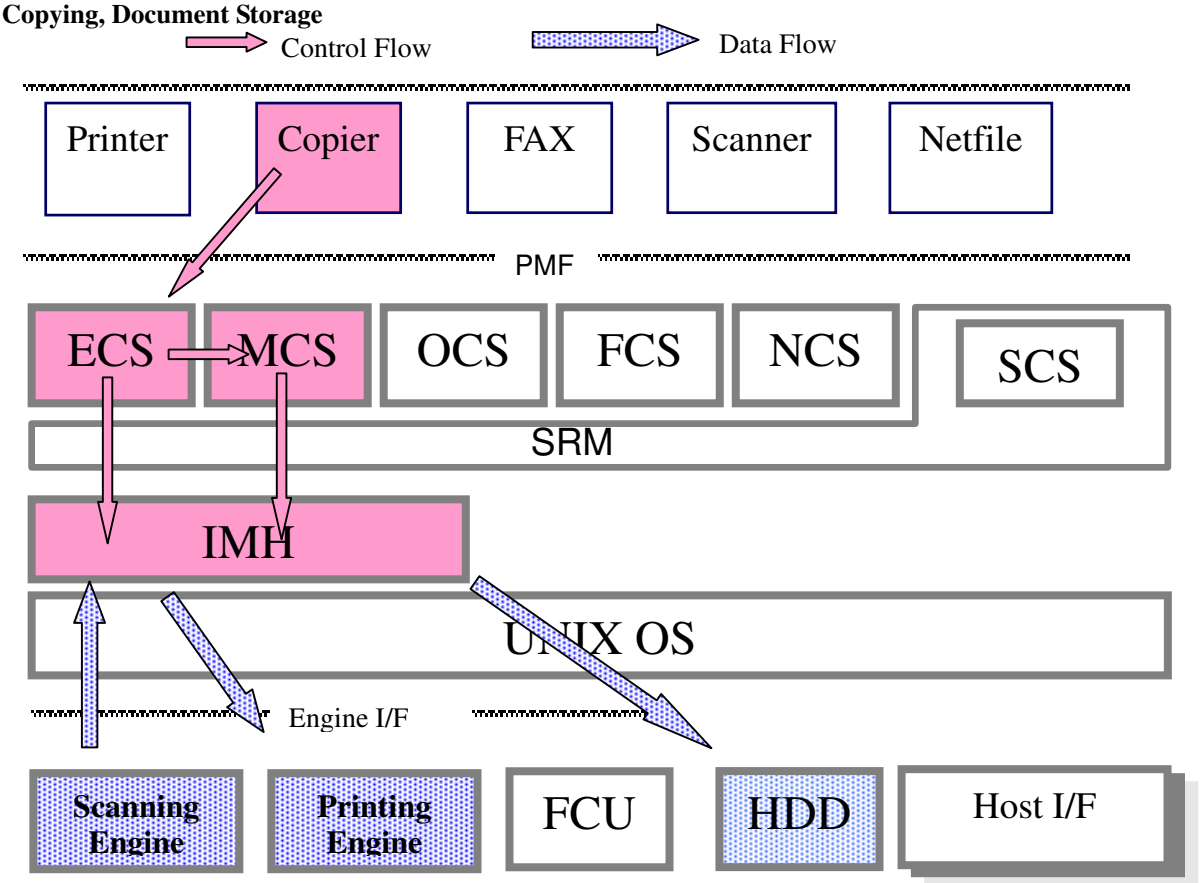
- Since the image data and page location data are erased at the conclusion of every copy job, it is not possible to perform a job re-print on the same data. In addition, documents stored in the Document Server with password protection can only be printed out when the correct password is entered. Further, since the Copier function does not have an external data interface, there is no possibility of the image data being mixed with external illegal data.

Software Flow

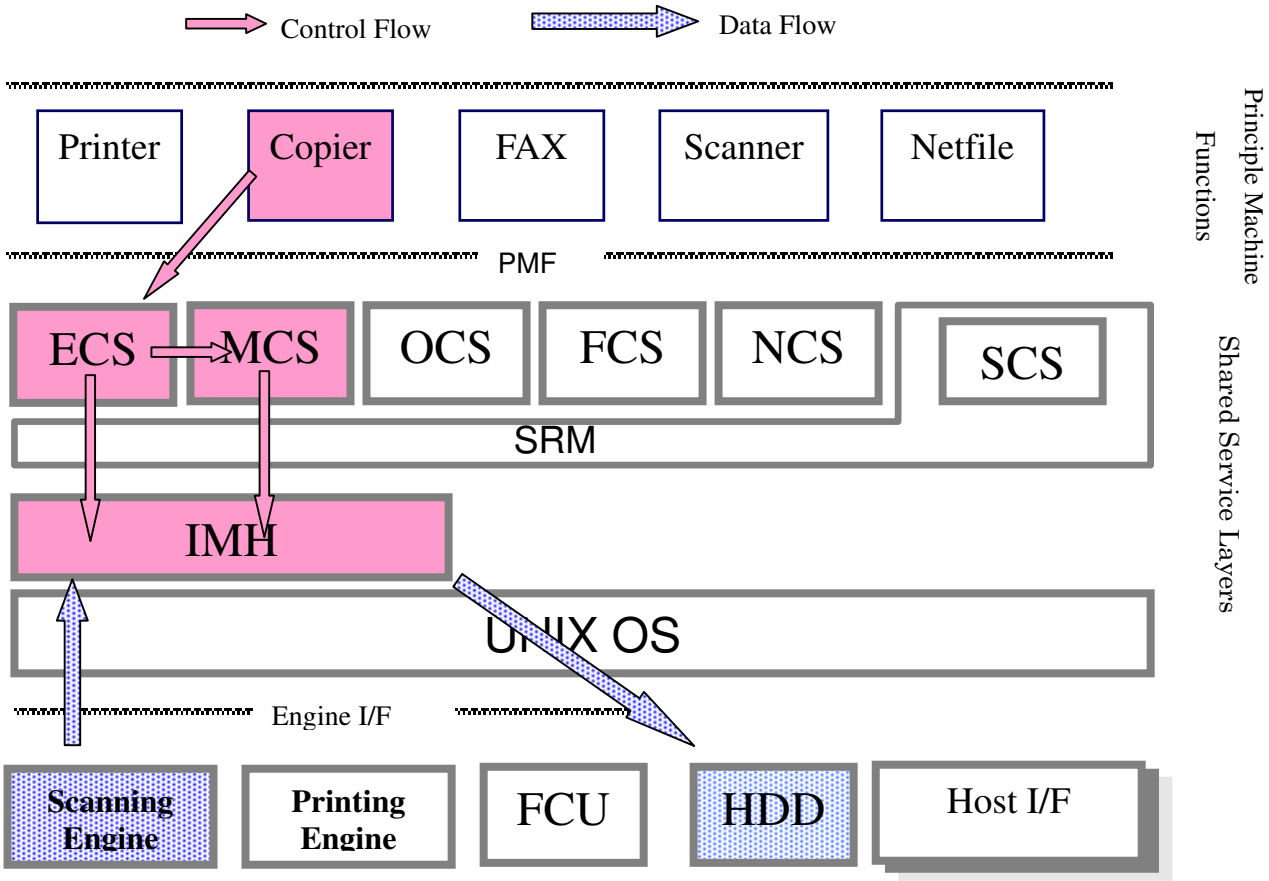
■ **Copying**



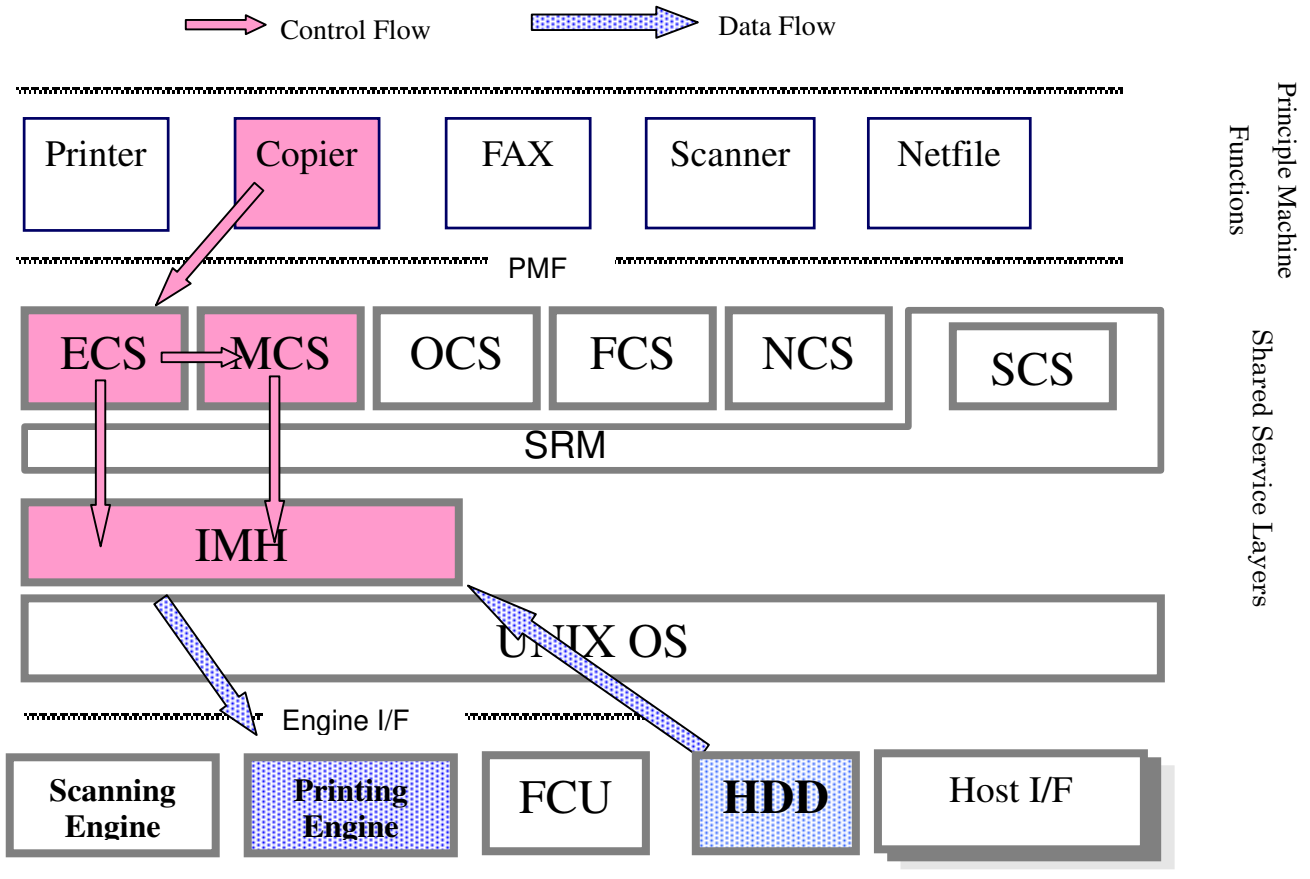
■ **Copying, Document Storage**



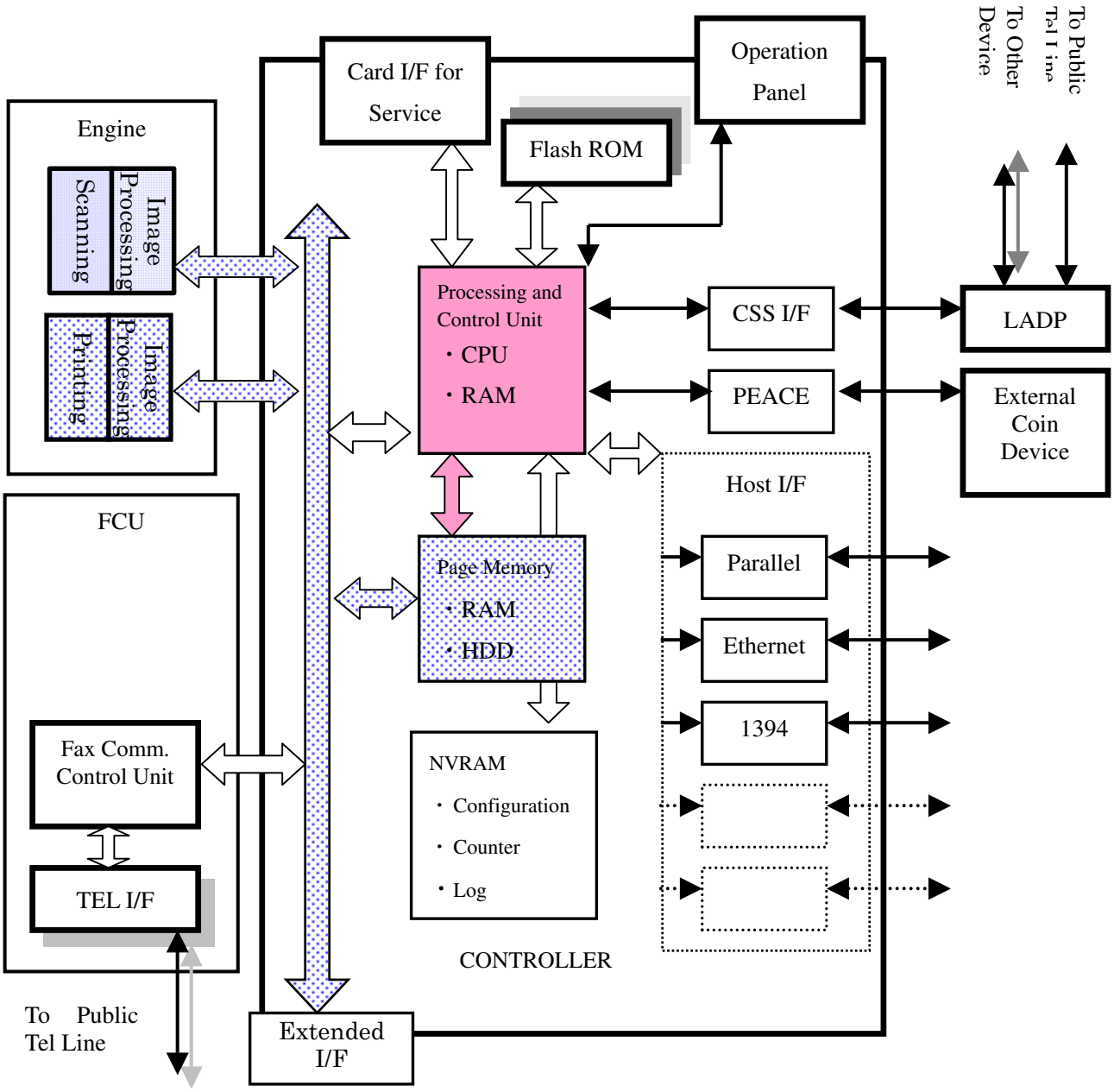
■**Scanning into Document Storage**



■**Printing Out Stored Documents**



Data Flow


Engine
Scanning
Image Processing
Printing
Image Processing
FCU
Fax Comm. Control Unit
TEL I/F
To Public Tel Line
Card I/F for Service
Operation Panel
Flash ROM
Processing and Control Unit
・CPU
・RAM
Page Memory
・RAM
・HDD
NVRAM
・Configuration
・Counter
・Log
CONTROLLER
Extended I/F
CSS I/F
PEACE
Host I/F
Parallel
Ethernet
1394
LADP
External Coin Device
To Other Device
To Public

2.2 CSS (Customer Support System) Copier

2.2.1 Overview of CSS Copier Operations

This feature allows CSS Call Centers to obtain service data from the machine via public telephone lines, which includes the machine's print-for-pay data such as the serial number and current counter values. The data request is received by the LADP, which in turn requests and obtains the information via the CSS I/F and informs the call center.

In addition, whenever a machine malfunction or error condition occurs, the MFP instructs the LADP to inform the call center. The LADP then contacts the call center via the telephone line and reports the nature of the machine failure, along with other information such as the serial number and counter values.

2.2.2 Data Flow

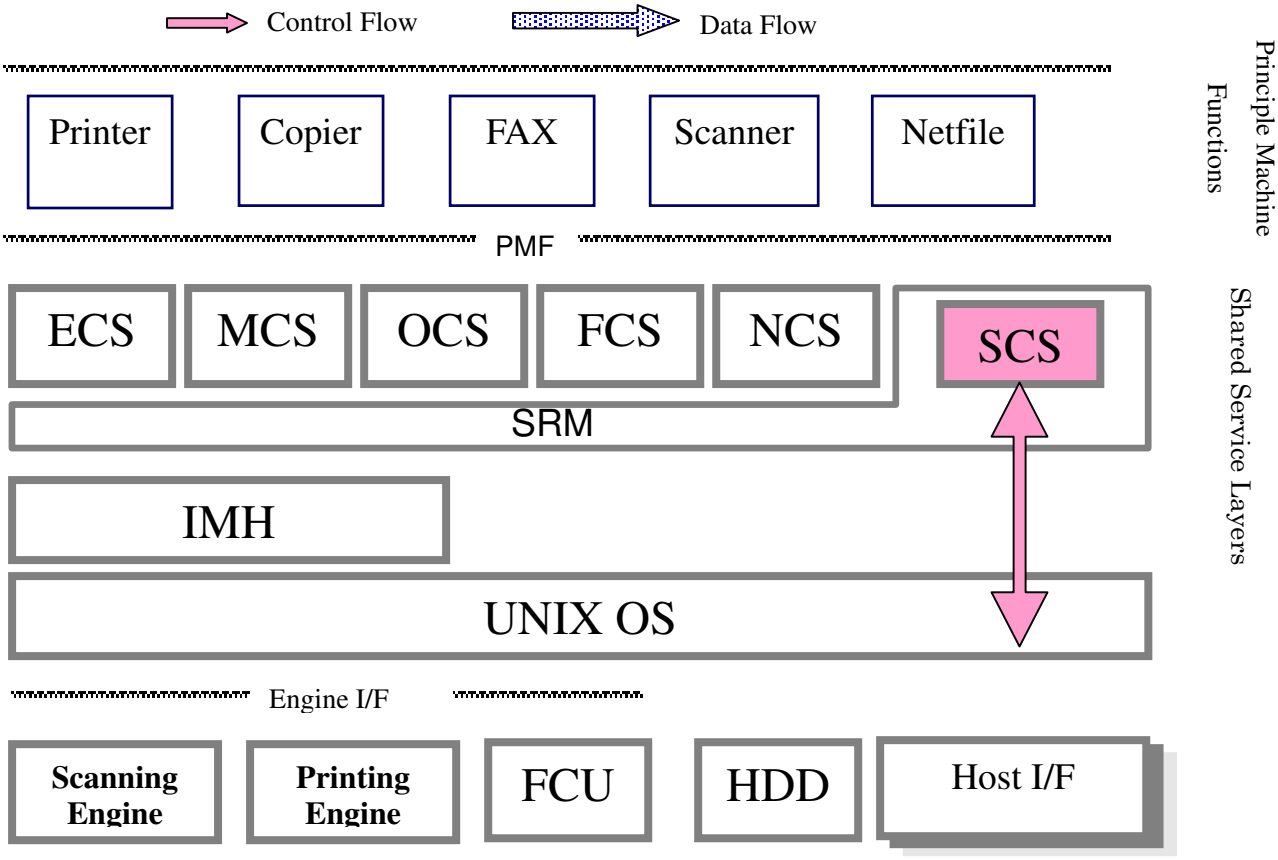
The MFP retrieves the requested service data from the RAM address specified in the SCS, and then sends it to the LADP via the CSS I/F. If a machine malfunction is detected at this time, this information is also sent to the LADP along the same route.

2.2.3 Data Security Considerations

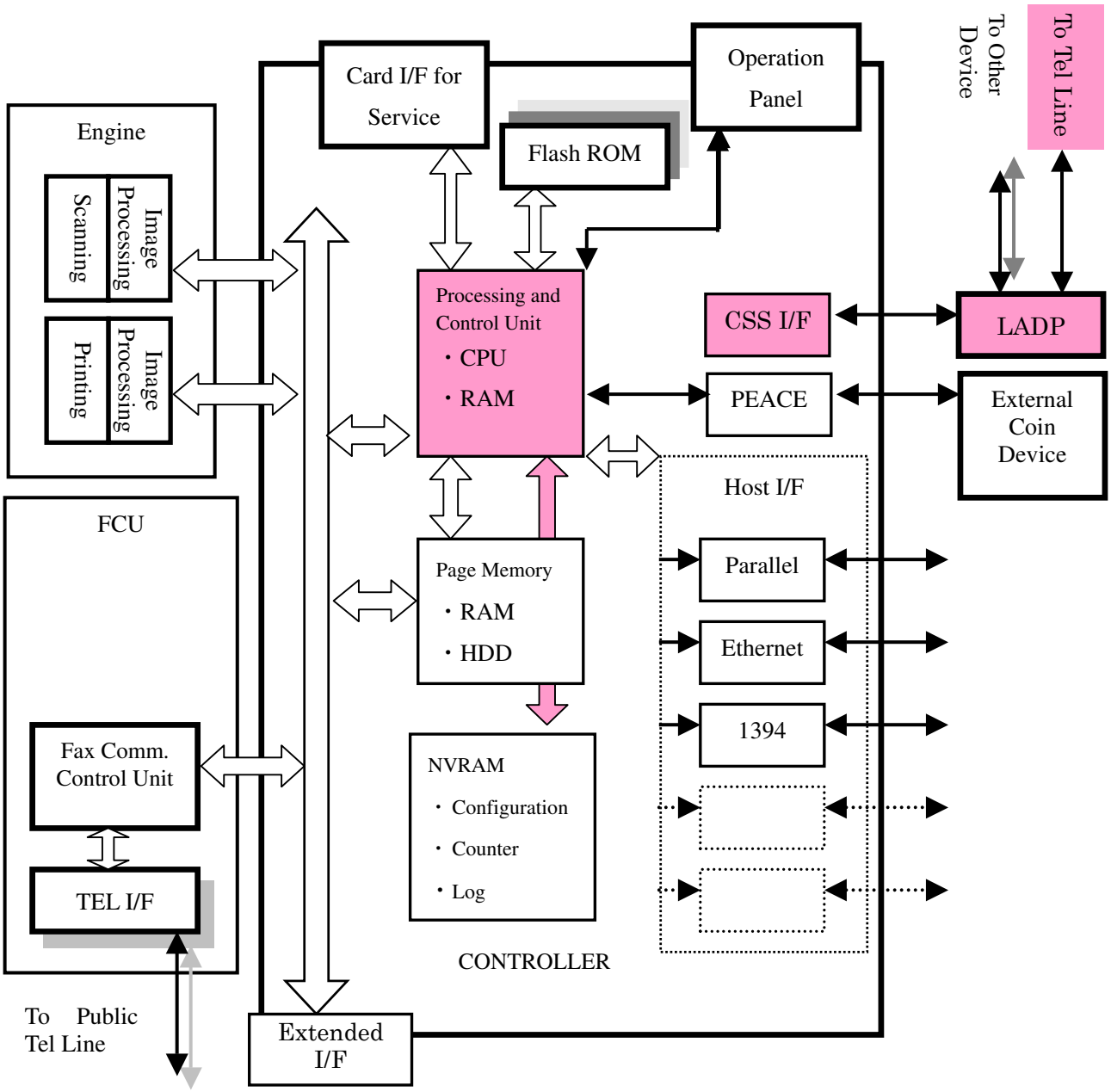
The CSS I/F is a single-chip IC responsible for controlling communication between itself and outside devices, performing such functions as protocol conversion and the destruction of any data received in illegal format. The mainframe CPU contains a set of pre-programmed operations that correspond to each command received through the CSS I/F, of which there are only three types: read, write and execute. These operational responses are identical to those for the read, write and execute command types executed from the operation panel inside Service Mode. In addition, since the parameters for each command are already predetermined, it is not possible to read or write data to an address of one's choosing, or to introduce and execute external programs.

This security filter in the CSS I/F ensures that even if undefined commands were received, they would be destroyed as soon as they reached the CSS I/F. In addition, since the IP firmware (LADP software) is stored in a Mask ROM, it cannot be overwritten by any external source.

Software Flow



Data Flow


Engine
Scanning
Image Processing
Printing
Image Processing
Card I/F for Service
Operation Panel
Flash ROM
To Other Device
To Tel Line
Processing and Control Unit
・CPU
・RAM
CSS I/F
LADP
PEACE
External Coin Device
Host I/F
FCU
Page Memory
・RAM
・HDD
Parallel
Ethernet
1394
Fax Comm. Control Unit
NVRAM
・Configuration
・Counter
・Log
TEL I/F
CONTROLLER
To Public Tel Line
Extended I/F

2.3 Printer

2.3.1 Overview of Printer Operations

- The printer language processing subsystem converts the printer language-encoded data received from the host computer into image data for printing out. The image data is then printed out by the printing subsystem.

- With regular print jobs, the image data is erased at the completion of the print job. When printing out images stored on the machine's HDD using Locked Print or Sample Print, the data is erased at the completion of the job in the case of Locked Print, and at the completion of the "real" (finalized) job in the case of Sample Print.

- Once the data sent from the host computer is accepted, and the processing subsystem begins processing the new print job, a print job log entry is created (temporary entry). The entry is then registered as soon as the job is completed.

2.3.2 Data Flow

1. Normal Printing

- As stated above, the printer language-encoded data sent from the host computer is converted into image data by the language processing subsystem, after which it is stored temporarily into the Page Memory as binary bitmap data. Once this has been done, the data is compressed in a Ricoh original compression format, and stored in the HDD as image data.

- With normal printing, the image data stored in the HDD is erased at the conclusion of the print job. When Sample Print is selected as the job type, the image data remains in the HDD, and is then erased at the conclusion of the next job. However if the main power is turned off in between these jobs, this data is erased.

- When Locked Print is selected as the job type, the image data is saved directly to the HDD without being printed out. This data can then be printed out from the operation panel, and is then erased from the HDD at the conclusion of the job. As with Sample Print, if the main power is turned off before the job is performed, this data is erased.

- When the Document Server is selected as the job type, the image data is stored directly to the HDD without being printed out. Along with the image data, part of the page location data necessary for the Document Server, i.e. the document's bibliographical information (size, date/time of job, etc.) is also saved to the hard drive. Once storage is complete, the remaining page location data is then deleted. The stored documents can then be printed out from the operation panel, or from the PC using DeskTopBinder V2 if the machine is equipped with the MLB option, after which they remain stored in the HDD. They will remain stored even when the machine main power is turned off.

- The page location data for the image data stored in the HDD is stored into volatile RAM memory in Ricoh original format, and is later erased at the same time the image data is erased (see above).

- The user code can be registered in the driver UI, and is then used as the user code for the machine operation log and the Document Server and Locked Print functions. The password for these functions is also registered in the driver UI, and must be entered whenever performing operations on Document Server documents (driver UI/operation panel) or Locked Print documents (operation panel). For details on how to change the passwords for documents already saved to the Document Server, please refer to the description of the Document Server feature in the Operating Instructions.

- A temporary job log is kept in volatile memory, containing the user name, number of pages, time of printing and job status. The contents of the log can be viewed through SNMP in the printer's Ricoh-original MIB, and are erased when the main power is turned off.

2. Encrypted PDF file printing with PDF Direct Print

- With PDF Direct Print, it is possible to print out an Adobe Acrobat-encrypted PDF file. The data is encrypted at the PC side using the SSL (Secure Sockets Layer) security protocol with RC4 at a 40-bit or 128-bit key strength, and requires a password to decrypt it for viewing in Adobe Acrobat or for printing from the MFP. The password is set in Adobe Acrobat, and is then registered in the machine from the operation panel or from the PC via a Web browser. The password functions as the decryption key, and is also protected by the SSL security protocol when sent along the network.

- When the printer receives the file, the printer language processing subsystem (PDF interpreter) recognizes it as an encrypted PDF file and uses the password stored in the machine to decrypt the data. Therefore if the password stored in the machine does not match the one set in the PC, the data itself will not be decrypted correctly, causing an error to occur and the job and data to be erased. If however the password in the machine is the same as the one set in the PC, the data will be decrypted correctly, after which printing follows the normal process described above.

- It is also possible to forbid printing on specific documents from inside Adobe Acrobat.

2.3.3 Data Security Considerations

1. Normal printing:

- The language processing subsystem only allows data in legal format to be processed. In the event that illegal data is received, the subsystem will declare an error and cancel the processing session. In addition, since communication paths between modules are exclusive, as mentioned in section 1.3.2, this data cannot be processed or executed as programs by other unauthorized modules.

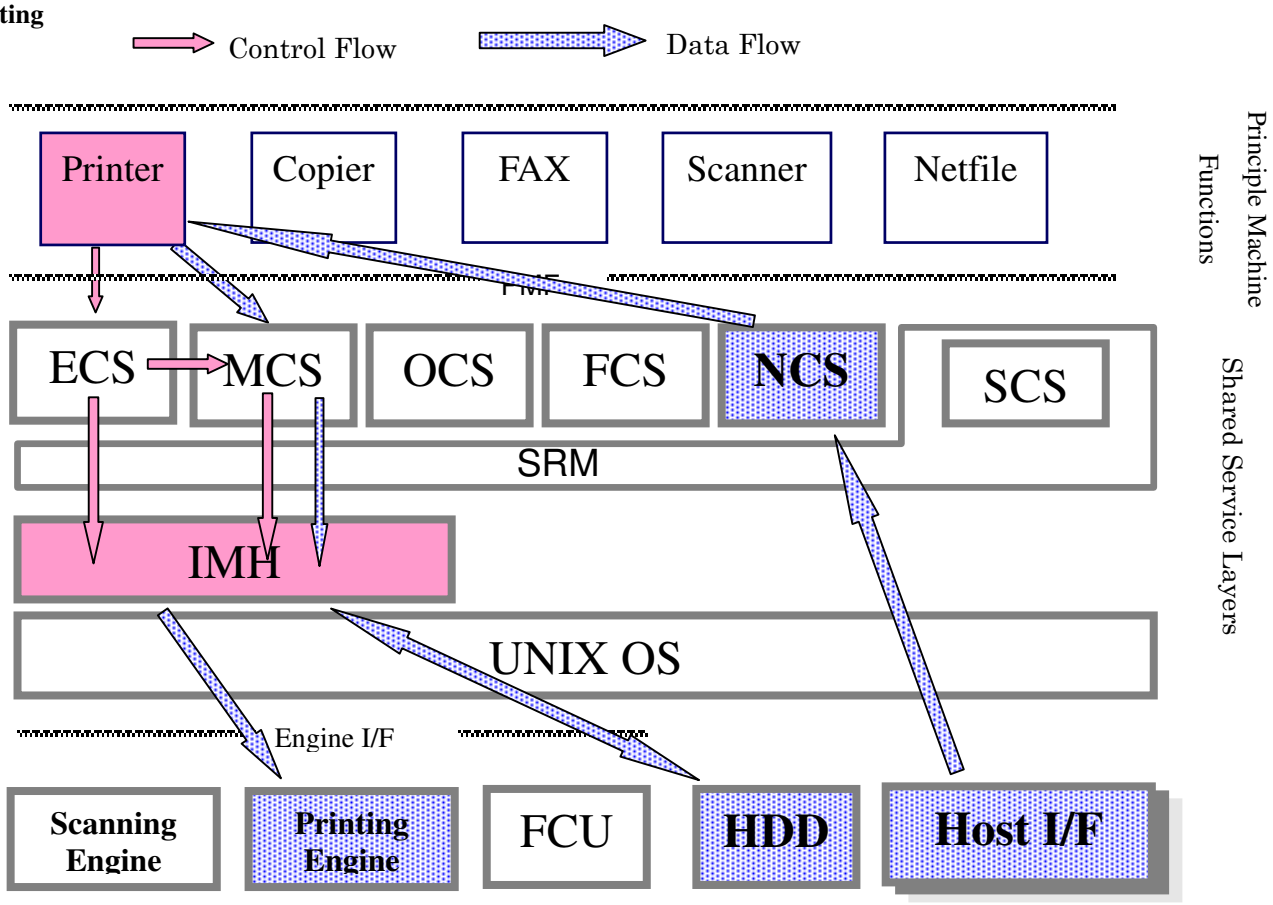
- As mentioned above, when printing out a document stored in the HDD with Locked Print, it is necessary to enter the corresponding password from the operation panel. This password is then checked against the one sent with the image data when it was first stored into HDD memory.

2. Encrypted PDF file printing with PDF Direct Print:

- The machine's PDF interpreter will delete any data it receives whose password does not match the one stored in the machine, or whose printing has been forbidden by Adobe Acrobat. It is therefore impossible for such data to be processed by other program modules.

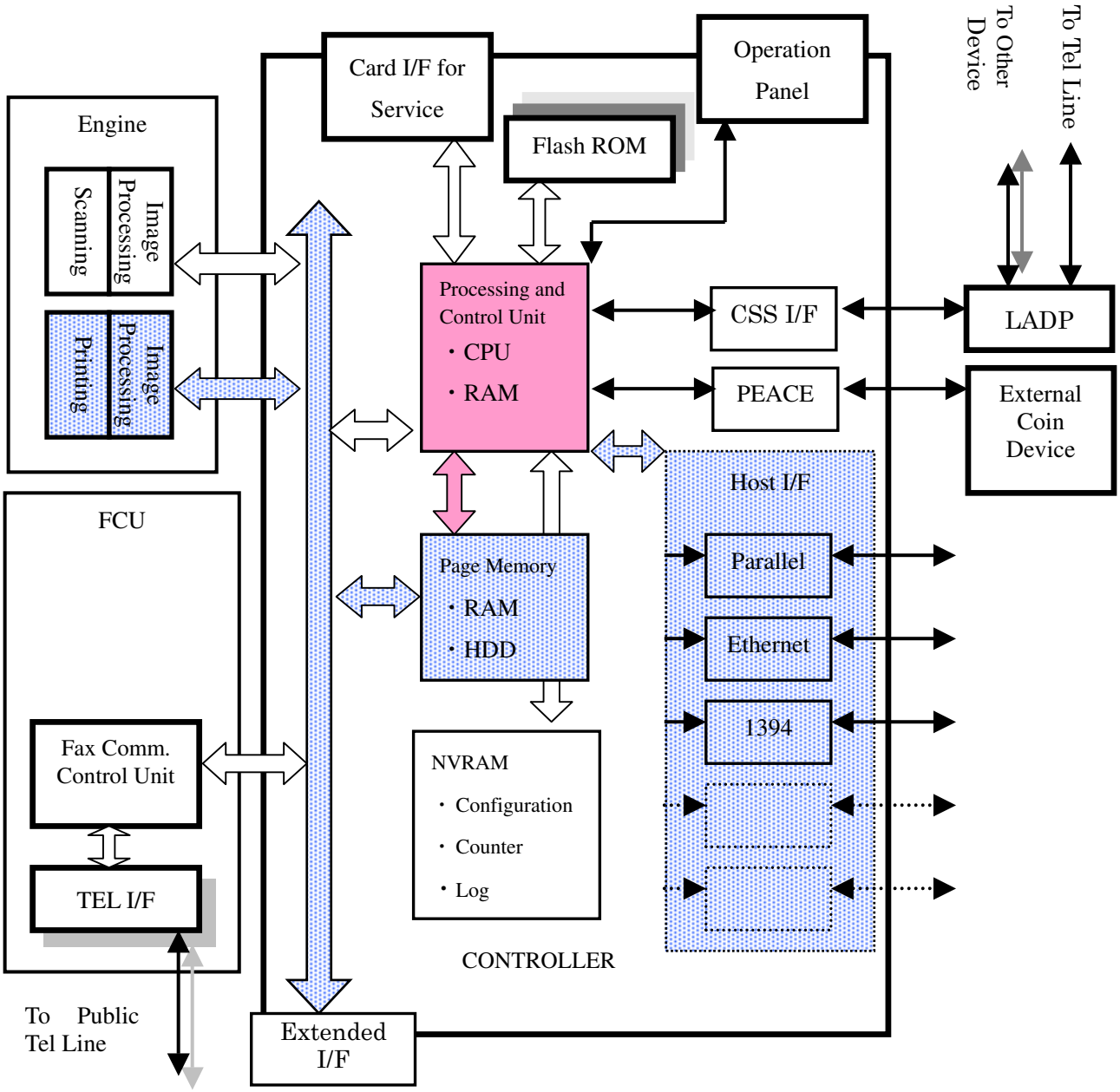
Software Flow

■ **Printing**



Data Flow

■**Printing**



2.4 Scanner

2.4.1 Overview of Scanner Operations

- Depending on the option selected, the Forwarding feature: 1) saves the scanned image to the HDD and then sends it via the network I/F to an SMTP server, FTP server, client PC with Windows 98 or newer, or ScanRouter V2, 2) saves the scanned image to the HDD alone without forwarding it, or 3) temporarily stores the image to the HDD and then forwards it to one of the destinations mentioned above. With the third option, the data temporarily stored to the HDD is deleted once the destination receives the transmission, or if transmission is not successful after a certain number of tries, the data is deleted at this time.

- With the TWAIN I/F, the TWAIN driver can initiate scanning from a network-connected client PC under specified conditions, after which the image is sent back to the TWAIN driver.

- Access to the Scanner function can be restricted with the use of user codes or an external coin/card operated device. Use of the TWAIN feature is only allowed after a crosscheck with the user code data registered in the TWAIN driver U/I.

- Operational log entries are created for both Scanning and Forwarding, which can be viewed from the operation panel or by printing out the log. These logs are stored in non-volatile memory, i.e. it is preserved even after the machine main power is turned off.

2.4.2 Data Flow

- The raw image data sent to the RAM managed by the IMH goes through MH/MR/MMR/JPEG compression or is left uncompressed, depending on the operator's settings. TIFF headers are attached to all data except JPEG-compressed files, after which PDF headers are added in cases where the data is being sent to the SMTP server. The data is then sent on to the network in a commonly-used image file format.

- The user code data sent from the TWAIN driver is in binary format, unchanged. In addition, passwords set at the operation panel for stored documents are not sent to ScanRouter V2 or DeskTopBinder V2. These passwords are used for access control when retrieving stored documents using DeskTopBinder V2, or when performing Remote Forwarding.

2.4.3 Data Security Considerations

The Forwarding feature:

- The MFP is only able to forward data to a single, pre-determined destination on the network (ScanRouterV2 or an SMTP server), and to the destinations registered locally in the machine. In addition, since there is no receiving aspect, there is no possibility for this function to receive illegal data through an external I/F.

- The TWAIN driver will not process any binary data that does not conform to the predetermined protocol of the command I/F.

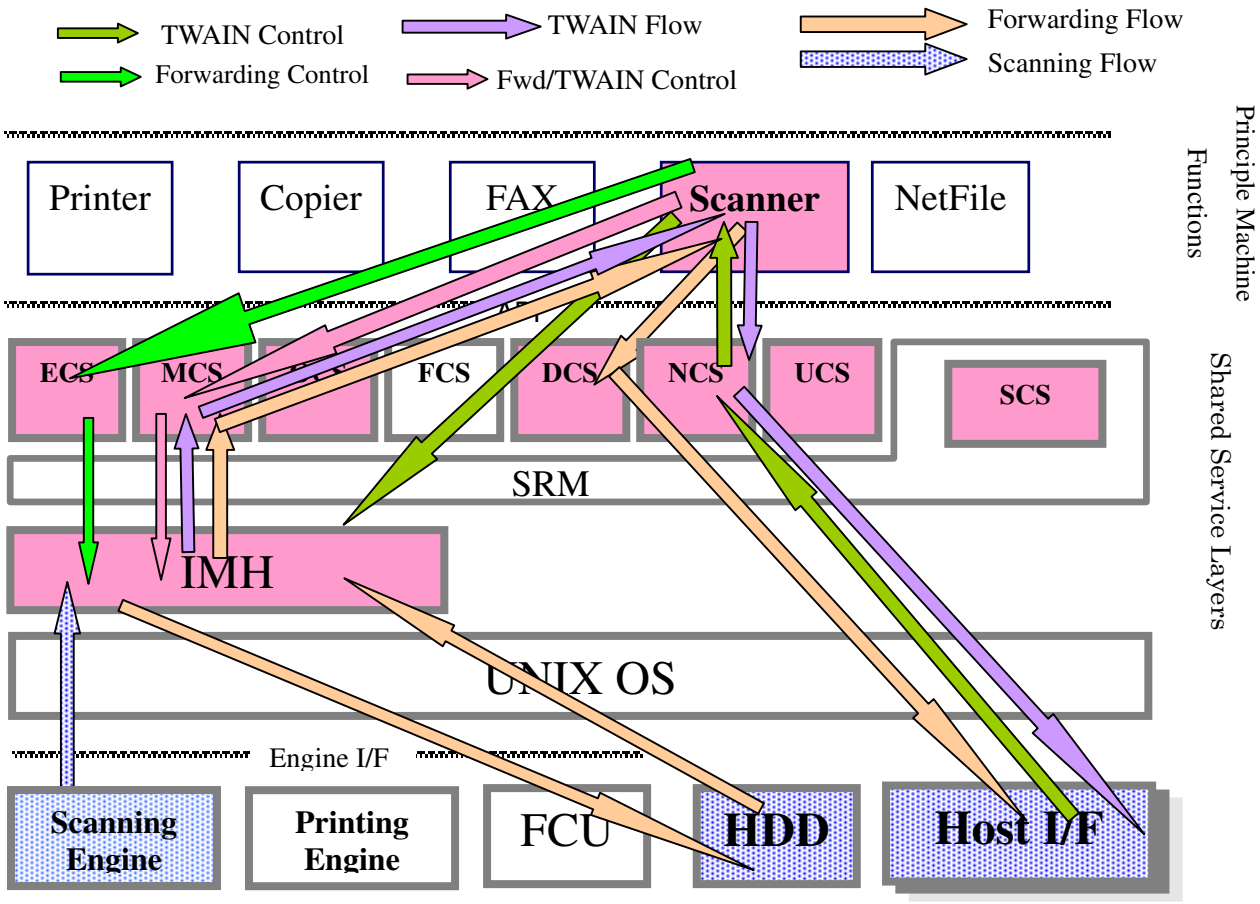
- It is possible to set the machine/related software to perform the following operations:
  - Require user code and password authentication before data is forwarded to an SMTP server, FTP server or Windows PC.
  - Encrypt the password sent to an SMTP server or Windows PC using Digest-MD5 or CRAM-MD5 encryption.
  - Require pre-approval from the POP server for connection to the SMTP server (POP before SMTP).
  - Require User Code and password authentication for obtaining email addresses from the LDAP server for use as Scan to Email destinations, as well as encrypt the password with Digest-MD5 or CRAM-MD5 encryption.
  - Require User Code authentication before storing an email destination obtained from the LDAP server in the MFP.
  - Require a numerical password (up to 8 digits long) when selecting an FTP or SMB destination stored in the MFP.
  - Require a numerical password (up to 8 digits long) when selecting the sender (MAIL FROM:) for transmissions to ScanRouter V2 as well as for Scan to Email, preventing any potential illegal use of this information.
  - Require that the sender (MAIL FROM:) be specified when sending to ScanRouter V2.

The security features described above are disabled at the time the product is shipped from the factory, but can be enabled and changed at the discretion of the machine administrator. Any changes in these settings requires the administrator's numerical password (6 to 8 digits long).

2.4.4 Terminology

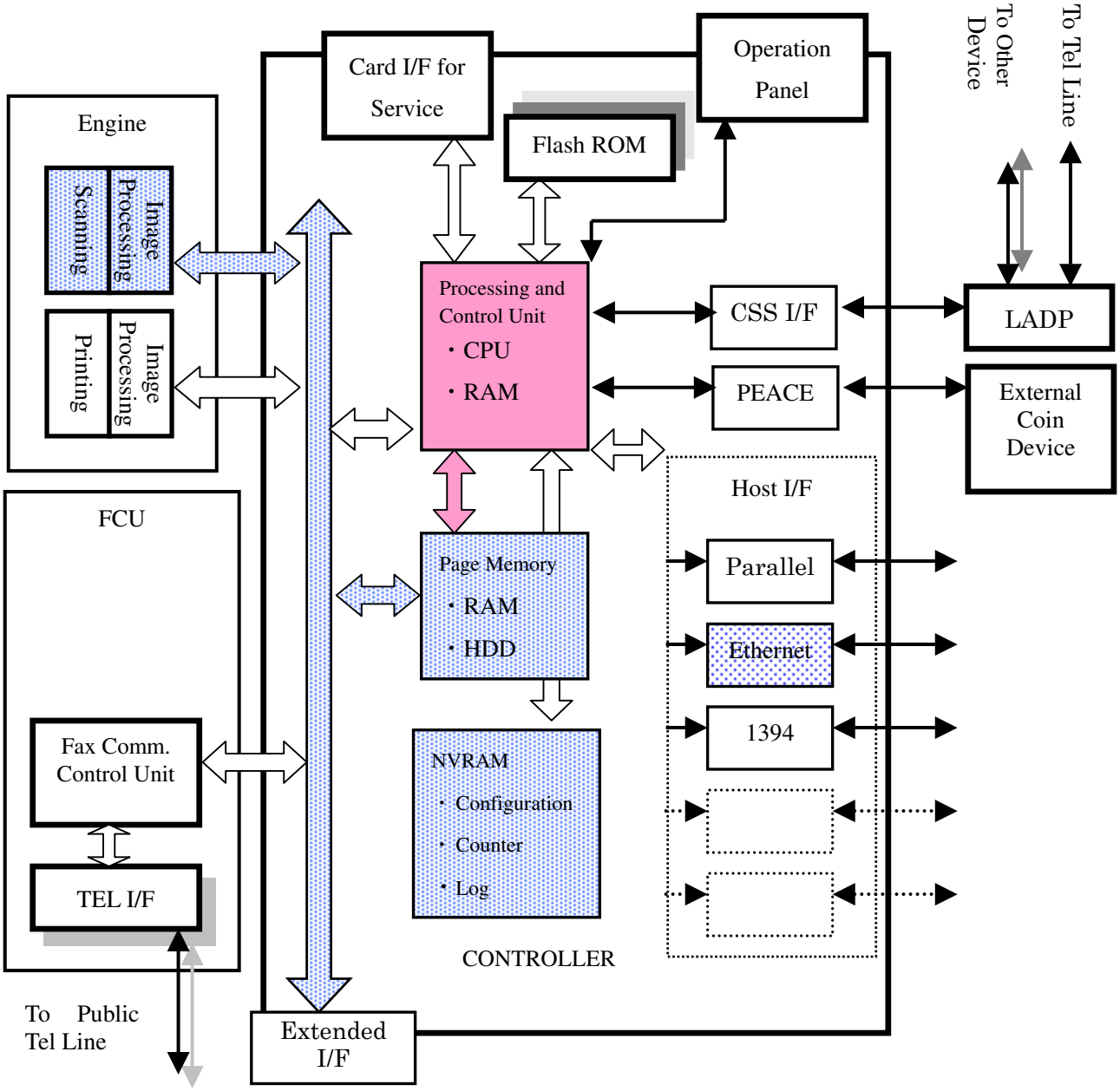
- **SMTP** (Simple Mail Transfer Protocol) [RFC2822]: A protocol used for the transmission of email over the Internet.
- **SMTP-AUTH** (SMTP AUTHentication) [RFC2554]: The protocol used for authentication when connecting to an SMTP server.
- **POP3** [RFC1939]: An email transfer protocol used when receiving email.
- **POP Before SMTP**: An authentication mechanism using POP3 protocol, developed to guard against SPAM mail (email sent indiscriminately to a large number of destinations).
- **SASL** (Simple Authentication and Security Layer) [RFC2222]: A framework that provides a common authentication processing mechanism for protocols that may require authentication, such as SMTP, POP3 and LDAP.
- **CRAM-MD5** [RFC2195]: A message digest functional algorithm that uses the MD5 algorithm to encrypt the challenge string and password.
- **DIGEST-MD5** [RFC2831]: A message digest functional algorithm developed as a countermeasure to dictionary and brute-force attacks. DIGEST-MD5 also supports realm designation (FQDN).
- **LDAP** (Lightweight Directory Access Protocol) [RFC1777], [RFC2251]: A protocol used for accessing directory services that manage items such as user address books.
- **SMB** (Server Message Block): A protocol used to enable file sharing between Windows PCs.
- **FTP** (File Transfer Protocol): A protocol used when transferring files over a TCP/IP network.

Software Flow



Data Flow

■**Scanning**



2.5 FAX

2.5.1 Overview of Fax Operations

- The FAX function sends the scanned image data from the scanner unit through a telecommunications line to other party's machine as a standard G3 or G4 FAX. Conversely, the machine will only accept incoming FAXes that conform to G3/G4 standards. The incoming document is then forwarded on to the printer unit for printing out.

- For Internet FAX transmission, the scanned image data is sent to the DCS, where it is converted into file attachment format for email transmission, after which it is sent to its destination via the network I/F. Conversely, the email-FAX data received as an Internet FAX is converted into image data and then forwarded on to the printer unit for printing out.

- It is possible to store transmission files in the Document Server for sending at a later time. The file is saved to the machine's hard drive, after which commands can be issued from the operation panel or through the network to send the file to its destination. Conversely, incoming FAXes can be stored I the Document Server for printing out at a later time. The incoming FAX is saved to the machine's hard drive, after which commands can be issued from the operation panel or via the network to print the file out.

- With PC FAX transmission, the image data received from the PC is then sent to its destination via a telecommunications line or network I/F.

- Restrictions can be placed on all FAX transmission operations, including Internet FAX, with the use of User Codes. For reception, it is possible to configure the machine to receive only those transmissions accompanied by a predetermined code. Operational log entries are made for each transmission and reception job, and are non-volatile, i.e. permanent. These entries can be viewed by printing out the Journal.

2.5.2 Data Flow

- FAX transmission is initiated from the operation panel, after which the scanning command is sent to the ECS via the FCS and the scanner engine is activated. At the same time, a transmission command is sent to the FCU via the FCUH. The image data in memory is then sent from the scanning unit to the FCU, and sent to its destination via the G3 or G4 line.

- With Internet FAX transmission, the image data is sent from the FCU to the HDD and then on to the host I/F, which sends the data to its destination via the network. The FAX data is then erased once it has been received by its destination, or once the maximum number of transmission retries has been reached.

- FAX reception begins when an incoming FAX is received by the FCU via the line I/F, after which the FCU sends the print command to the FAX function via the FCUH and FCS. This command is then transferred to the ECS via the FCS, and the printing engine is activated.

- With Internet FAX reception, the incoming data from the network is sent to the HDD and then on to the FCU, where it is stored. The data flow following this for printing out the file is the same as described in the paragraph above.

- With FAX Reception Document Server files, the incoming FAX is stored to the Document Server on the machine's HDD.

- With PC-FAX transmission, the data sent from the PC is stored in the machine's HDD or FCU if the machine does not have a hard drive. The transmission flow following this is the same as described above.

2.5.3 Data Security Considerations

- The FCU supports only G3 and G4 FAX protocols. Therefore, even if a connection is established with a terminal not using these protocols, the machine will view this as a communication failure and terminate the connection. This prevents access from telecommunications lines to internal networks via the FCU, and ensures that no illegal data can be introduced via these lines.

- Internet FAX supports TIFF files and text-based email only, which is true for both reception and transmission. If the data received through this function is in any other format, a communication error will result.

- Internet FAX can also be set to forward incoming FAXes to specific destinations preset in the machine. With servers using SMTP reception/delivery, the receiver can set the server to prohibit the delivery of incoming Internet FAX documents from specific senders, restricting SMTP access.

- With PC FAX transmission, the language processing subsystem is only able to process data that conforms to PC-FAX standards. If any other type of data is received, an error will result and the processing is terminated.

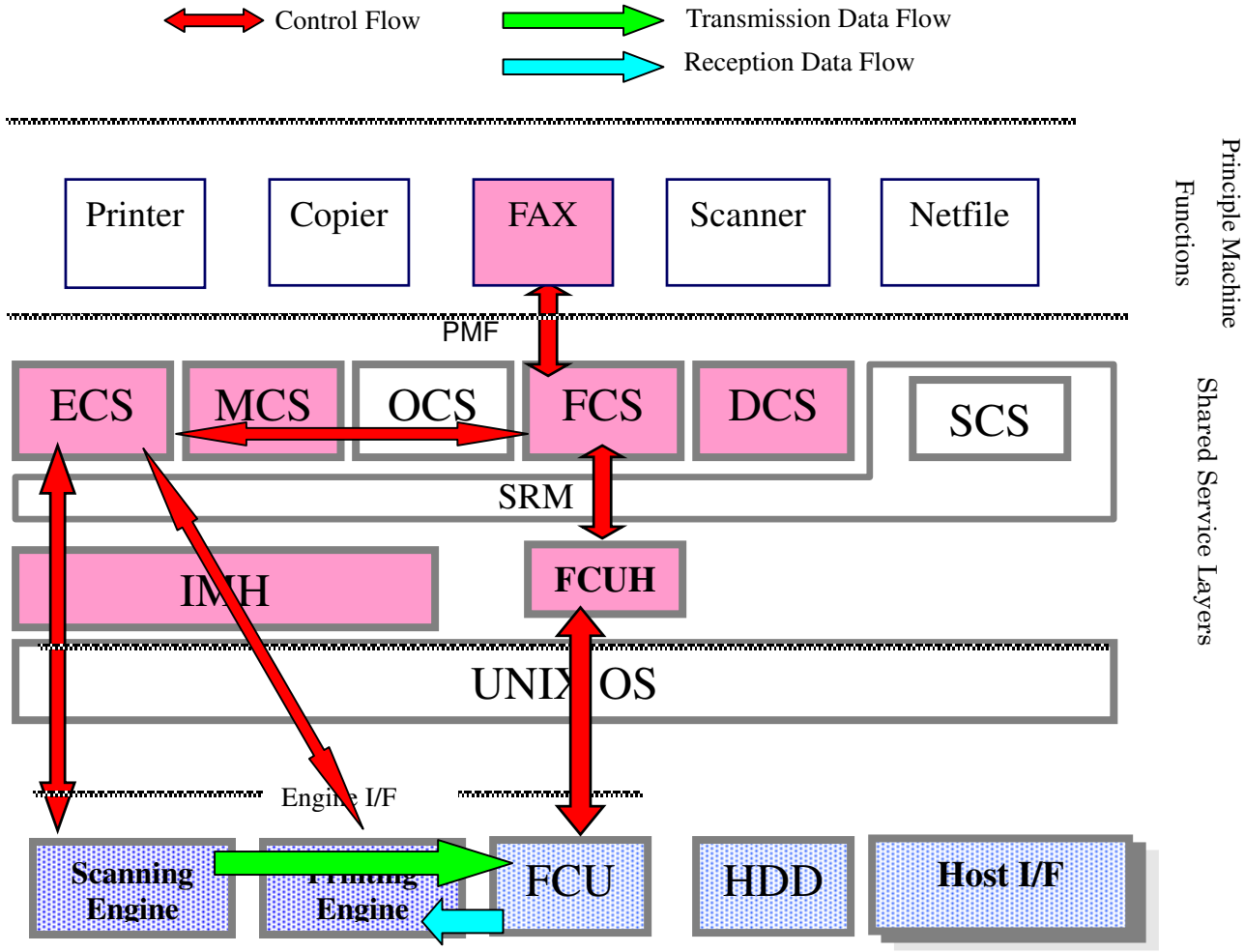
- For more details, please refer to section *2.4 Scanner.*

Note:

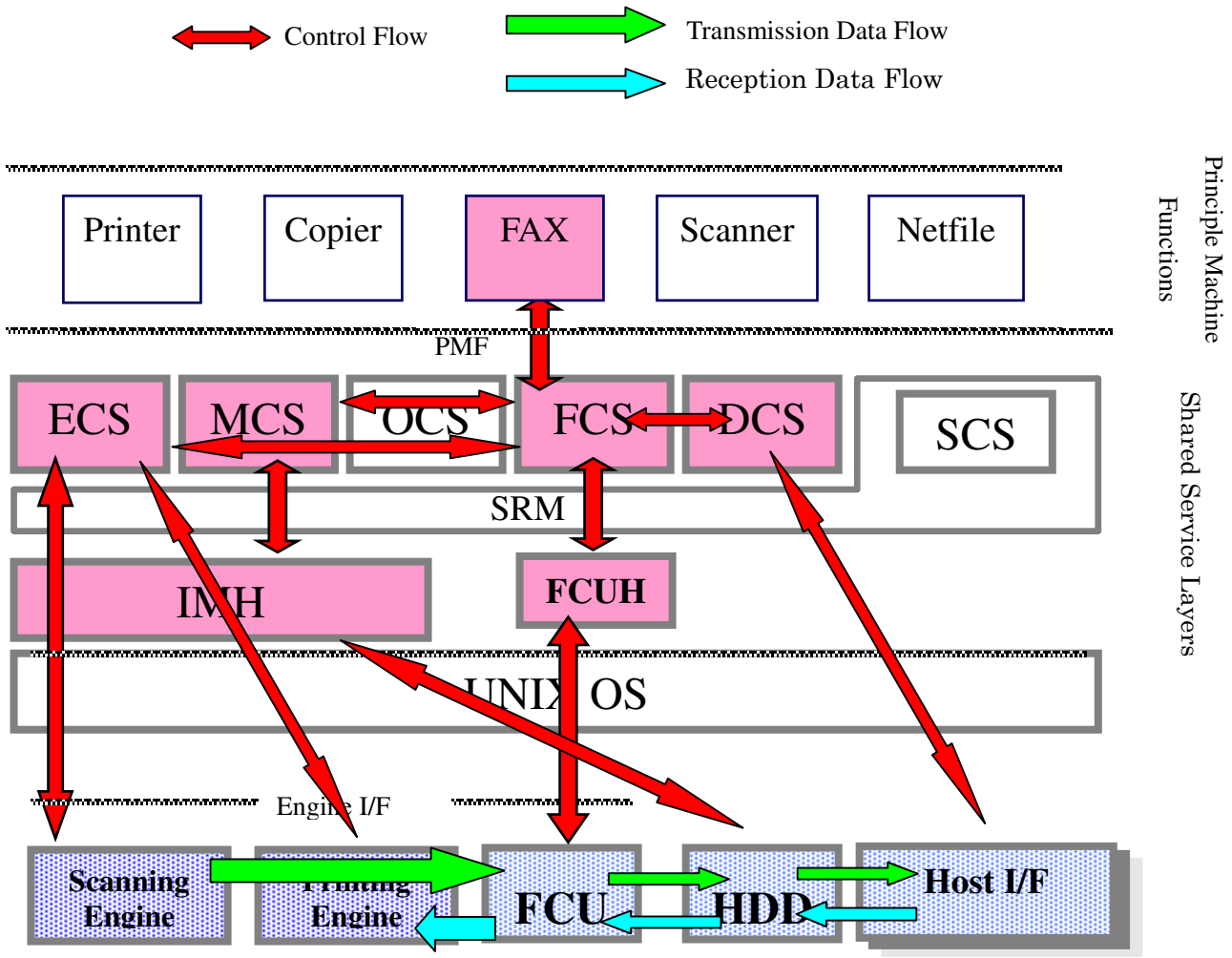
1. The access control used for SMTP reception/delivery operates in accordance with RFC2305.
2. The SMTP-AUTH feature operates in accordance with RFC2554.

Software Flow

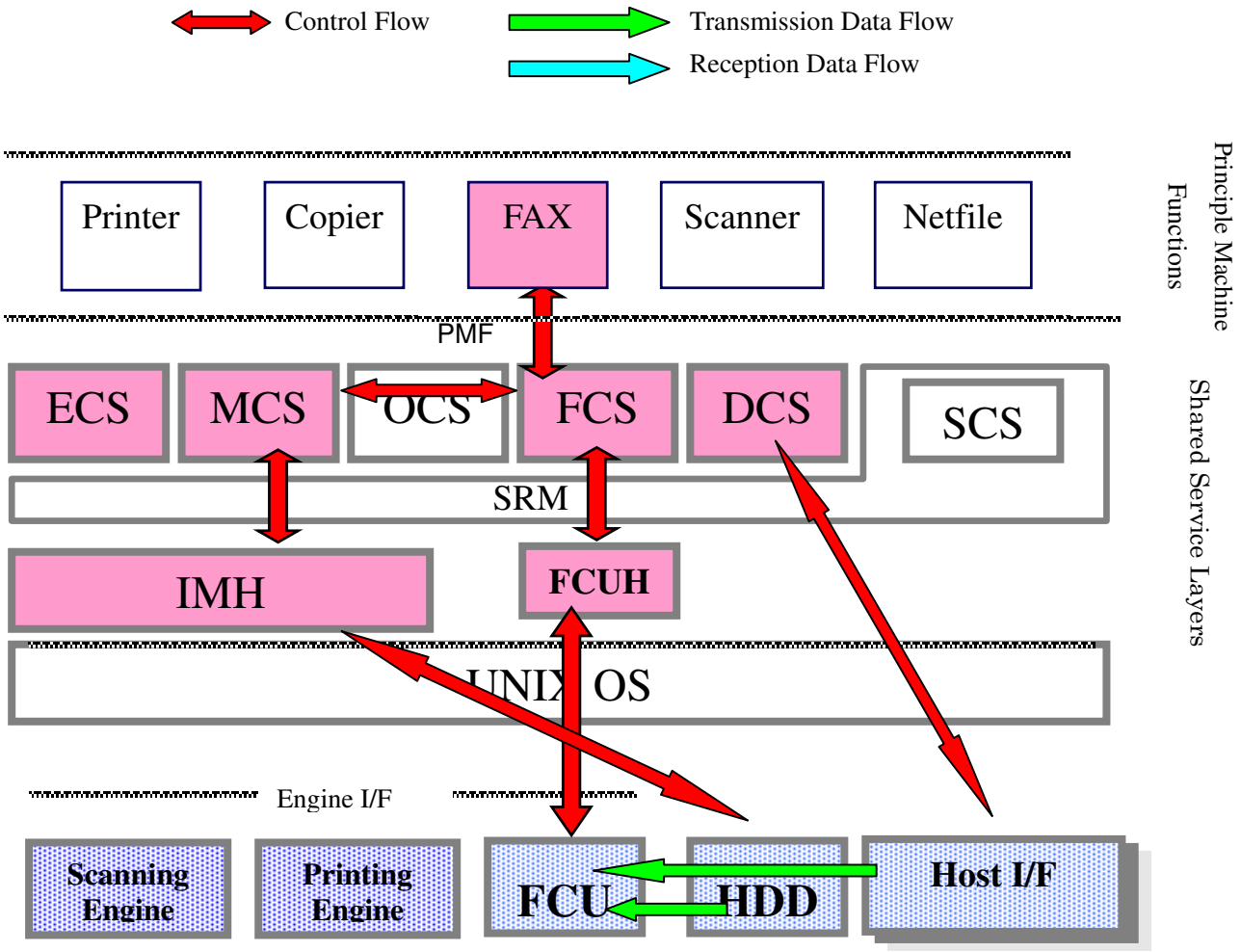
■ **Fax Transmission/Reception**



■ **Internet Fax: Transmission of Scanned Data, Reception of Data via Network**

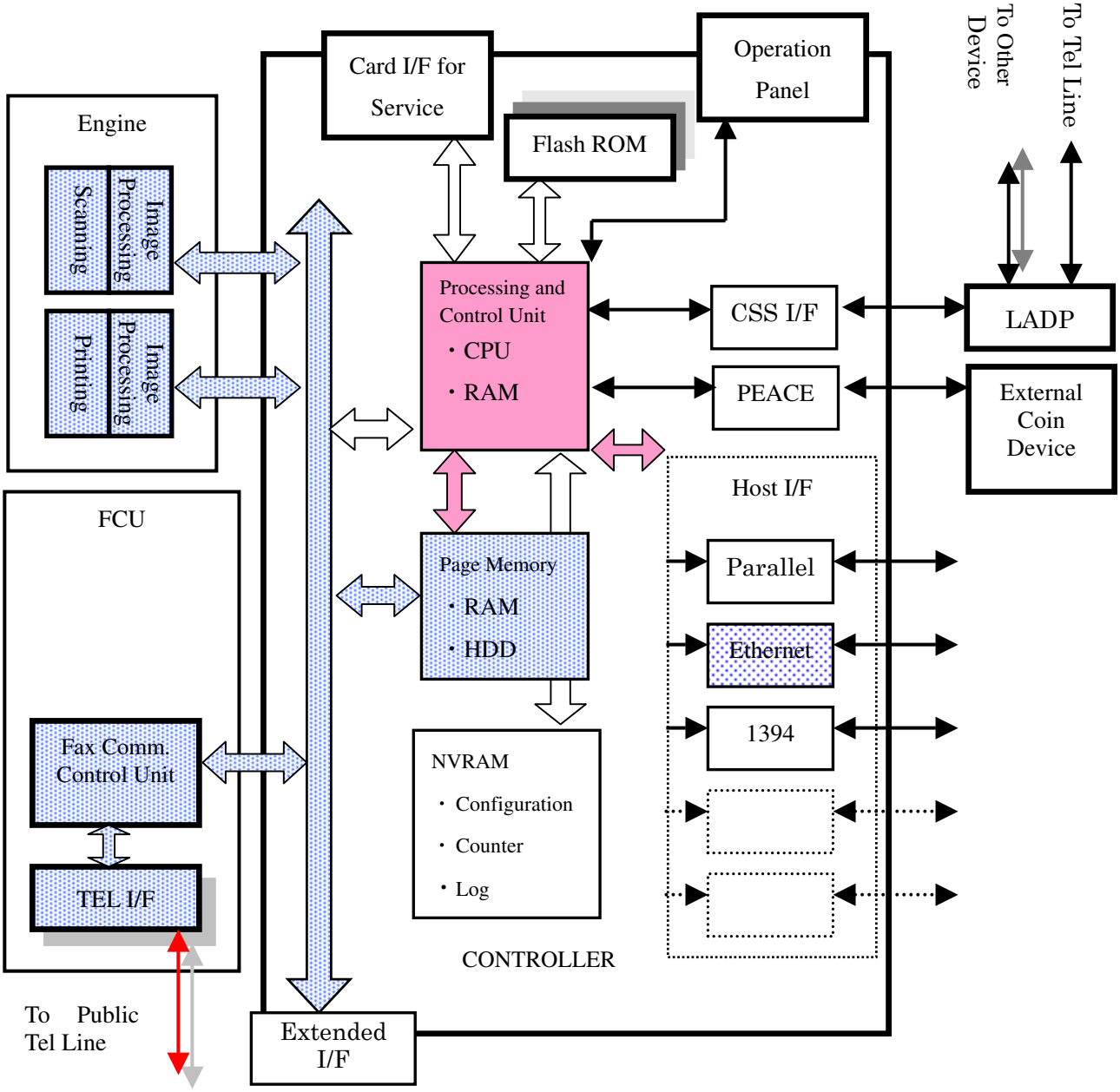


■ **PC Fax Transmission**



Data Flow

■**FAX**



2.6 NetFile

2.6.1 Overview of NetFile Operations

- The NetFile function operates in correspondence with the DeskTopBinder V2 and Ridoc Edit Manager Pro applications installed on a network-connected client PC. When the machine saves a document from any of its principle functions to the HDD for permanent storage, a thumbnail image of the first page is created, which can then be sent to DeskTopBinder V2 or Ridoc Edit Manager Pro upon request.

- If the MLB is installed, thumbnails can be created and sent to the above applications for all other pages upon request.

- NetFile can also modify the filename and other properties of the stored documents, according to the instructions issued by the operator from these two applications.

- In addition, NetFile is able to send these applications the full-sized images of documents stored using any of the primary machine functions. However, since copier and printer documents are stored in Ricoh original file format, the MLB is necessary to convert them into commonly-used file formats such as JPEG or TIFF.

- When restoring copier or printer or printer files originally sent to Ridoc Edit Manager Pro via the MLB as TIFF/JPEG2000 data at full-size back to the machine, the MLB converts the data back to its Ricoh original format and stores it in the HDD. Since these files are stored separately from their original counterparts, it is not possible to corrupt or damage image files already stored in the HDD with illegal data.

- It is possible to perform the following operations from DeskTopBinder V2 and Ridoc Edit Manager Pro:
  - Print out documents that were stored using the Copier, FAX and Printer functions, as well as documents restored to the machine from Ridoc Edit Manager Pro
  - Forward documents stored with the Scanner function to ScanRouter V2
  - Send documents stored with the FAX function as facsimiles

- When the relevant machine settings are enabled, the machine will place controls on the printing or FAX transmission of stored documents based on the user information registered in DeskTopBinder V2 and Ridoc Edit Manager Pro. Similarly, a password is required whenever performing operations on these documents from these two applications.

2.6.2 Data Flow

Creating thumbnails

When the MLB is not installed, the MCS uses its modules to create thumbnails of the first page of images stored in the HDD. When the MLB is installed, the IMH uses its modules and the MLB to create these thumbnails. The data from the first page of the file is read into memory, after which a thumbnail is created while the image is in memory (MCS), or after the MLB compresses the image and converts the file format (IMH). When the MLB is installed, and a request is sent for thumbnails of page 2 or onward from Ridoc Edit Manager Pro, Netfile sends the request to the IMH via the MCS. The IMH then generates the thumbnail for the requested page(s) in the same way as described above for page 1. In all cases, the thumbnail file created is stored and managed in the machine HDD. The file format is JPEG (JFIF).

Sending thumbnails

To send a copy of the thumbnail file to DeskTopBinder V2 or Ridoc Edit Manager Pro, the thumbnail file stored in the HDD is read directly into Image Memory and then sent to the PC via the NCS.

Deleting thumbnails

When the number of thumbnails for pages 2 and onward created by requests from Ridoc Edit Manager Pro reaches a certain limit, Netfile will choose the oldest thumbnail and send a request to the MCS to delete it, after which the MCS deletes the specified thumbnail from HDD memory. Also, the MCS deletes all thumbnails for pages 2 and onward from HDD memory whenever the main power is turned on or a system reset is performed.

Sending stored images to the PC

The image data stored in the HDD is read directly into Image Memory via the MCS, and then sent over the network via the NCS to one of the two PC applications above. The IMH uses its modules and the MLB to convert the Copier and Printer documents from their Ricoh original format into a commonly-used format (JPEG or TIFF). Note that although the MLB must be installed to perform this operation on Copier and Printer documents, this board is not necessary to do the same for Scanner or FAX transmission documents.

In addition, on MFP models that support direct storage of incoming FAX documents to the HDD, it is possible to send these stored FAX documents directly to DeskTopBinder V2. The data flow for this process is the same as described in the paragraph above. As with the above operations, such FAX operations do not require the MLB.

Restoring images back to the machine

When restoring copier or printer documents captured to Ridoc Edit Manager Pro with full-size TIFF or JPEG2000 format back to the machine, the data is sent to and stored in the HDD via the host IF, NCS and MCS (reverse pathway of that described above). Before storage, the IMH uses its modules and the MLB to convert the file format from TIFF/JPEG2000 back to Ricoh original format. These restored files are saved in a separate location than their original counterparts.

Printing out stored documents

When printing out documents stored in the machine from DeskTopBinder V2 or Ridoc Edit Manager Pro, the print command for the specified file is sent to the ECS. However with some MFP models, Netfile sends this command via the program modules used to print out Copier documents stored on the MFP hard drive, after which it is forwarded on to the ECS. The ECS, in tandem with the IMH, loads the image out of HDD storage and prints it out via the printing engine.

Forwarding stored scanner documents

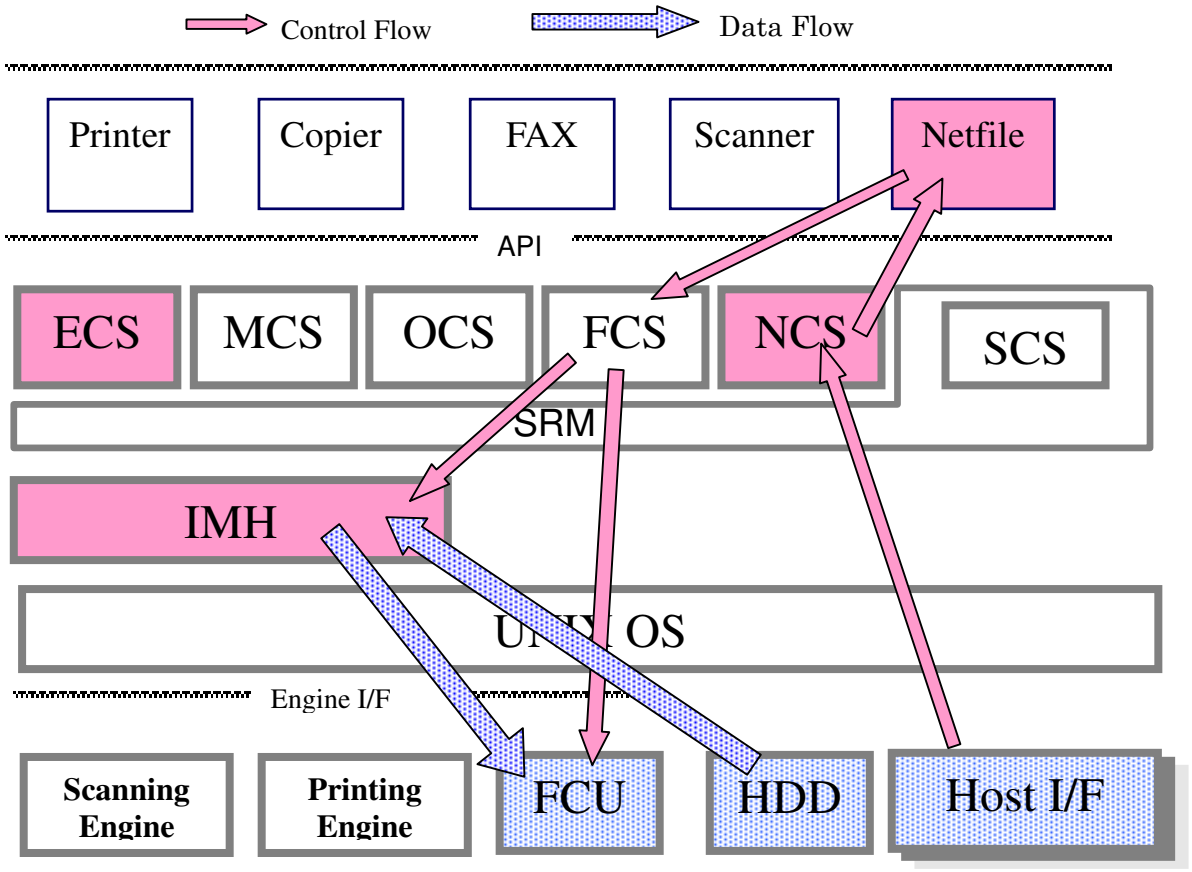
When forwarding Scanner documents stored in the machine from DeskTopBinder V2 or Ridoc Edit Manager Pro, the Forwarding command for the specified file is sent to the Scanner function's Forwarding module. The module, in tandem with the MCS and IMH, loads the image out of HDD storage and forwards it to ScanRouter V2 via the NCS.

User Codes, passwords and other secondary document data

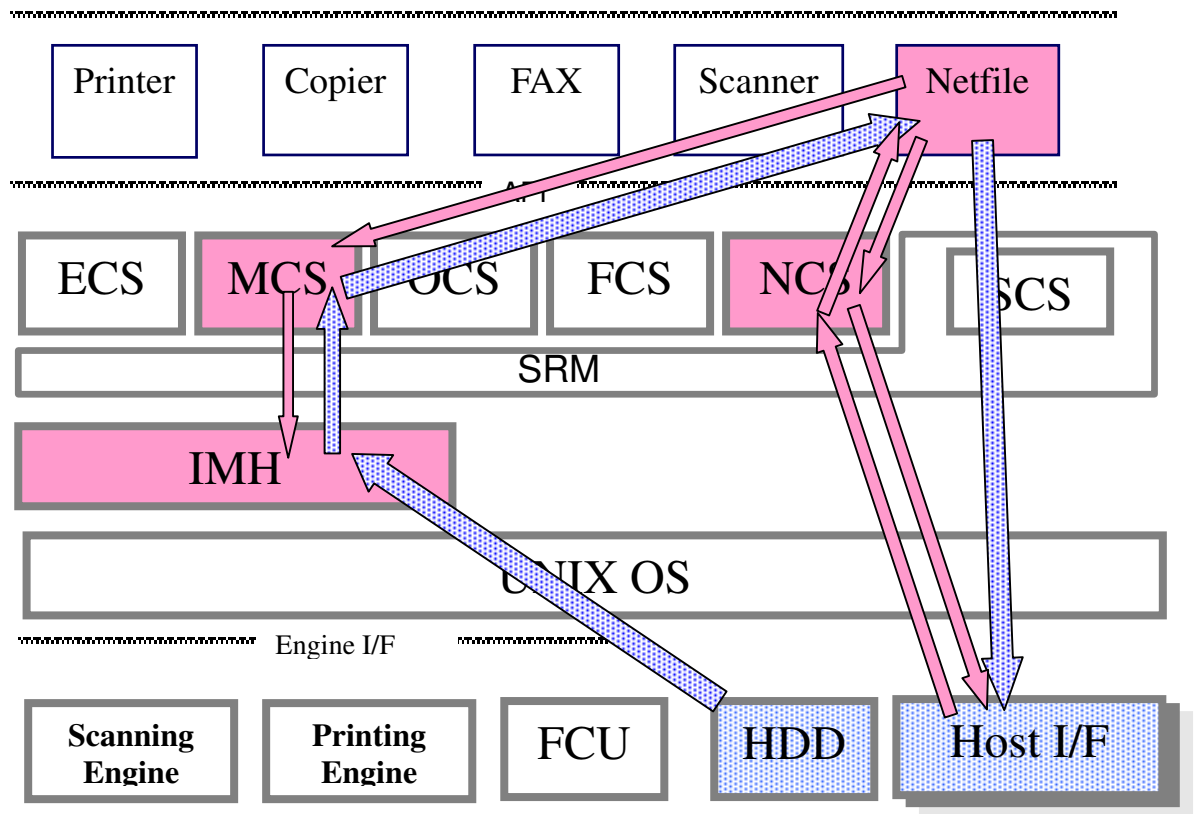
For password-protected documents, a password is always necessary whenever performing any operation from DeskTopBinder V2 or Ridoc Edit Manager Pro installed on a network PC. When communicating with either of these PC applications, the machine exchanges XML text through http protocol, which contains the necessary user code and password information. However since these are encrypted before being sent, even in the event that the transmission were intercepted, it would be impossible to decipher the contents.

Software Flows I, II

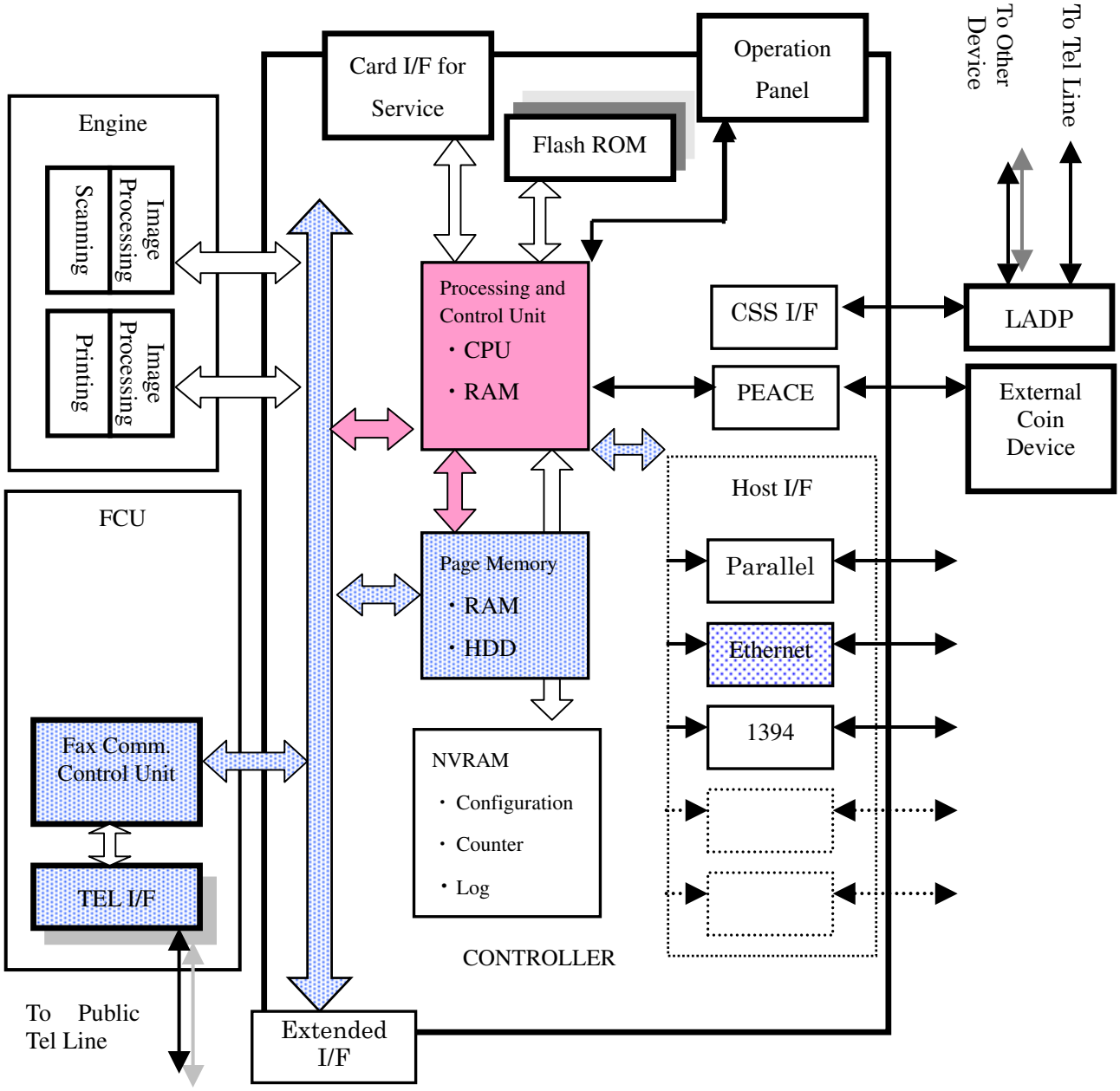
I.



II.



Data Flow


To Other Device
To Tel Line
Card I/F for Service
Operation Panel
Flash ROM
Engine
Scanning
Image Processing
Printing
Image Processing
Processing and Control Unit
・CPU
・RAM
CSS I/F
LADP
PEACE
External Coin Device
Host I/F
FCU
Page Memory
・RAM
・HDD
Parallel
Ethernet
1394
Fax Comm. Control Unit
TEL I/F
NVRAM
・Configuration
・Counter
・Log
CONTROLLER
To Public Tel Line
Extended I/F

2.6.3 Data Security Considerations

Conditions necessary for reusing stored documents

It is possible to protect stored documents with a password. In order to reuse these documents or their thumbnails, it is necessary to input the correct password first. Otherwise, the machine will prohibit such operations. In addition, when Extended Security is enabled, just as with the password input screen on the machine operation panel, there is a limit to the number of times the password can be input from DeskTopBinder V2 and Ridoc Edit Manager Pro to perform operations on stored documents. If the operator inputs an incorrect password in excess of the maximum allowable tries, the machine inhibits any further operations on the protected document, preventing any illegal use of the data by a third party.

DeskTopBinder V2, Ridoc Edit Manager Pro and the MFP product contain an access restriction feature whereby each function can be enabled or disabled for each user. To do this, users must be registered in the MFP as well as the software application. In addition, with the use of User Codes registered in the MFP FAX function, it is possible to limit operations performed on FAX reception documents to specific users. Operators without a registered User Code are prohibited from performing operations on these documents.

Protection against the introduction of illegal data, programs

Netfile will reject any data that does not conform to its predetermined communication protocols, which precludes any possibility of such data from mixing together with any programs or data in the MFP or being released to the network.

Furthermore, even if a document restored to the machine from Ridoc Edit Manager Pro contained illegal data, the result would simply be a data conversion error by the MLB, and the illegal data would not be able to affect any of the documents or programs in the machine. In addition, since the restored documents (if accepted) are always stored in a separate location than their original counterparts, they would not be able to damage these original documents at all.

Due to these safeguards, there is no possibility of the introduction of illegal data or programs when restoring documents to the MFP product. In addition, all other image data correspondence between the machine and PC applications is unidirectional from the machine to the PC, which eliminates any possibility of the introduction of illegal data.