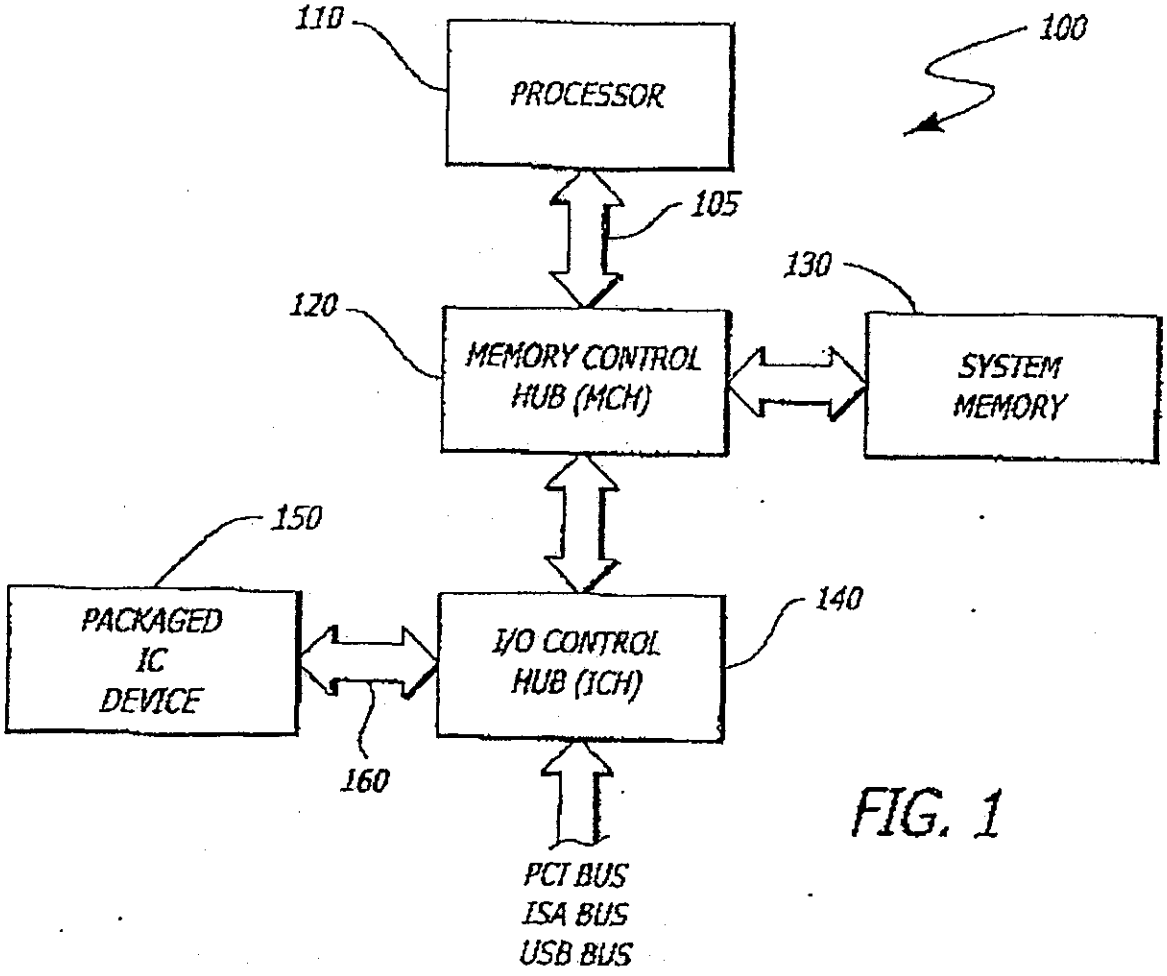

110
PROCESSOR
100
105
130
120
MEMORY CONTROL HUB (MCH)
SYSTEM MEMORY
150
PACKAGED IC DEVICE
140
I/O CONTROL HUB (ICH)
160
PCI BUS
ISA BUS
USB BUS

FIG. 1

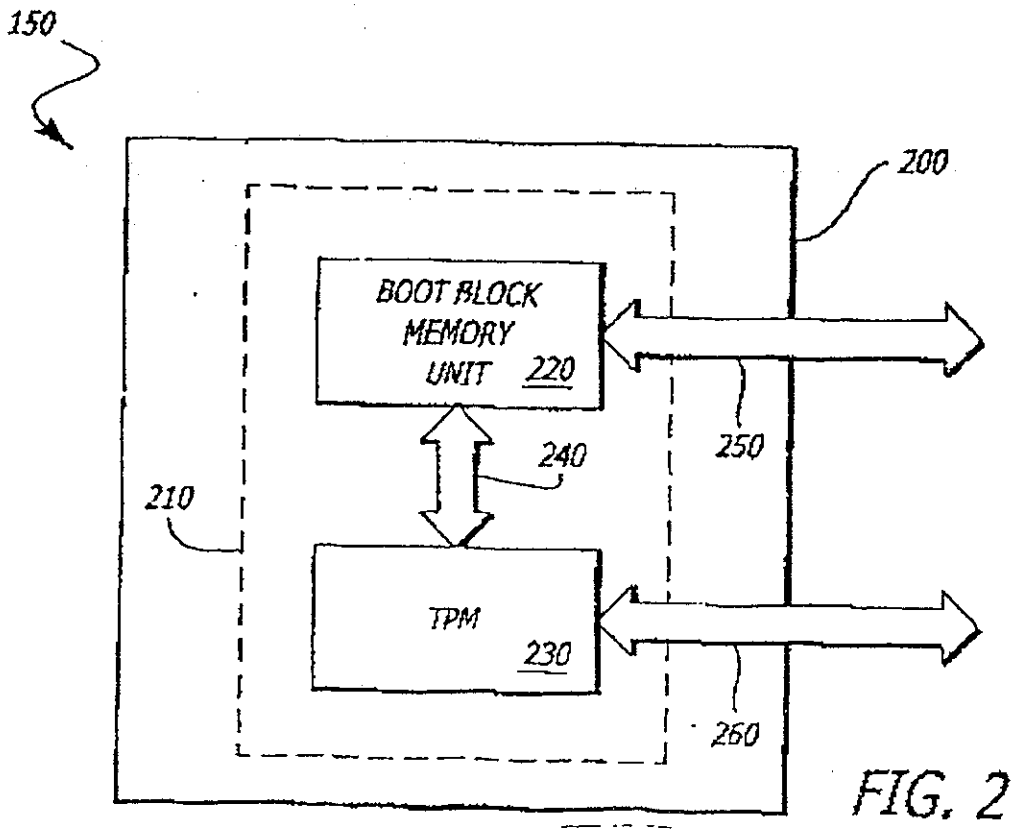

150
200
BOOT BLOCK MEMORY UNIT 220
240
250
210
TPM 230
260

FIG. 2

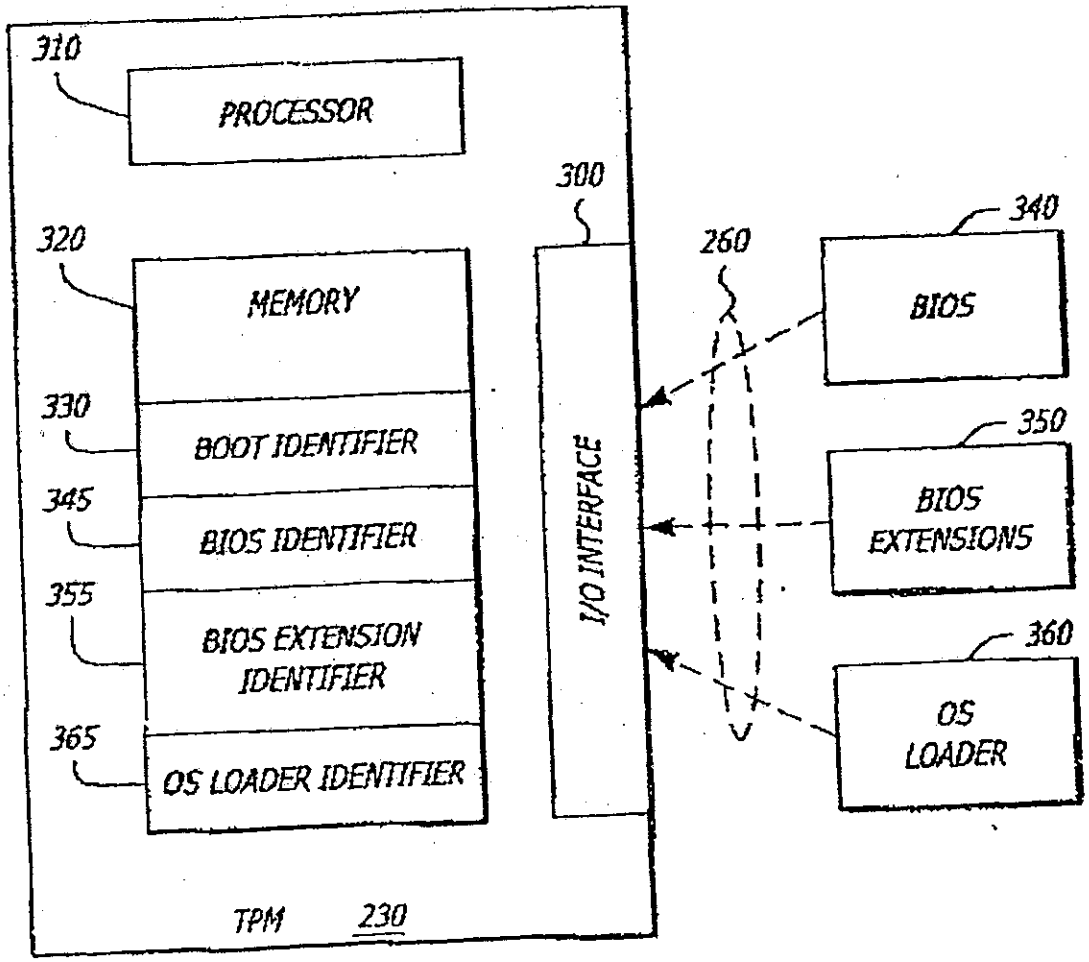

310
PROCESSOR
300
320
MEMORY
260
340
BIOS
330
BOOT IDENTIFIER
350
345
BIOS IDENTIFIER
BIOS EXTENSIONS
355
BIOS EXTENSION IDENTIFIER
360
365
OS LOADER IDENTIFIER
OS LOADER
I/O INTERFACE
TPM 230

FIG. 3

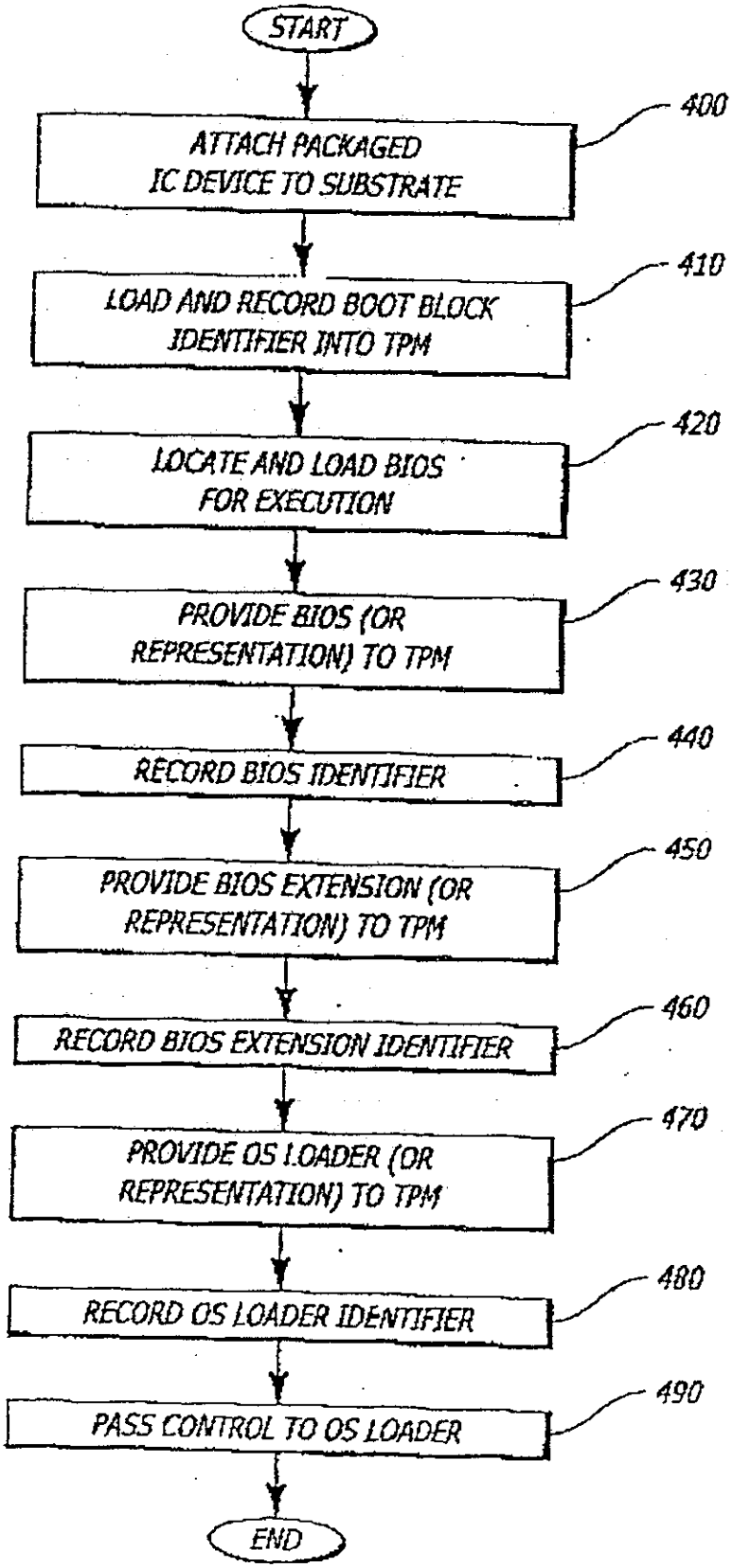

START
ATTACH PACKAGED IC DEVICE TO SUBSTRATE
400
LOAD AND RECORD BOOT BLOCK IDENTIFIER INTO TPM
410
LOCATE AND LOAD BIOS FOR EXECUTION
420
PROVIDE BIOS (OR REPRESENTATION) TO TPM
430
RECORD BIOS IDENTIFIER
440
PROVIDE BIOS EXTENSION (OR REPRESENTATION) TO TPM
450
RECORD BIOS EXTENSION IDENTIFIER
460
PROVIDE OS LOADER (OR REPRESENTATION) TO TPM
470
RECORD OS LOADER IDENTIFIER
480
PASS CONTROL TO OS LOADER
490
END

FIG. 4