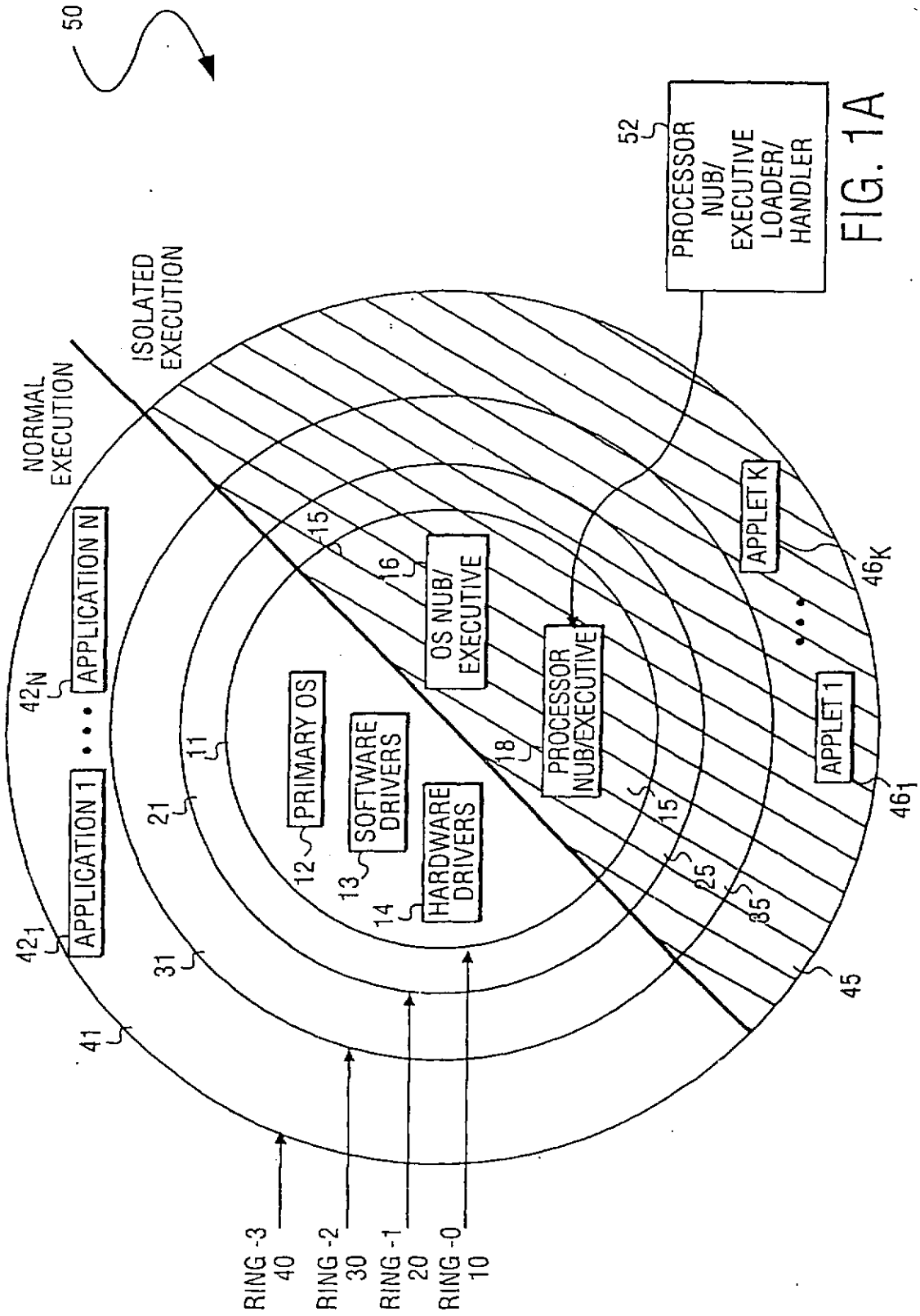

50
52
PROCESSOR NUB/ EXECUTIVE LOADER/ HANDLER
ISOLATED EXECUTION
NORMAL EXECUTION
APPLICATION N
APPLICATION 1
42N
421
41
31
21
11
PRIMARY OS
SOFTWARE DRIVERS
HARDWARE DRIVERS
12
13
14
15
16
OS NUB/ EXECUTIVE
18
PROCESSOR NUB/EXECUTIVE
APPLET K
APPLET 1
46K
461
45
25
35
RING -3 40
RING -2 30
RING -1 20
RING -0 10

FIG. 1A

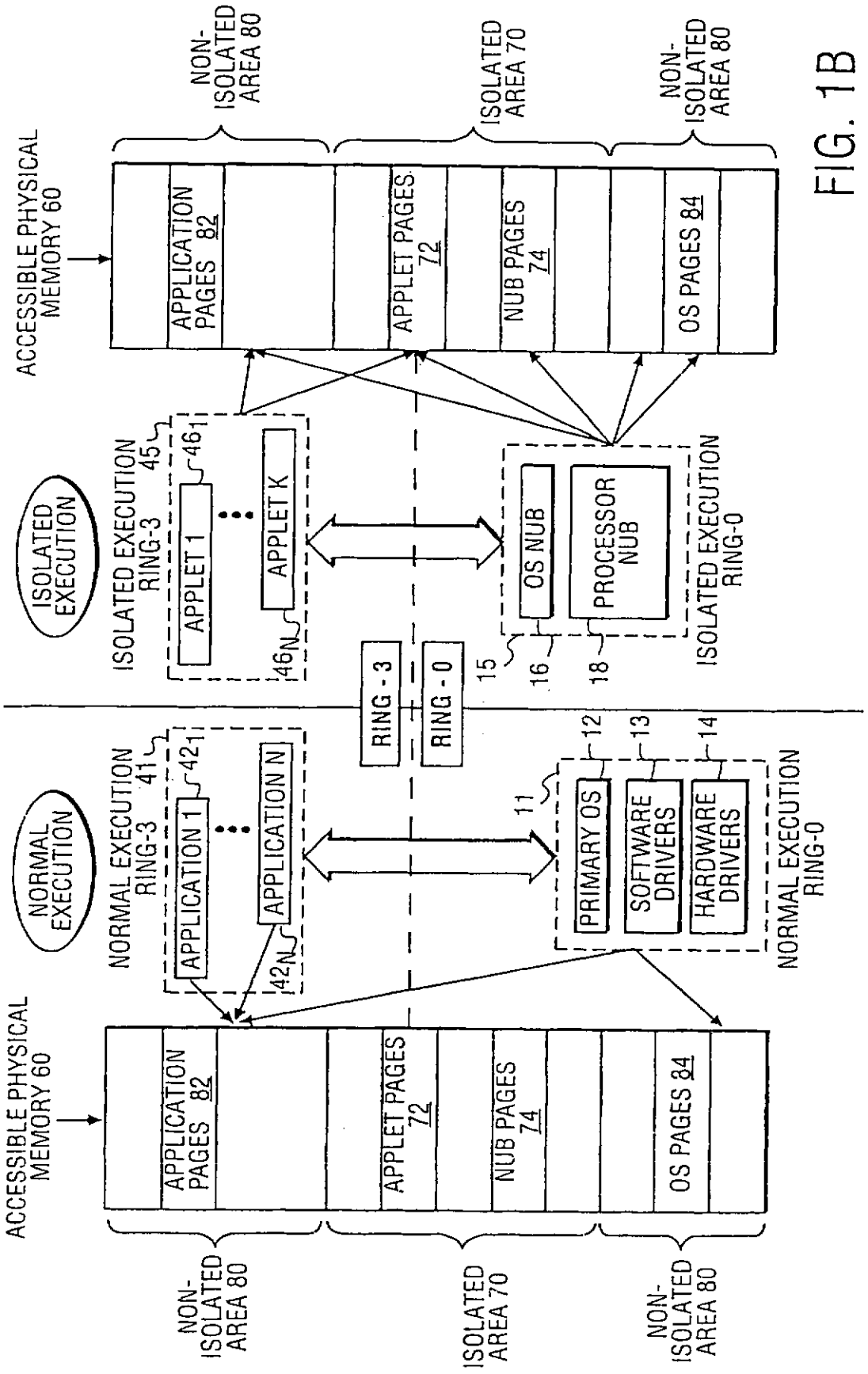

ACCESSIBLE PHYSICAL MEMORY 60
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
ISOLATED EXECUTION
ISOLATED EXECUTION RING-3 45
APPLET 1 46_1
APPLET K 46_N
OS NUB 16
PROCESSOR NUB 18
ISOLATED EXECUTION RING-0
RING - 3
RING - 0
15
NORMAL EXECUTION
NORMAL EXECUTION RING-3 41
APPLICATION 1 42_1
APPLICATION N 42_N
11
PRIMARY OS 12
SOFTWARE DRIVERS 13
HARDWARE DRIVERS 14
NORMAL EXECUTION RING-0
ACCESSIBLE PHYSICAL MEMORY 60
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80

FIG. 1B

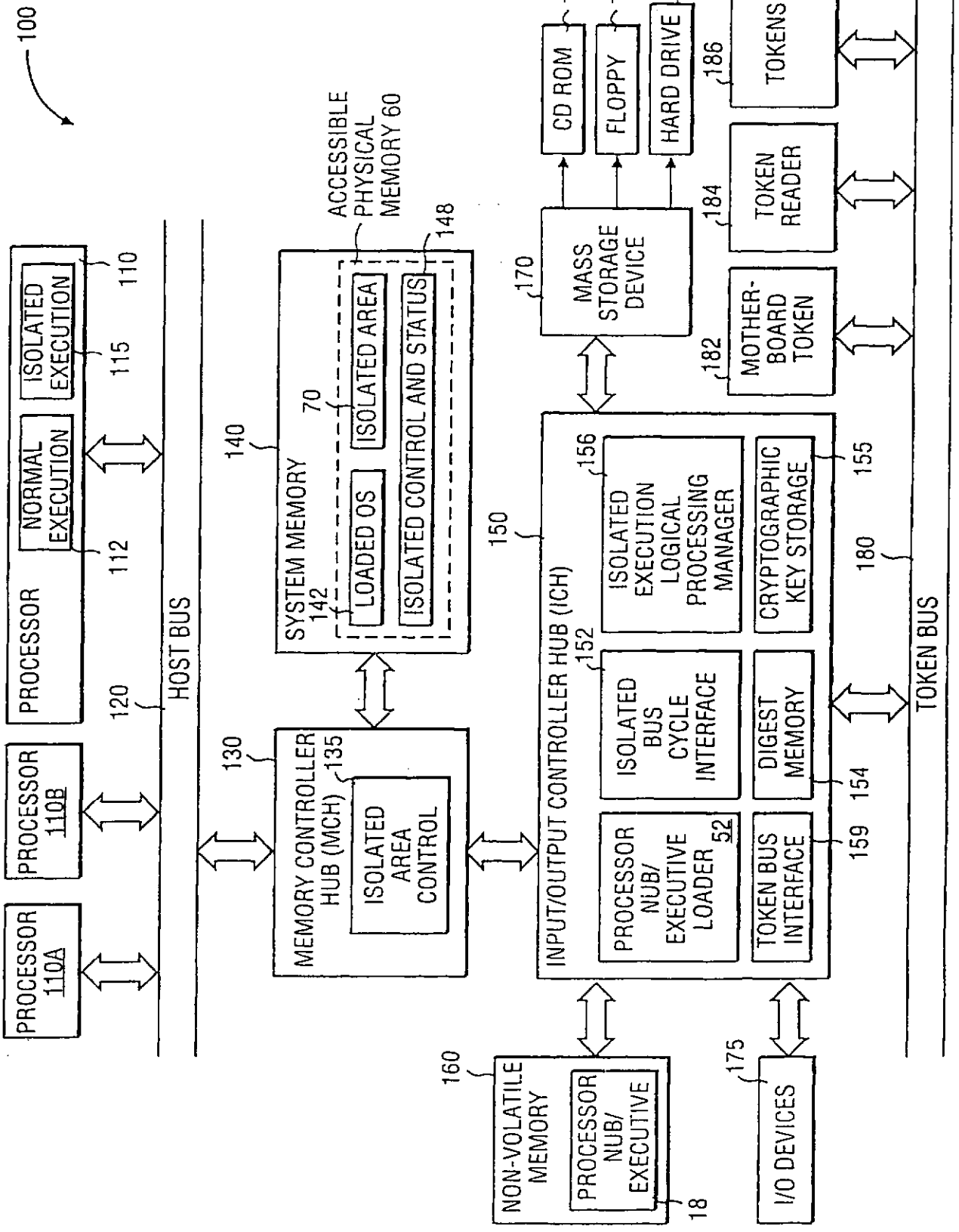

100
PROCESSOR 110A
PROCESSOR 110B
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
110
115
112
120
HOST BUS
130
MEMORY CONTROLLER HUB (MCH)
135
ISOLATED AREA CONTROL
140
SYSTEM MEMORY
142
LOADED OS
ISOLATED AREA
ISOLATED CONTROL AND STATUS
148
ACCESSIBLE PHYSICAL MEMORY 60
150
INPUT/OUTPUT CONTROLLER HUB (ICH)
152
ISOLATED BUS CYCLE INTERFACE
156
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
155
CRYPTOGRAPHIC KEY STORAGE
154
DIGEST MEMORY
159
TOKEN BUS INTERFACE
PROCESSOR NUB/ EXECUTIVE LOADER 52
180
TOKEN BUS
160
NON-VOLATILE MEMORY
PROCESSOR NUB/ EXECUTIVE
18
175
I/O DEVICES
170
MASS STORAGE DEVICE
172
CD ROM
174
FLOPPY
176
HARD DRIVE
182
MOTHER-BOARD TOKEN
184
TOKEN READER
186
TOKENS

FIG. 1C

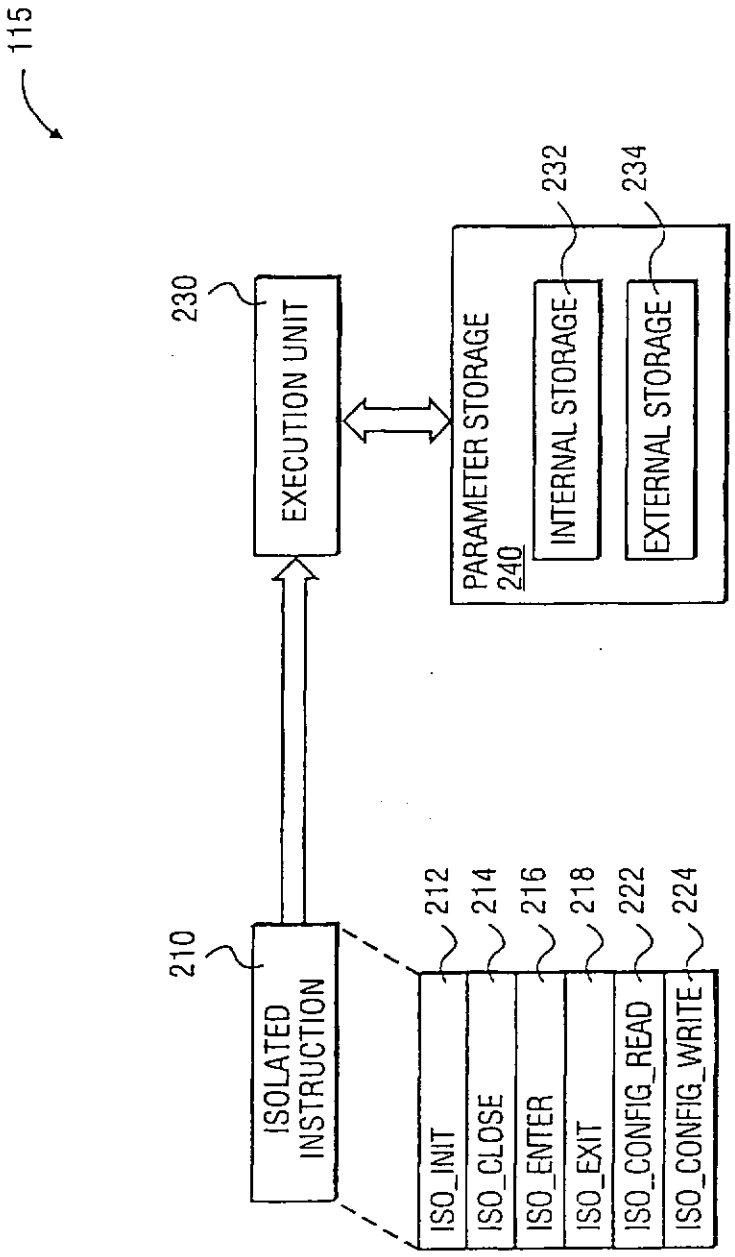

115
230
EXECUTION UNIT
232
234
PARAMETER STORAGE
240
INTERNAL STORAGE
EXTERNAL STORAGE
210
ISOLATED INSTRUCTION
212
214
216
218
222
224
ISO_INIT
ISO_CLOSE
ISO_ENTER
ISO_EXIT
ISO_CONFIG_READ
ISO_CONFIG_WRITE

FIG. 2

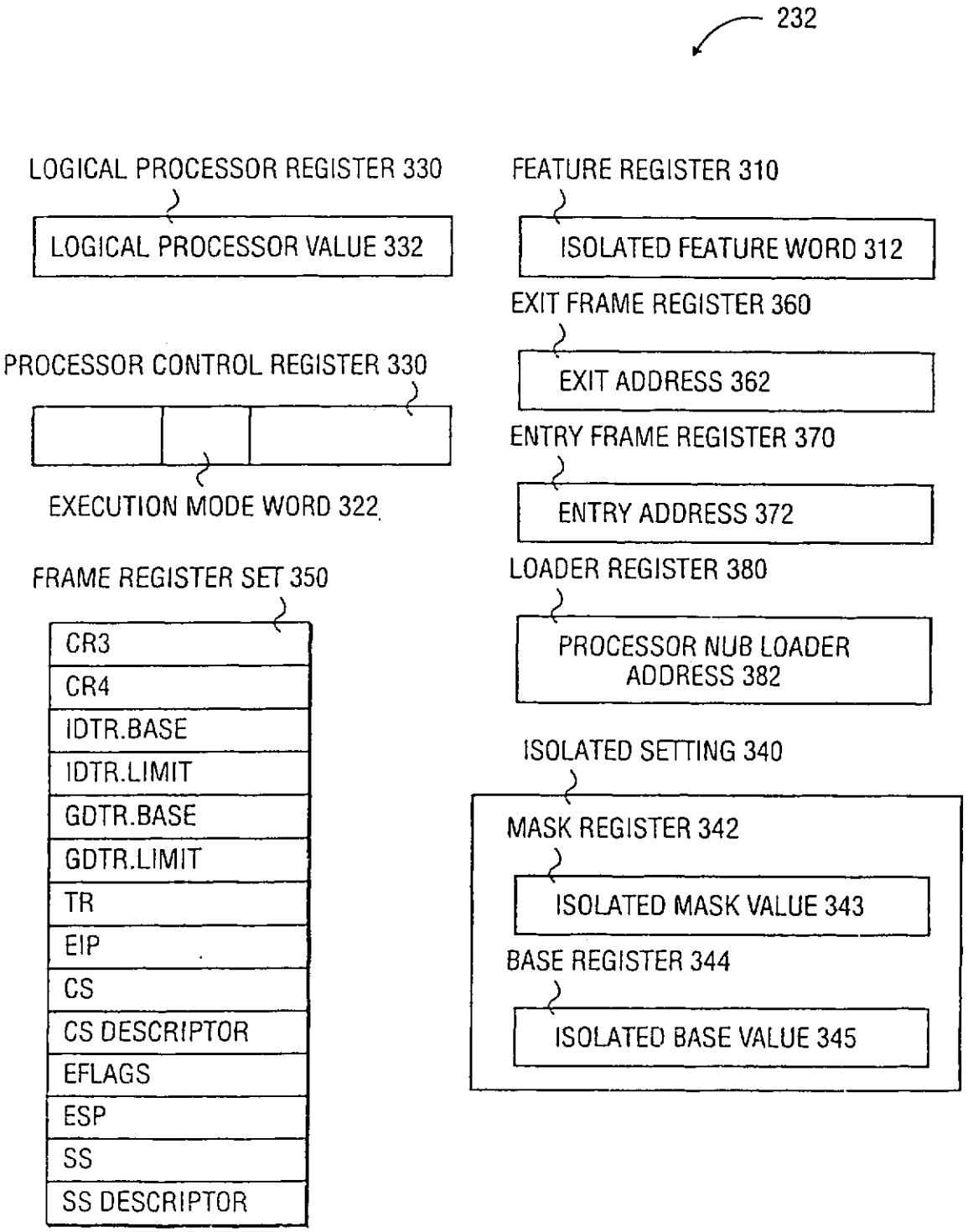

232
LOGICAL PROCESSOR REGISTER 330
LOGICAL PROCESSOR VALUE 332
PROCESSOR CONTROL REGISTER 330
EXECUTION MODE WORD 322
FRAME REGISTER SET 350
CR3
CR4
IDTR.BASE
IDTR.LIMIT
GDTR.BASE
GDTR.LIMIT
TR
EIP
CS
CS DESCRIPTOR
EFLAGS
ESP
SS
SS DESCRIPTOR
FEATURE REGISTER 310
ISOLATED FEATURE WORD 312
EXIT FRAME REGISTER 360
EXIT ADDRESS 362
ENTRY FRAME REGISTER 370
ENTRY ADDRESS 372
LOADER REGISTER 380
PROCESSOR NUB LOADER ADDRESS 382
ISOLATED SETTING 340
MASK REGISTER 342
ISOLATED MASK VALUE 343
BASE REGISTER 344
ISOLATED BASE VALUE 345

FIG. 3

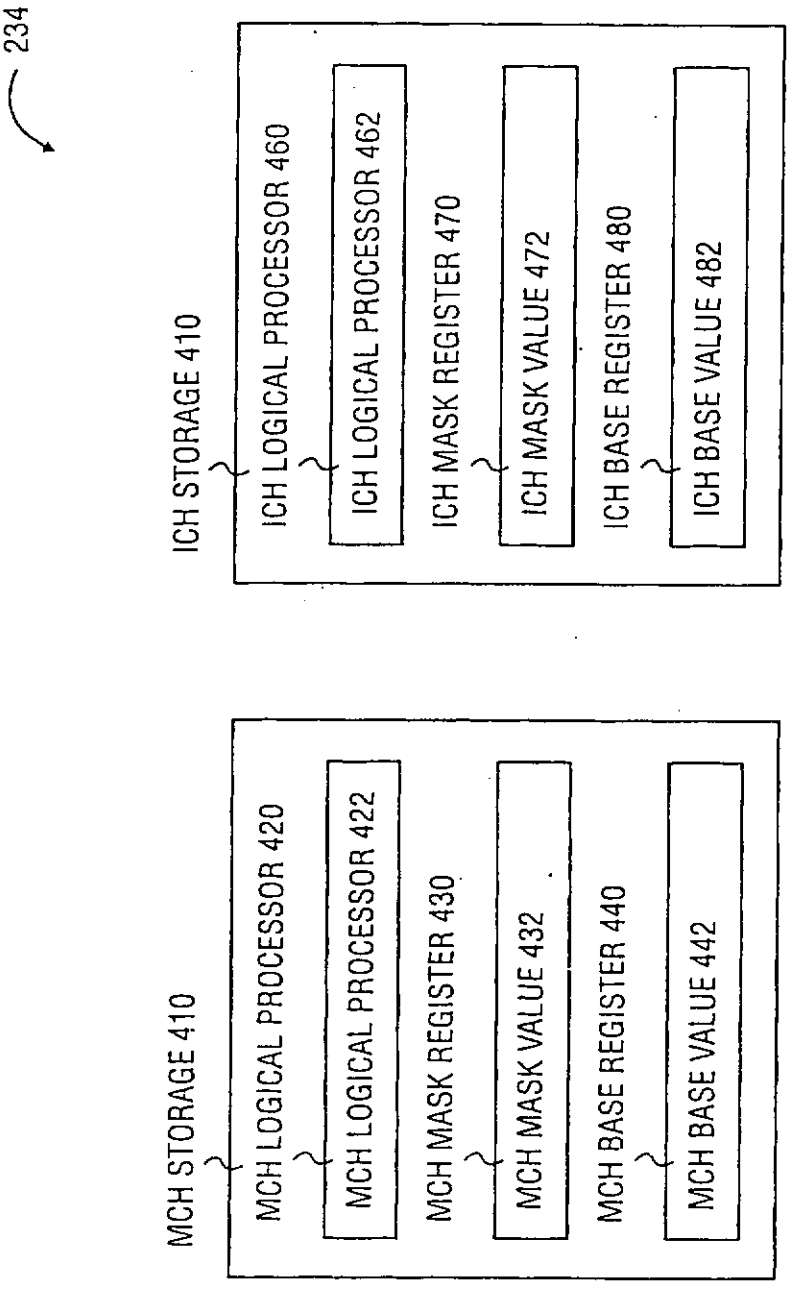

234
ICH STORAGE 410
ICH LOGICAL PROCESSOR 460
ICH LOGICAL PROCESSOR 462
ICH MASK REGISTER 470
ICH MASK VALUE 472
ICH BASE REGISTER 480
ICH BASE VALUE 482
MCH STORAGE 410
MCH LOGICAL PROCESSOR 420
MCH LOGICAL PROCESSOR 422
MCH MASK REGISTER 430
MCH MASK VALUE 432
MCH BASE REGISTER 440
MCH BASE VALUE 442

FIG. 4

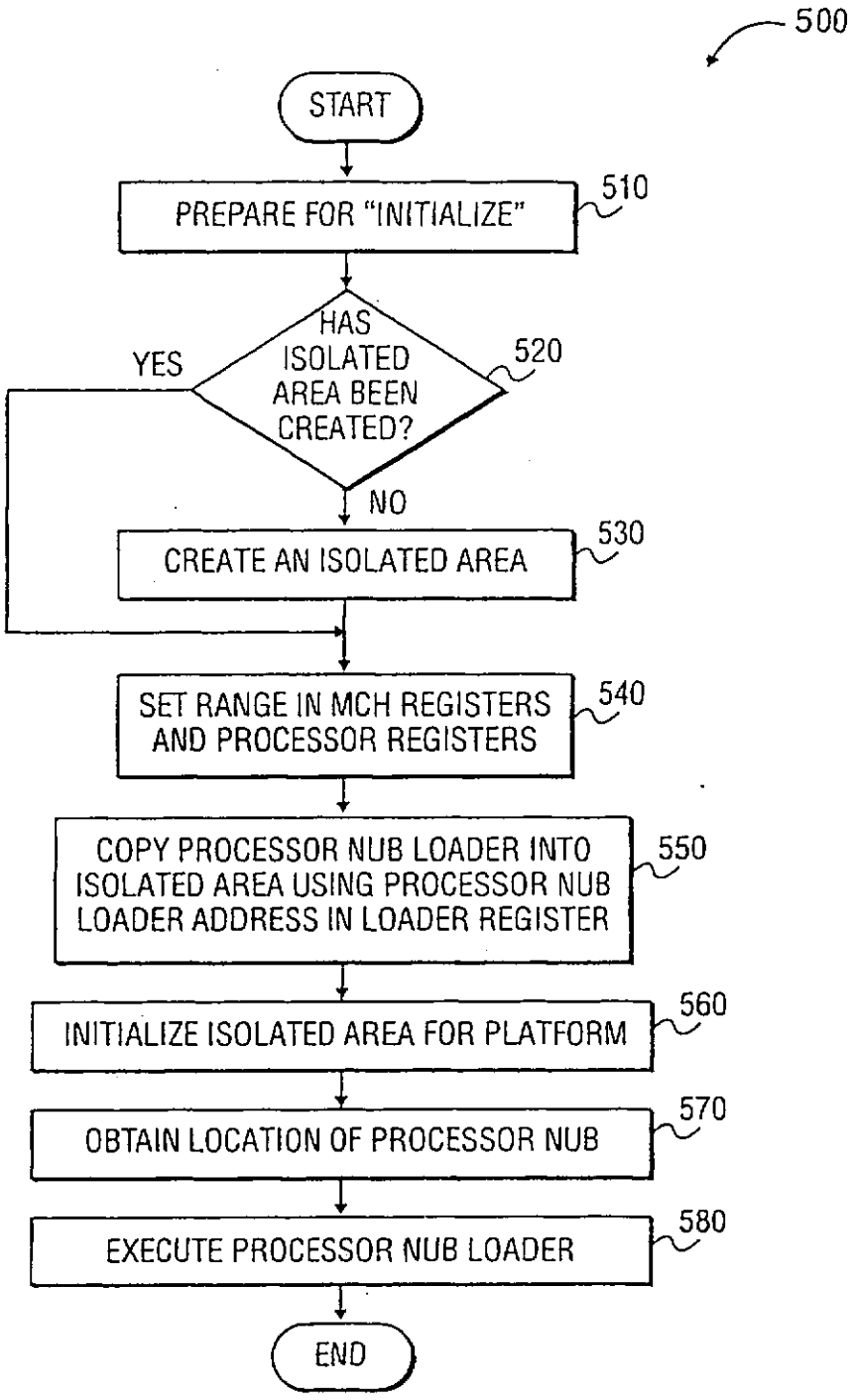

500
START
PREPARE FOR "INITIALIZE"
510
HAS ISOLATED AREA BEEN CREATED?
520
YES
NO
CREATE AN ISOLATED AREA
530
SET RANGE IN MCH REGISTERS AND PROCESSOR REGISTERS
540
COPY PROCESSOR NUB LOADER INTO ISOLATED AREA USING PROCESSOR NUB LOADER ADDRESS IN LOADER REGISTER
550
INITIALIZE ISOLATED AREA FOR PLATFORM
560
OBTAIN LOCATION OF PROCESSOR NUB
570
EXECUTE PROCESSOR NUB LOADER
580
END

FIG. 5

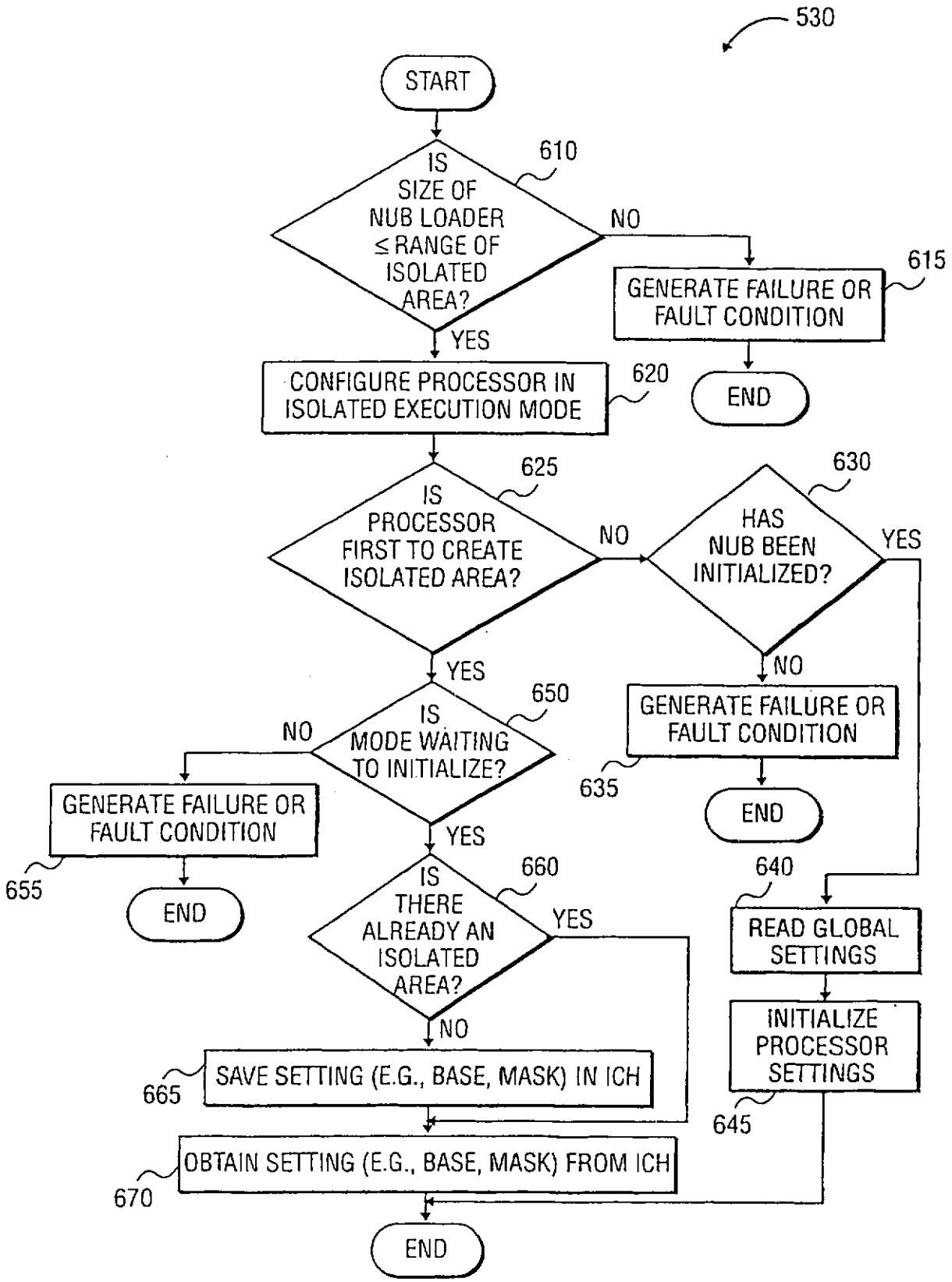

530
START
610
IS SIZE OF NUB LOADER ≤ RANGE OF ISOLATED AREA?
NO
615
GENERATE FAILURE OR FAULT CONDITION
END
YES
CONFIGURE PROCESSOR IN ISOLATED EXECUTION MODE
620
625
IS PROCESSOR FIRST TO CREATE ISOLATED AREA?
NO
630
HAS NUB BEEN INITIALIZED?
YES
YES
NO
650
IS MODE WAITING TO INITIALIZE?
NO
GENERATE FAILURE OR FAULT CONDITION
635
END
655
GENERATE FAILURE OR FAULT CONDITION
END
YES
660
IS THERE ALREADY AN ISOLATED AREA?
YES
640
READ GLOBAL SETTINGS
INITIALIZE PROCESSOR SETTINGS
645
NO
665
SAVE SETTING (E.G., BASE, MASK) IN ICH
OBTAIN SETTING (E.G., BASE, MASK) FROM ICH
670
END

FIG. 6A

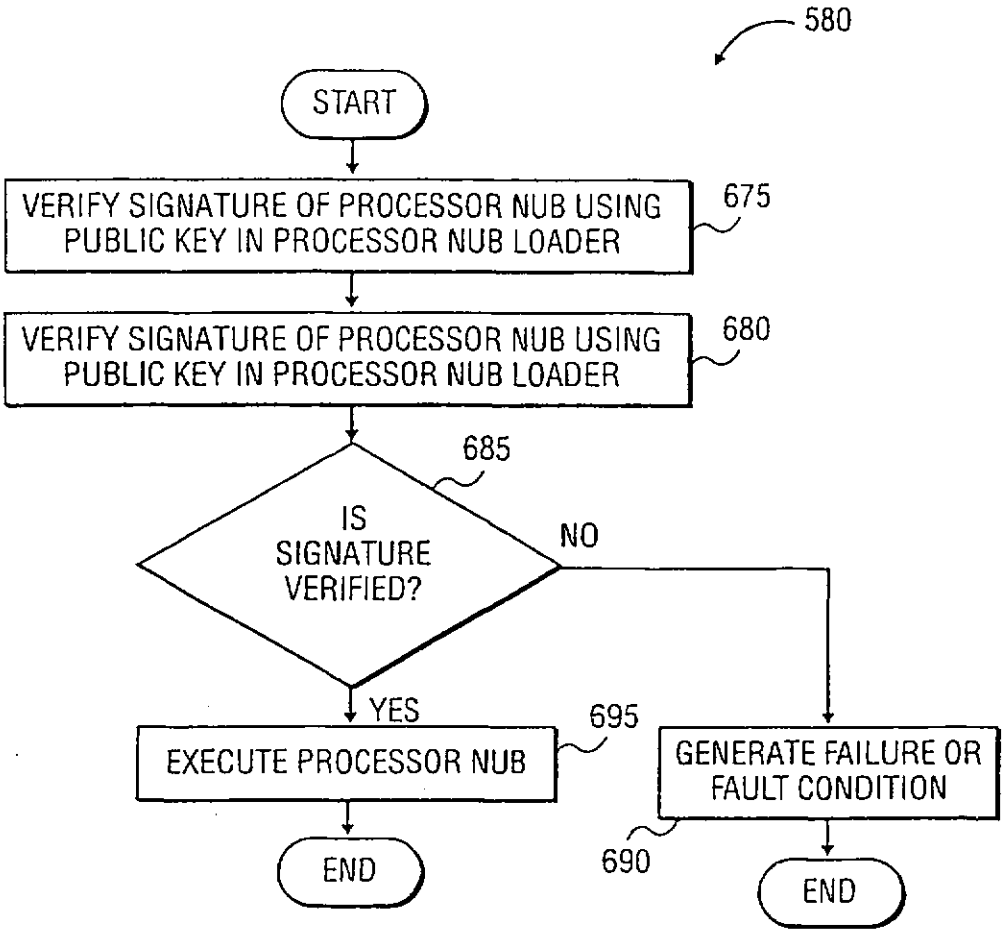

580
START
VERIFY SIGNATURE OF PROCESSOR NUB USING PUBLIC KEY IN PROCESSOR NUB LOADER
675
VERIFY SIGNATURE OF PROCESSOR NUB USING PUBLIC KEY IN PROCESSOR NUB LOADER
680
685
IS SIGNATURE VERIFIED?
NO
YES
695
EXECUTE PROCESSOR NUB
GENERATE FAILURE OR FAULT CONDITION
690
END
END

FIG. 6B

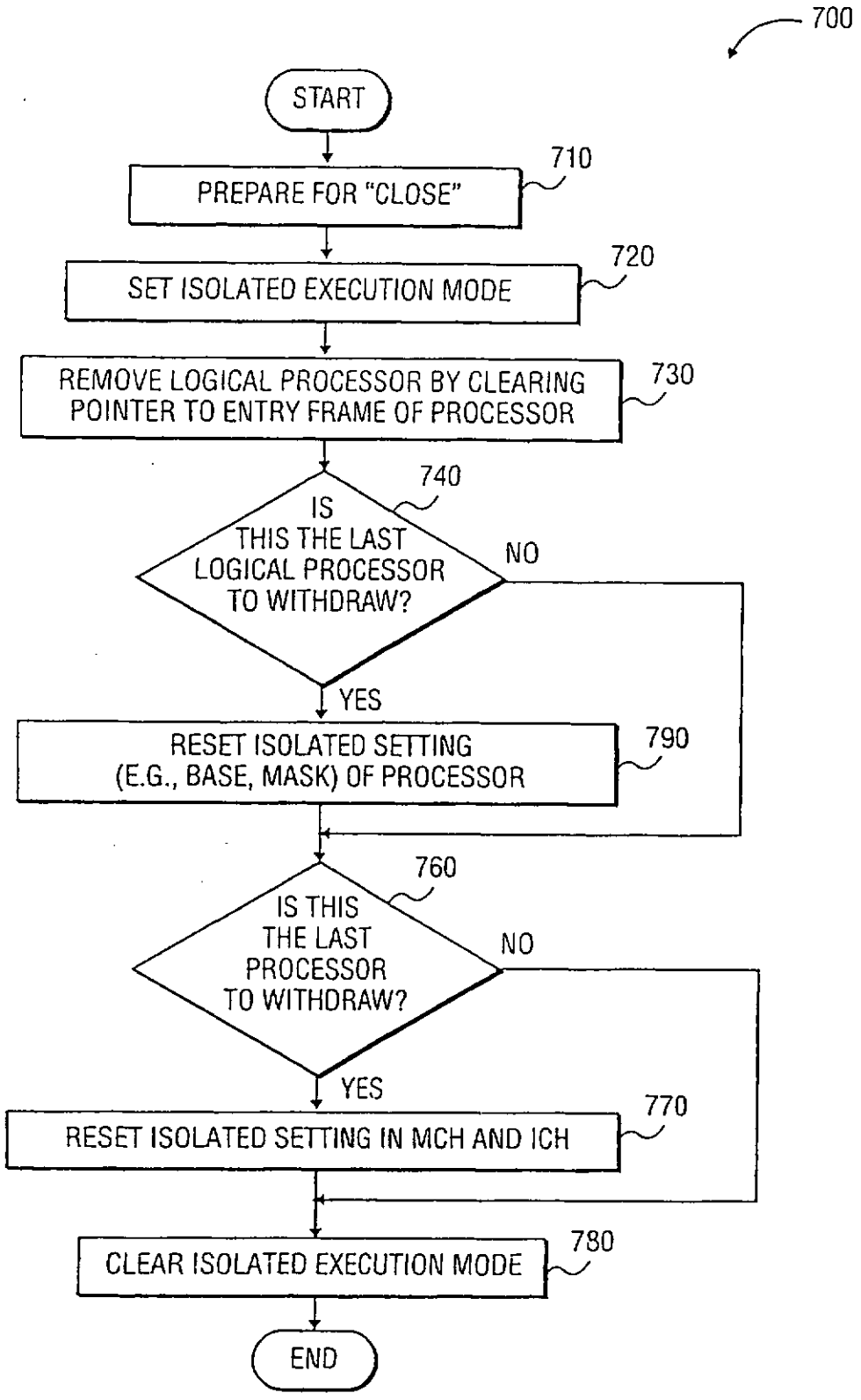

700
START
PREPARE FOR "CLOSE"
710
SET ISOLATED EXECUTION MODE
720
REMOVE LOGICAL PROCESSOR BY CLEARING POINTER TO ENTRY FRAME OF PROCESSOR
730
740
IS THIS THE LAST LOGICAL PROCESSOR TO WITHDRAW?
NO
YES
RESET ISOLATED SETTING (E.G., BASE, MASK) OF PROCESSOR
790
760
IS THIS THE LAST PROCESSOR TO WITHDRAW?
NO
YES
RESET ISOLATED SETTING IN MCH AND ICH
770
CLEAR ISOLATED EXECUTION MODE
780
END

FIG. 7

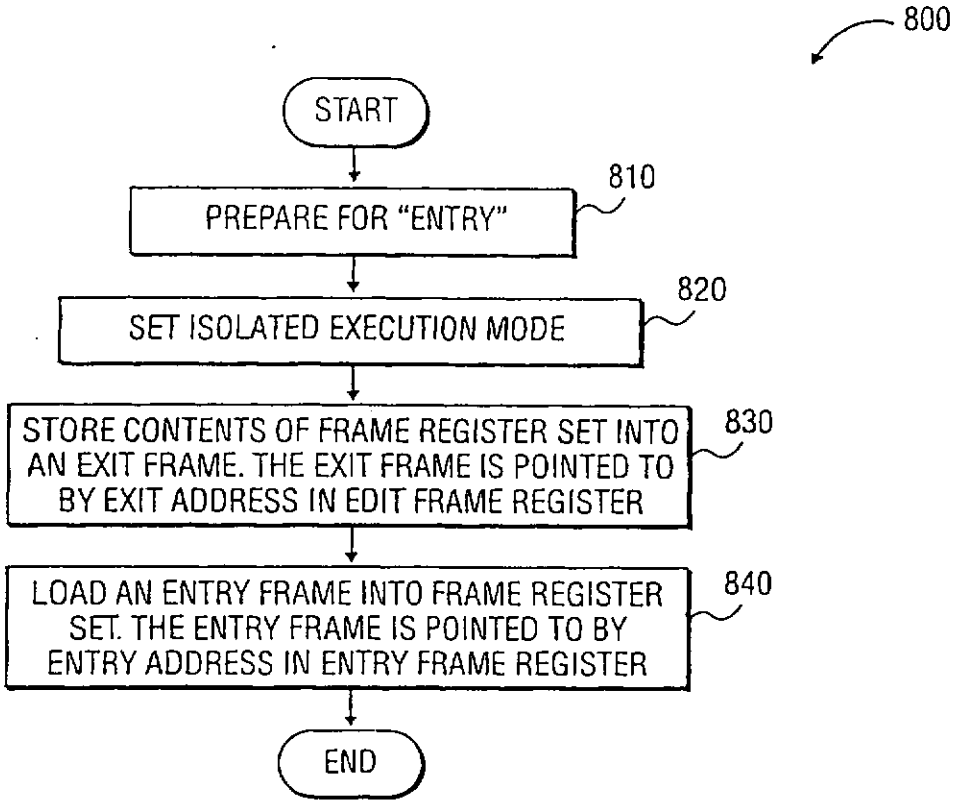

800
START
PREPARE FOR "ENTRY"
810
SET ISOLATED EXECUTION MODE
820
STORE CONTENTS OF FRAME REGISTER SET INTO AN EXIT FRAME. THE EXIT FRAME IS POINTED TO BY EXIT ADDRESS IN EDIT FRAME REGISTER
830
LOAD AN ENTRY FRAME INTO FRAME REGISTER SET. THE ENTRY FRAME IS POINTED TO BY ENTRY ADDRESS IN ENTRY FRAME REGISTER
840
END

FIG. 8A

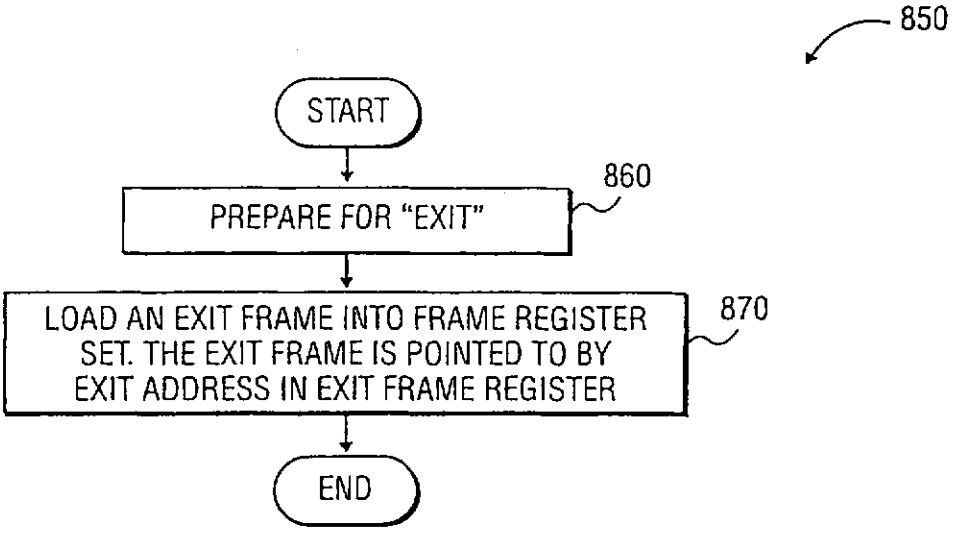

850
START
PREPARE FOR "EXIT"
860
LOAD AN EXIT FRAME INTO FRAME REGISTER SET. THE EXIT FRAME IS POINTED TO BY EXIT ADDRESS IN EXIT FRAME REGISTER
870
END

FIG. 8B

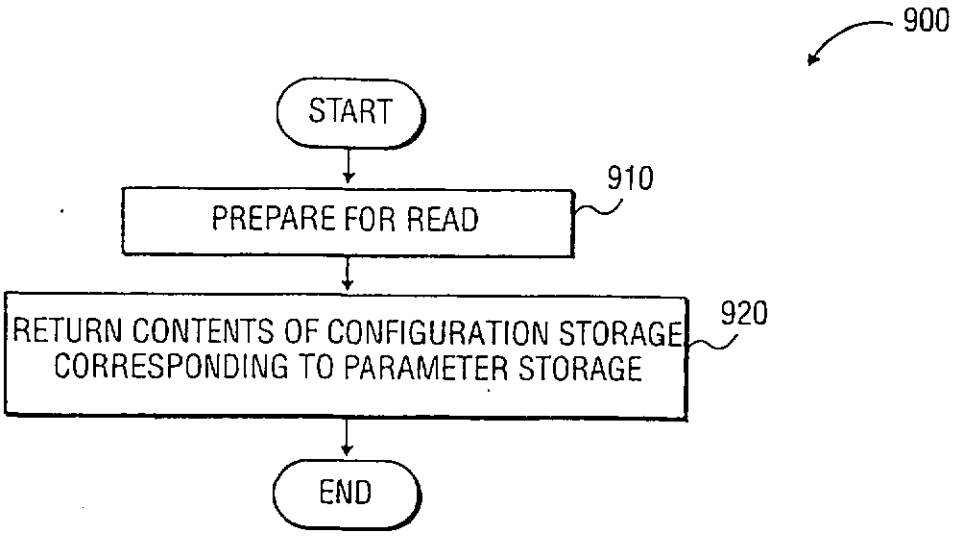

900
START
910
PREPARE FOR READ
920
RETURN CONTENTS OF CONFIGURATION STORAGE CORRESPONDING TO PARAMETER STORAGE
END

FIG. 9A

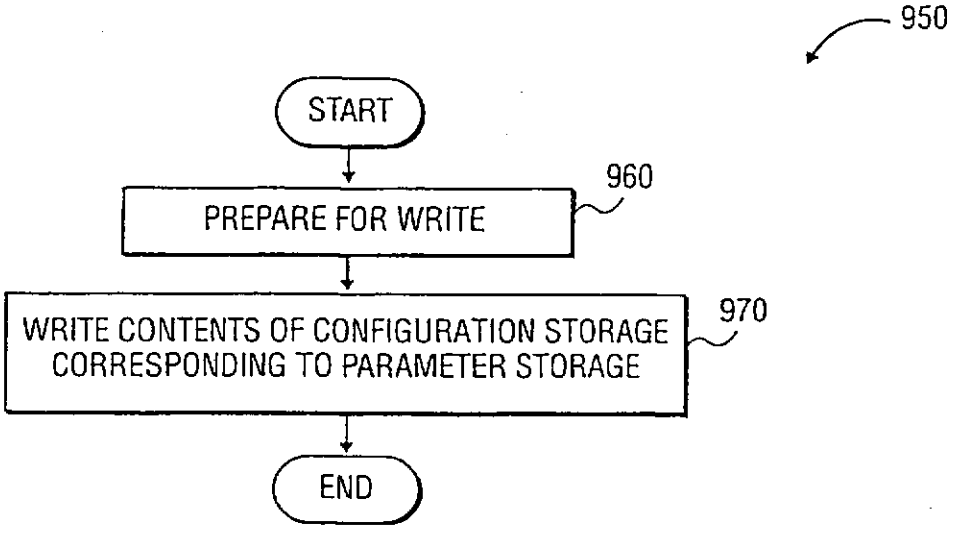

950
START
960
PREPARE FOR WRITE
970
WRITE CONTENTS OF CONFIGURATION STORAGE CORRESPONDING TO PARAMETER STORAGE
END

FIG. 9B