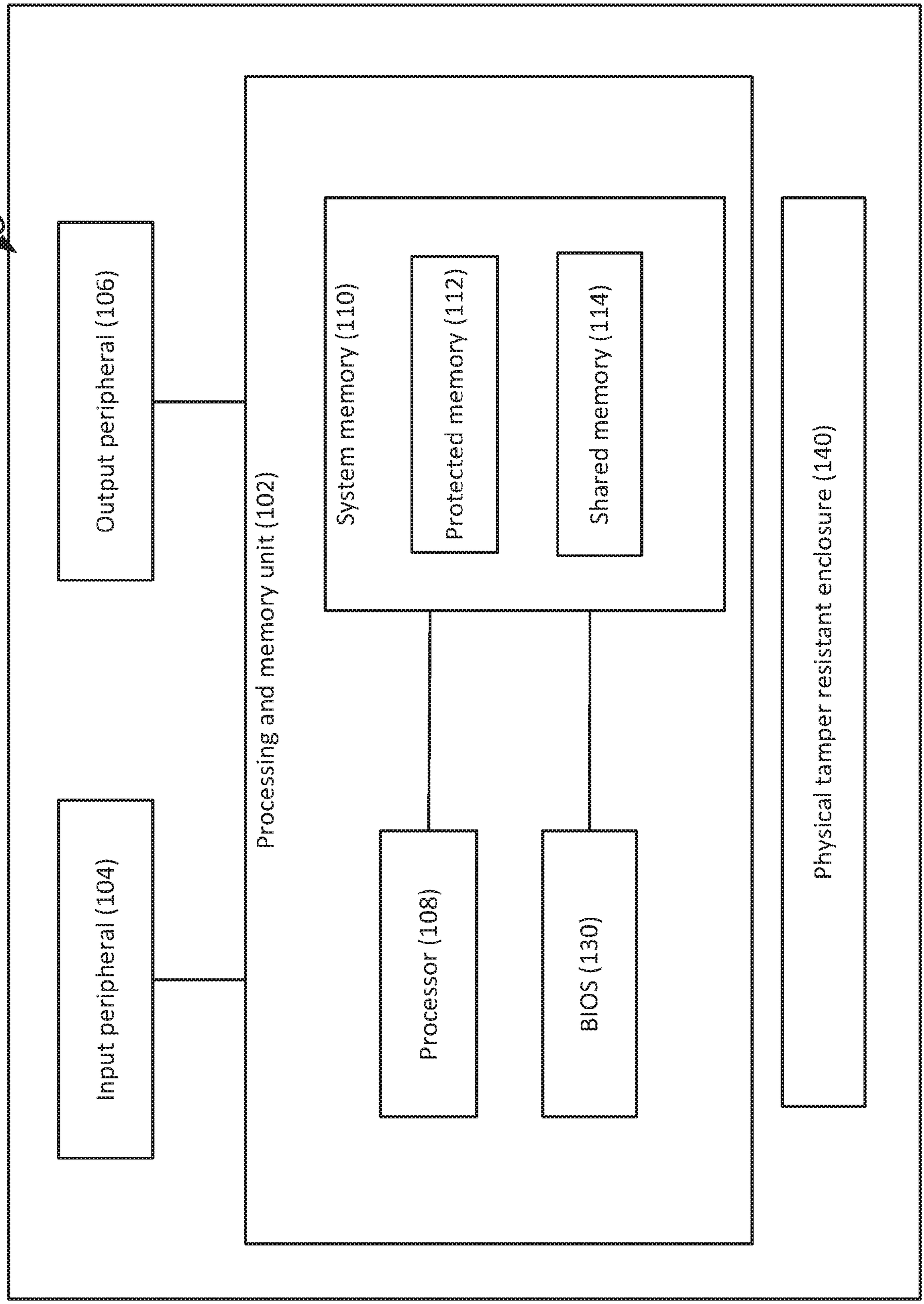

100
Output peripheral (106)
Processing and memory unit (102)
System memory (110)
Protected memory (112)
Shared memory (114)
Processor (108)
BIOS (130)
Input peripheral (104)
Physical tamper resistant enclosure (140)

FIG. 1a

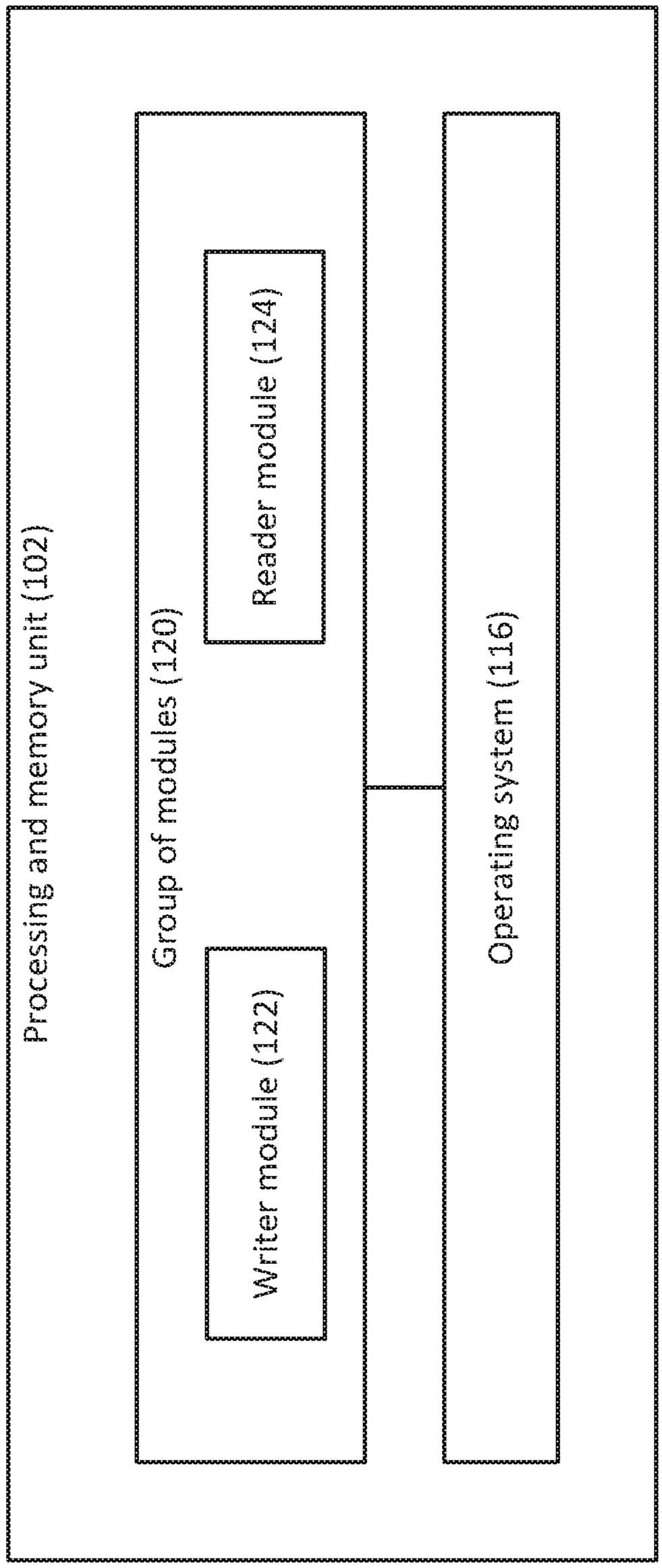

Processing and memory unit (102)
Group of memory modules (120)
Reader module (124)
Writer module (122)
Operating system (116)

FIG. 1b

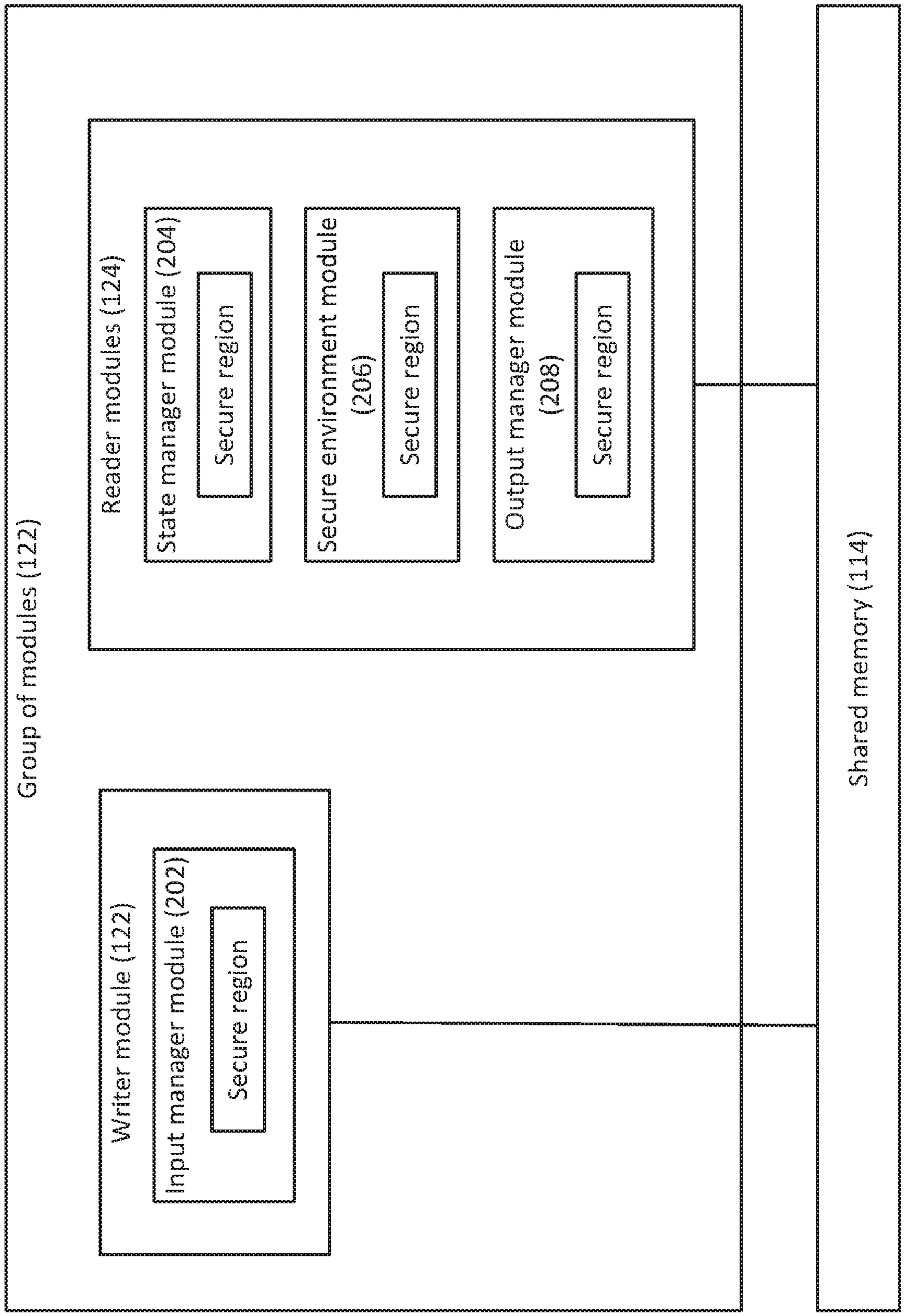
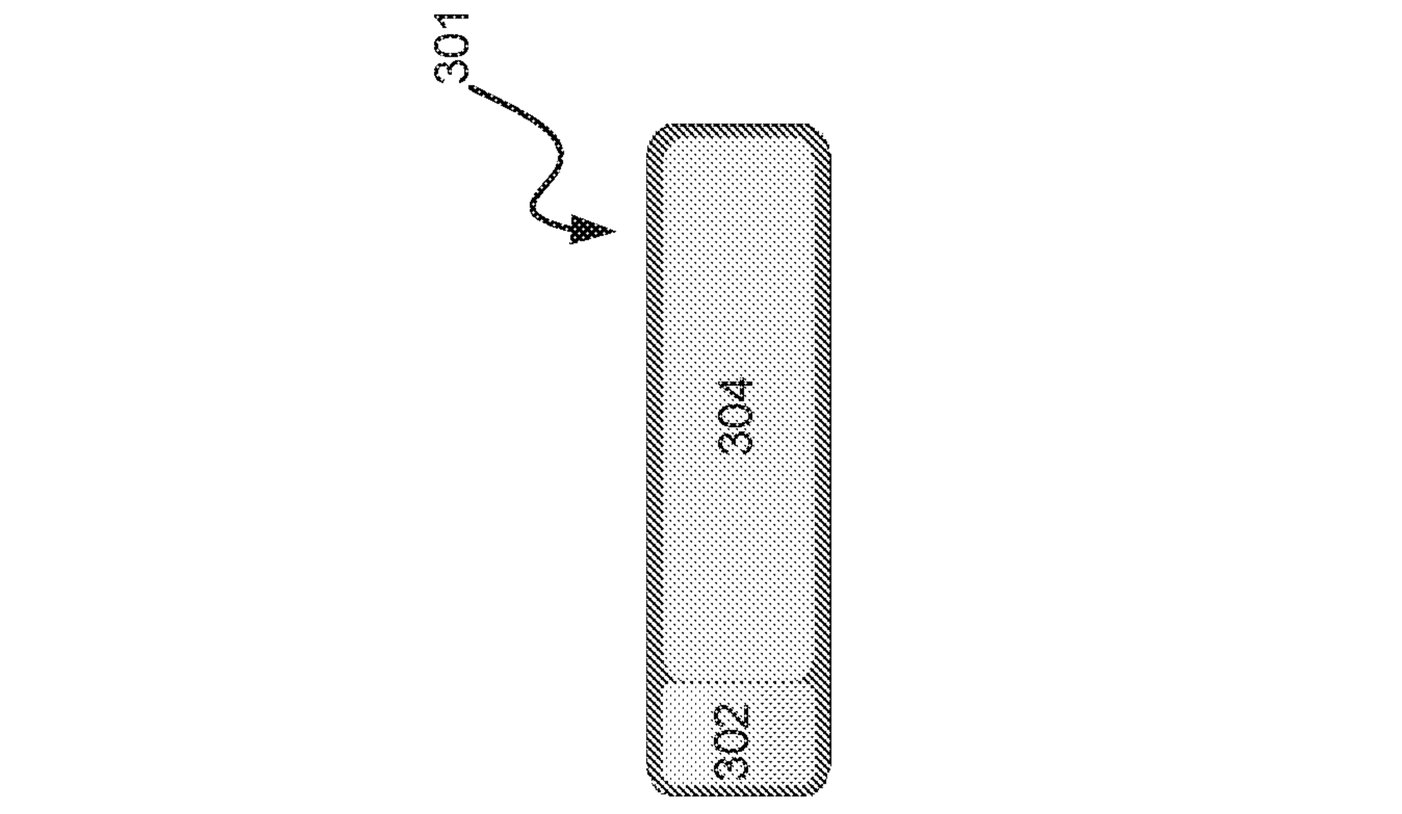

Group of modules (122)
Reader modules (124)
State manager module (204)
Secure region
Secure environment module (206)
Secure region
Output manager module (208)
Secure region
Writer module (122)
Input manager module (202)
Secure region
Shared memory (114)

FIG. 2



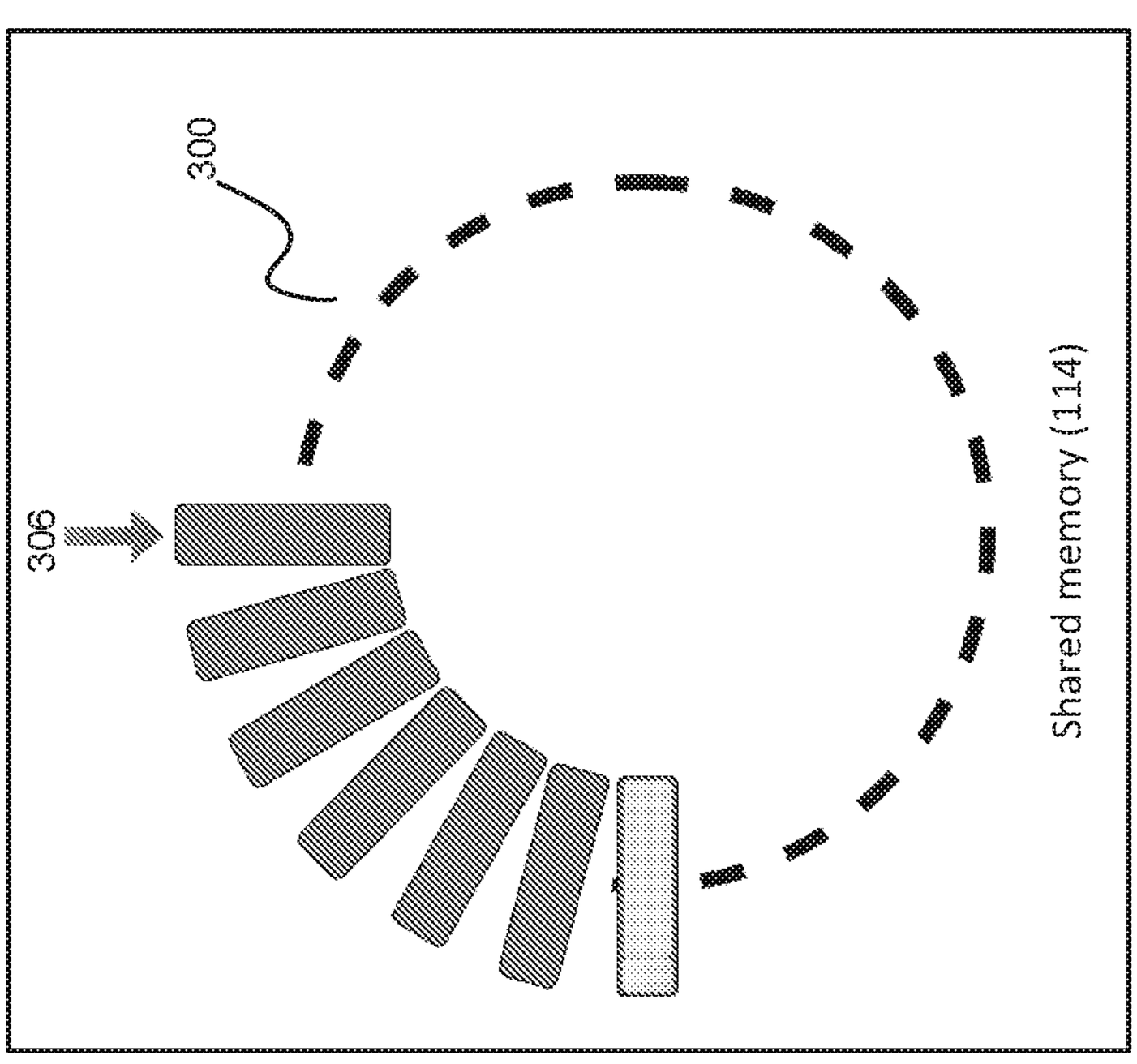


FIG. 3

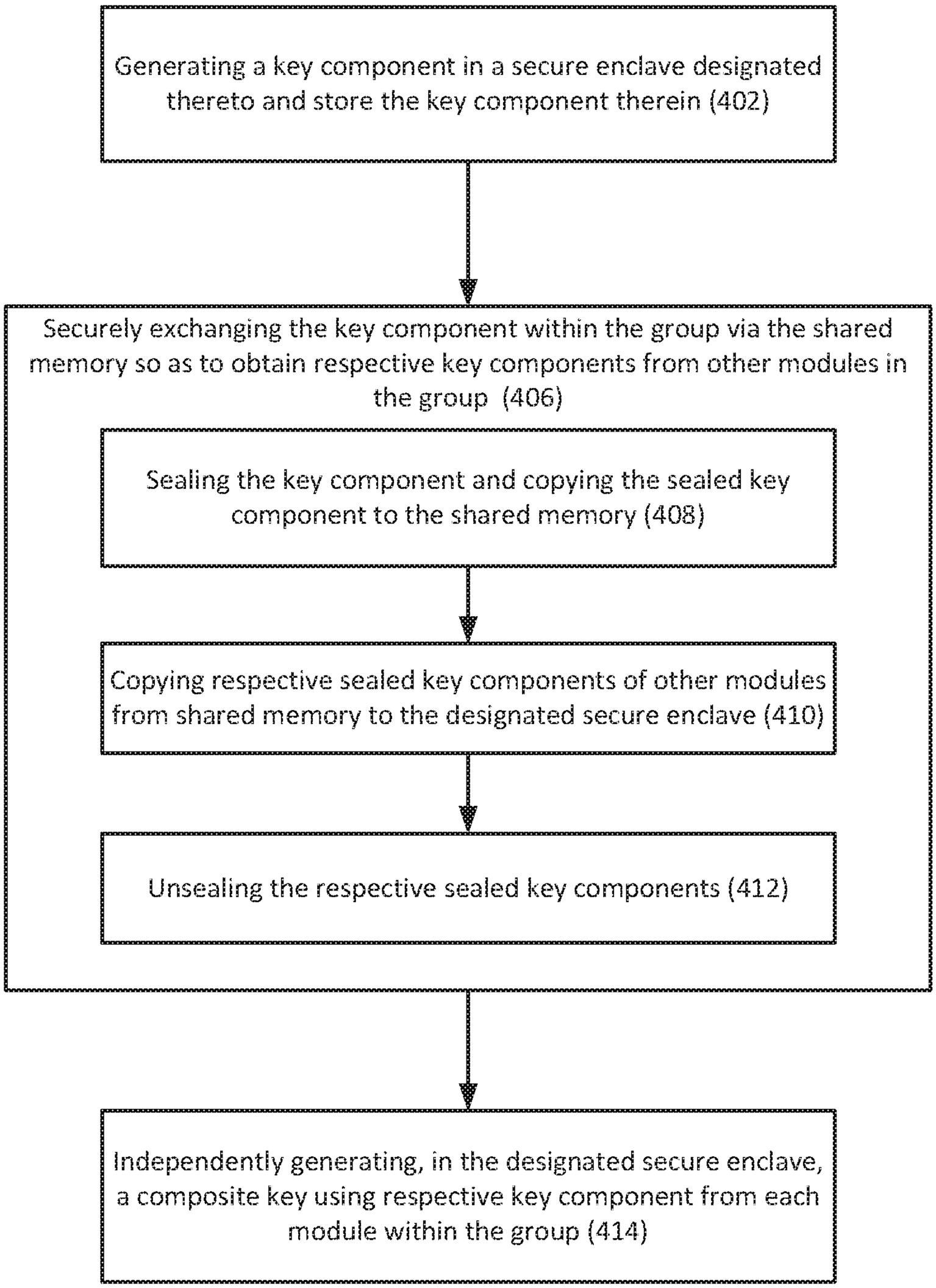

Generating a key component in a secure enclave designated thereto and store the key component therein (402)
Securely exchanging the key component within the group via the shared memory so as to obtain respective key components from other modules in the group (406)
Sealing the key component and copying the sealed key component to the shared memory (408)
Copying respective sealed key components of other modules from shared memory to the designated secure enclave (410)
Unsealing the respective sealed key components (412)
Independently generating, in the designated secure enclave, a composite key using respective key component from each module within the group (414)

FIG. 4

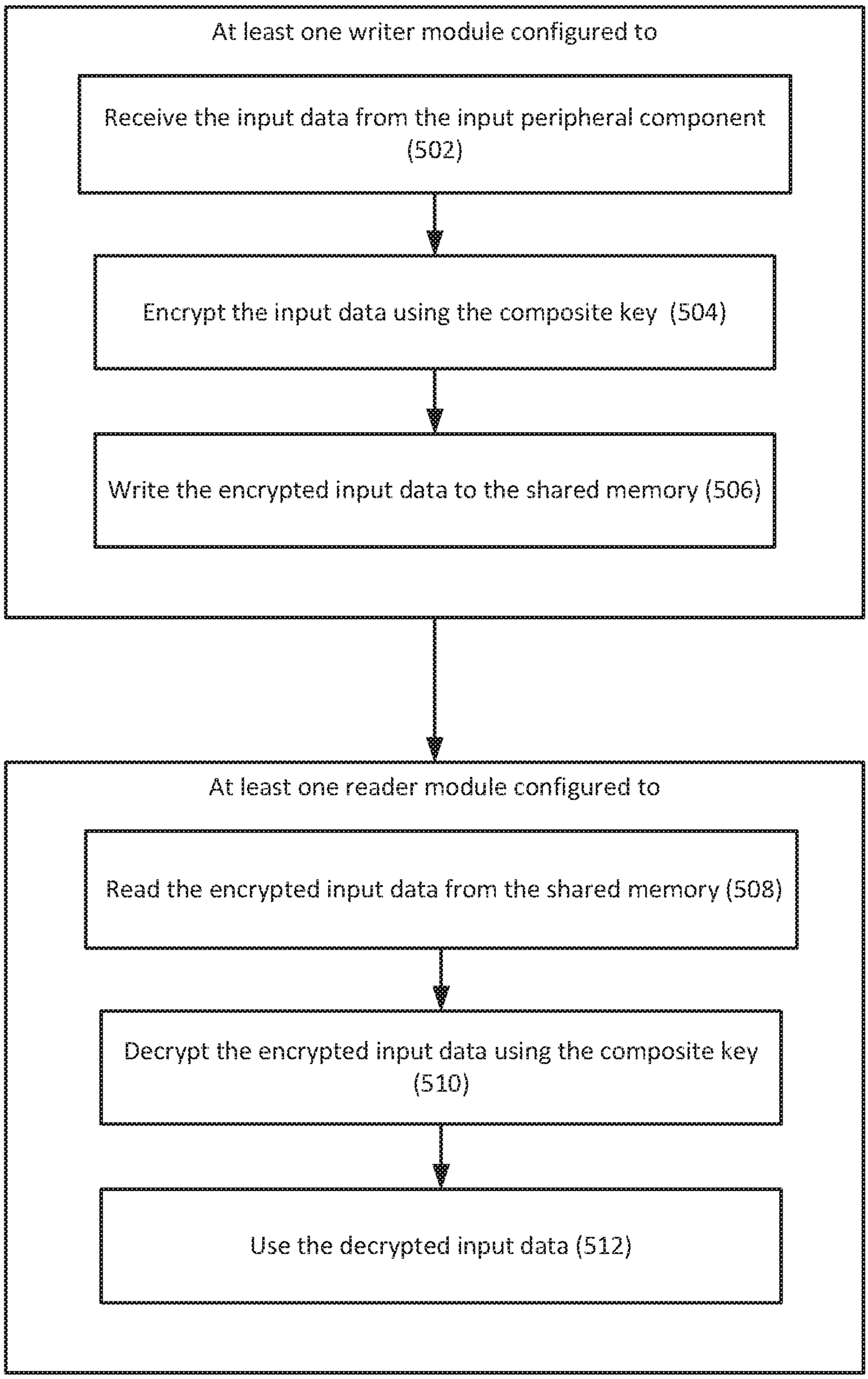

At least one writer module configured to
Receive the input data from the input peripheral component (502)
Encrypt the input data using the composite key (504)
Write the encrypted input data to the shared memory (506)
At least one reader module configured to
Read the encrypted input data from the shared memory (508)
Decrypt the encrypted input data using the composite key (510)
Use the decrypted input data (512)

FIG. 5

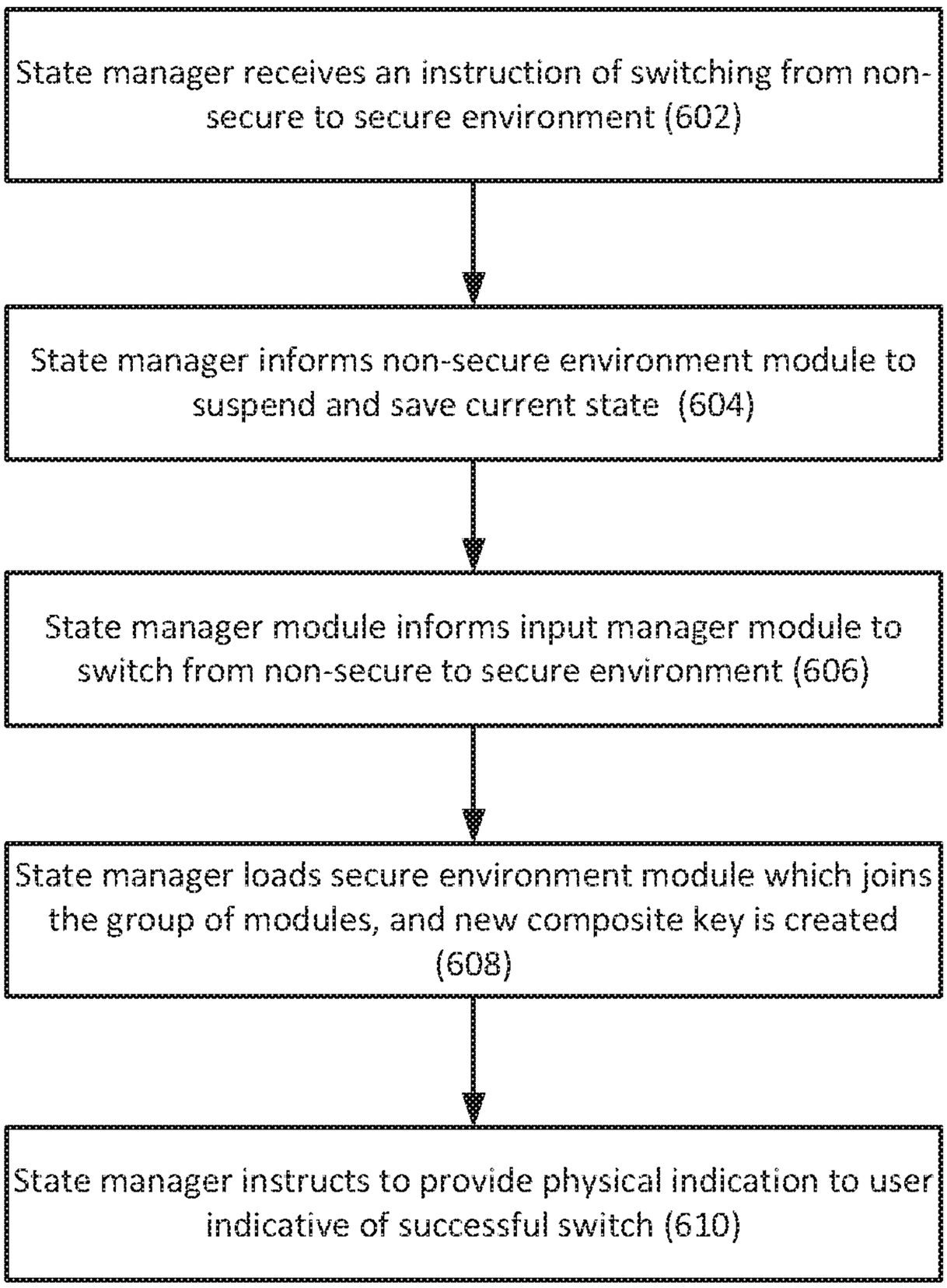

State manager receives an instruction of switching from non-secure to secure environment (602)
State manager informs non-secure environment module to suspend and save current state (604)
State manager module informs input manager module to switch from non-secure to secure environment (606)
State manager loads secure environment module which joins the group of modules, and new composite key is created (608)
State manager instructs to provide physical indication to user indicative of successful switch (610)

FIG. 6

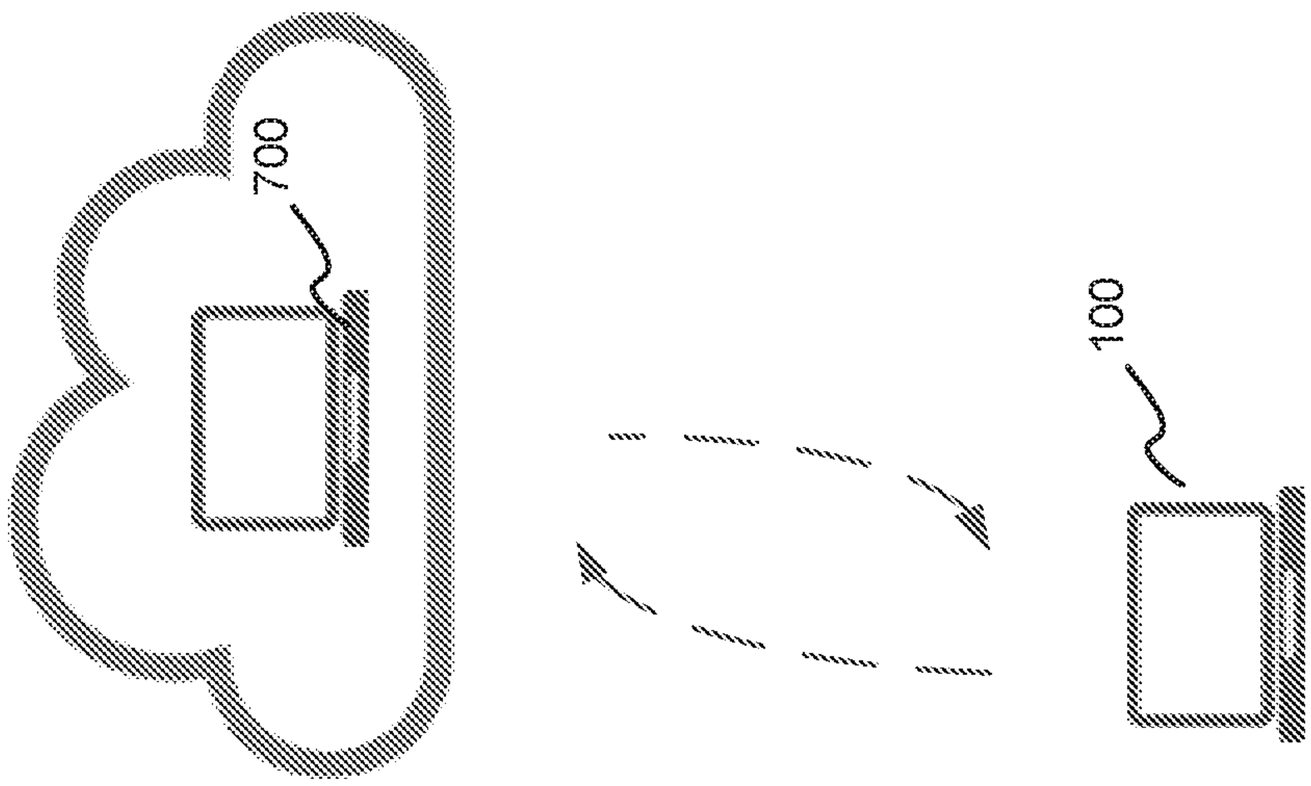


FIG. 7

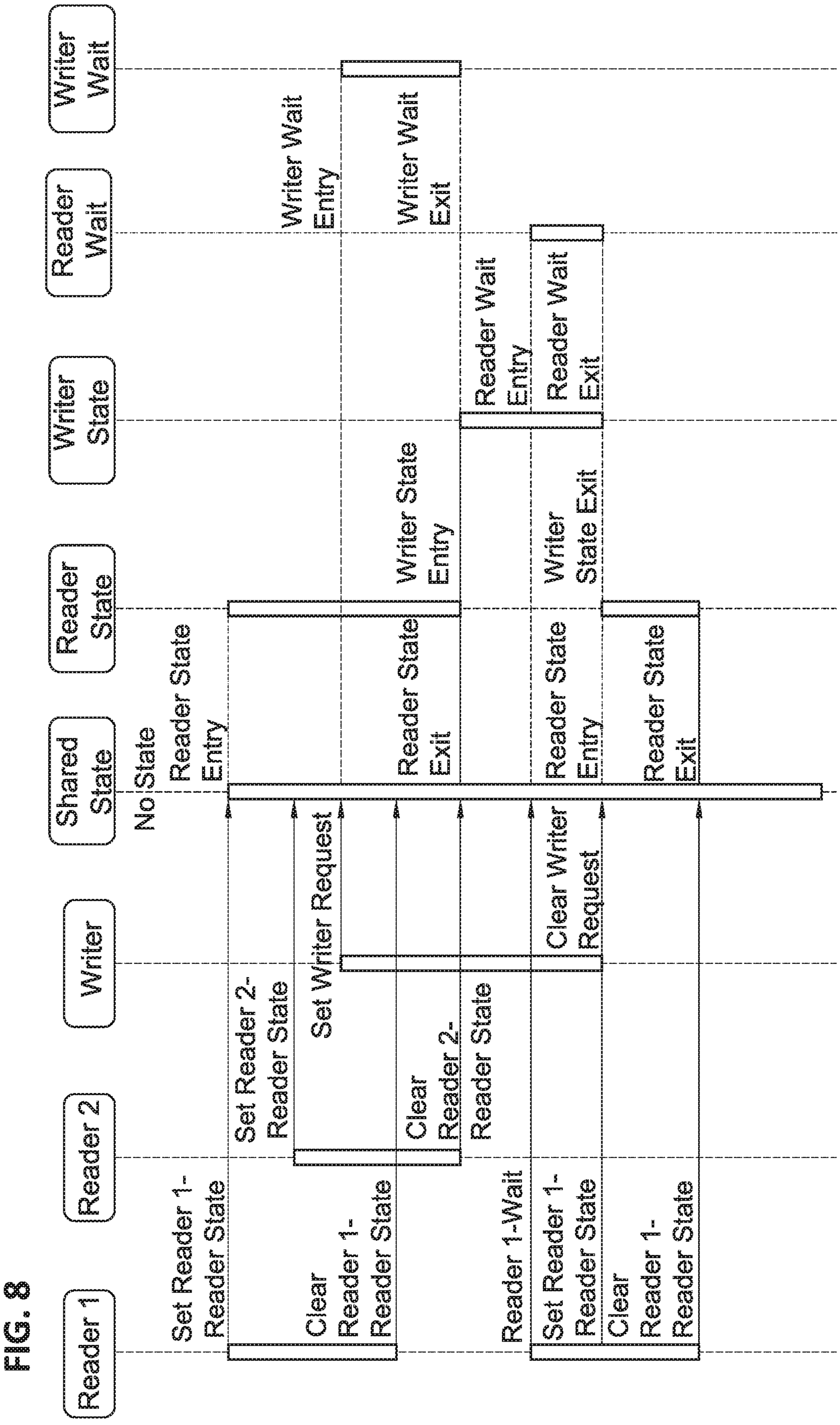

Reader 1
Reader 2
Writer
Shared State
Writer State
Reader Wait
Writer State
Reader State
Set Reader 1-Reader State
Reader 2-Reader State
No State
Reader State Entry
Set Writer Request
Writer State Entry
Clear Reader 1-Reader State
Reader 2-Reader State
Writer State Exit
Clear Writer Request
Reader Wait Entry
Reader State Exit
Writer Wait Entry
Writer Wait Exit
Reader 1-Wait
Set Reader 1-Reader State
Clear Reader 1-Reader State
Clear Reader 2-Reader State
Reader 2-Reader State
Reader State Entry
Reader State Exit
Reader Wait
Reader Wait Entry
Reader Wait Exit
Writer Wait

FIG. 8