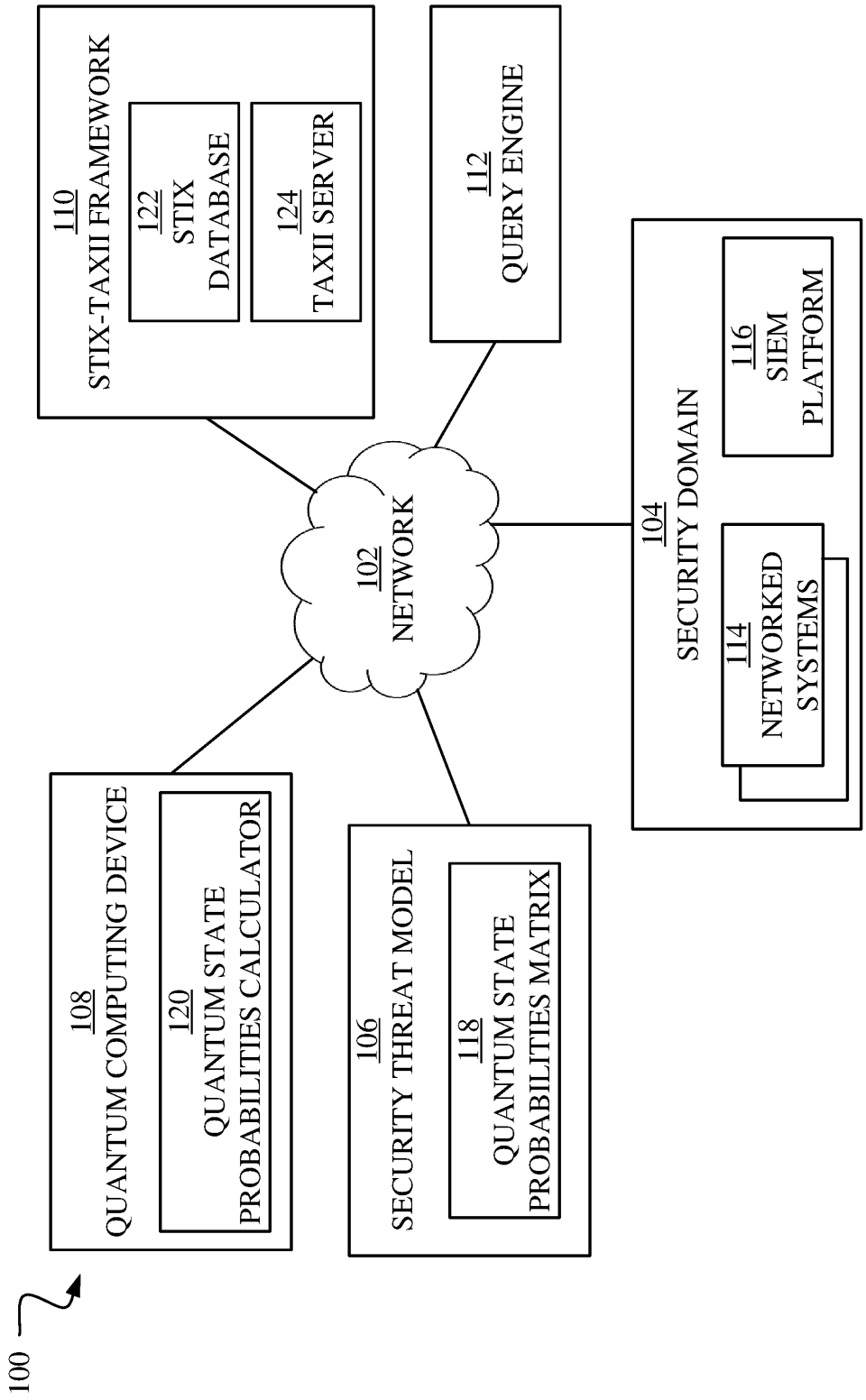

100
108
QUANTUM COMPUTING DEVICE
120
QUANTUM STATE
PROBABILITIES CALCULATOR
106
SECURITY THREAT MODEL
118
QUANTUM STATE
PROBABILITIES MATRIX
102
NETWORK
110
STIX-TAXII FRAMEWORK
122
STIX
DATABASE
124
TAXII SERVER
112
QUERY ENGINE
104
SECURITY DOMAIN
114
NETWORKED
SYSTEMS
116
SIEM
PLATFORM

FIG. 1

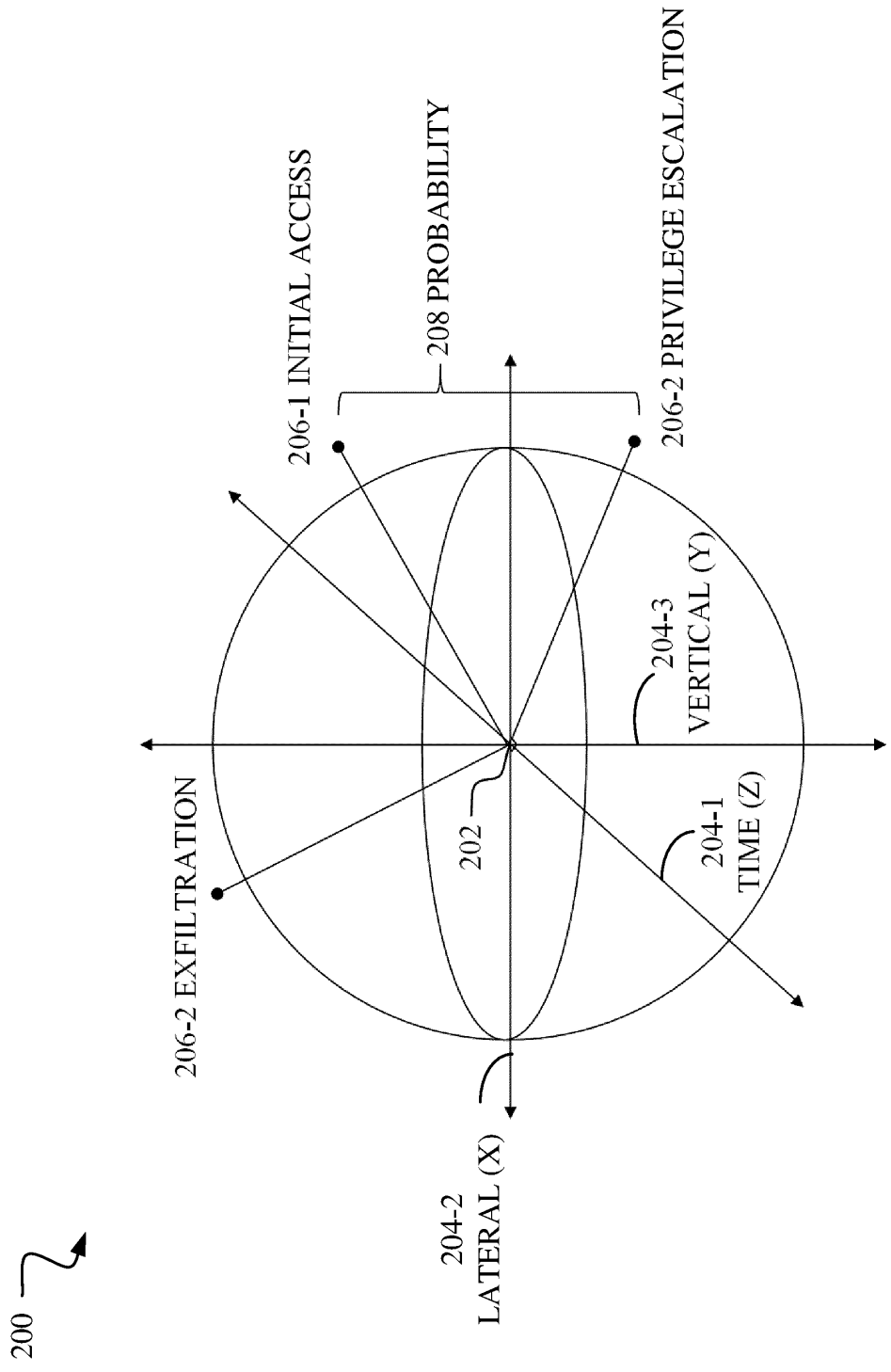

200
206-1 INITIAL ACCESS
208 PROBABILITY
206-2 PRIVILEGE ESCALATION
206-2 EXFILTRATION
202
204-3
VERTICAL (Y)
204-1
TIME (Z)
204-2
LATERAL (X)

FIG. 2

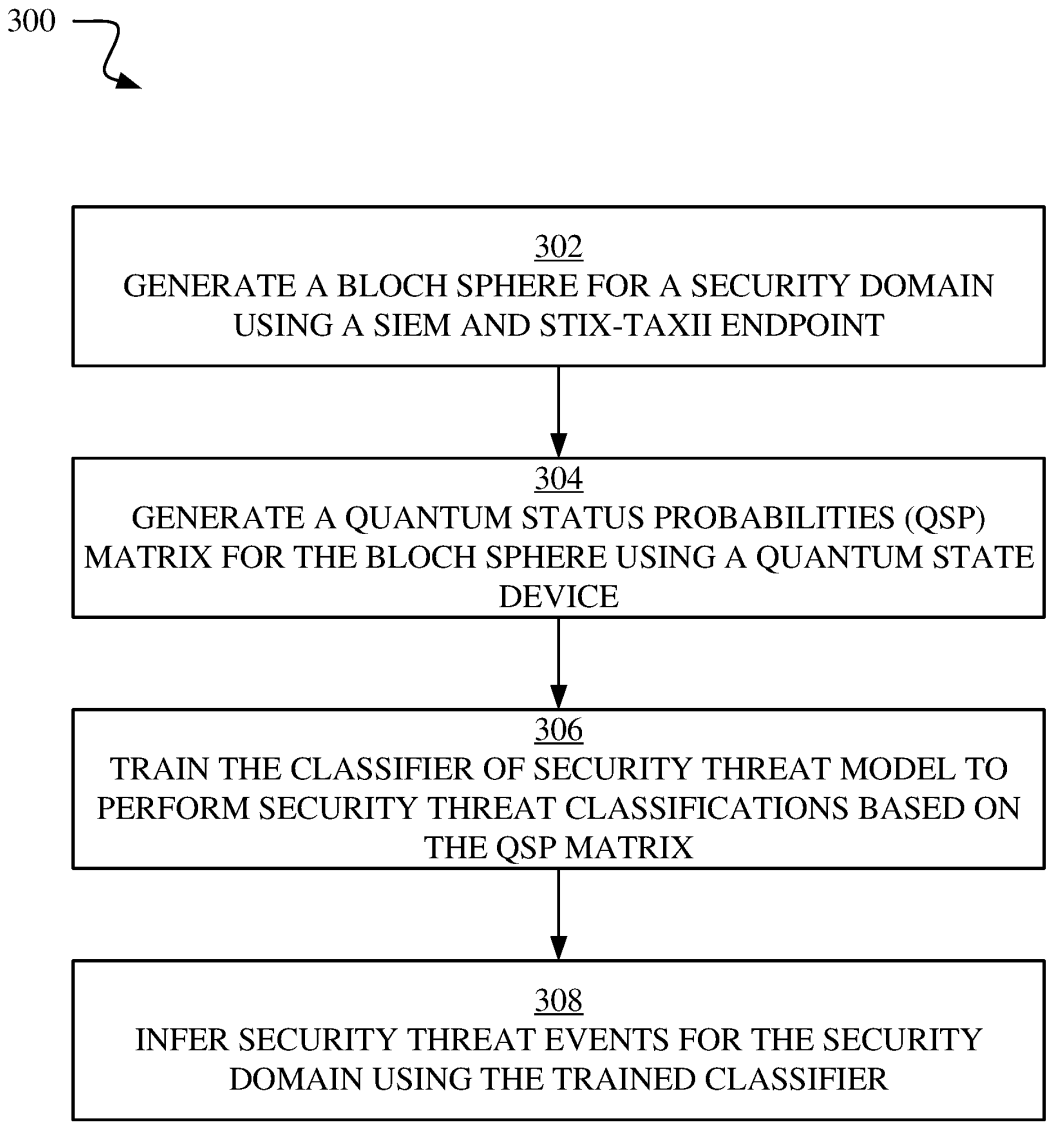

300
302
GENERATE A BLOCH SPHERE FOR A SECURITY DOMAIN USING A SIEM AND STIX-TAXII ENDPOINT
304
GENERATE A QUANTUM STATUS PROBABILITIES (QSP) MATRIX FOR THE BLOCH SPHERE USING A QUANTUM STATE DEVICE
306
TRAIN THE CLASSIFIER OF SECURITY THREAT MODEL TO PERFORM SECURITY THREAT CLASSIFICATIONS BASED ON THE QSP MATRIX
308
INFER SECURITY THREAT EVENTS FOR THE SECURITY DOMAIN USING THE TRAINED CLASSIFIER

**FIG. 3**

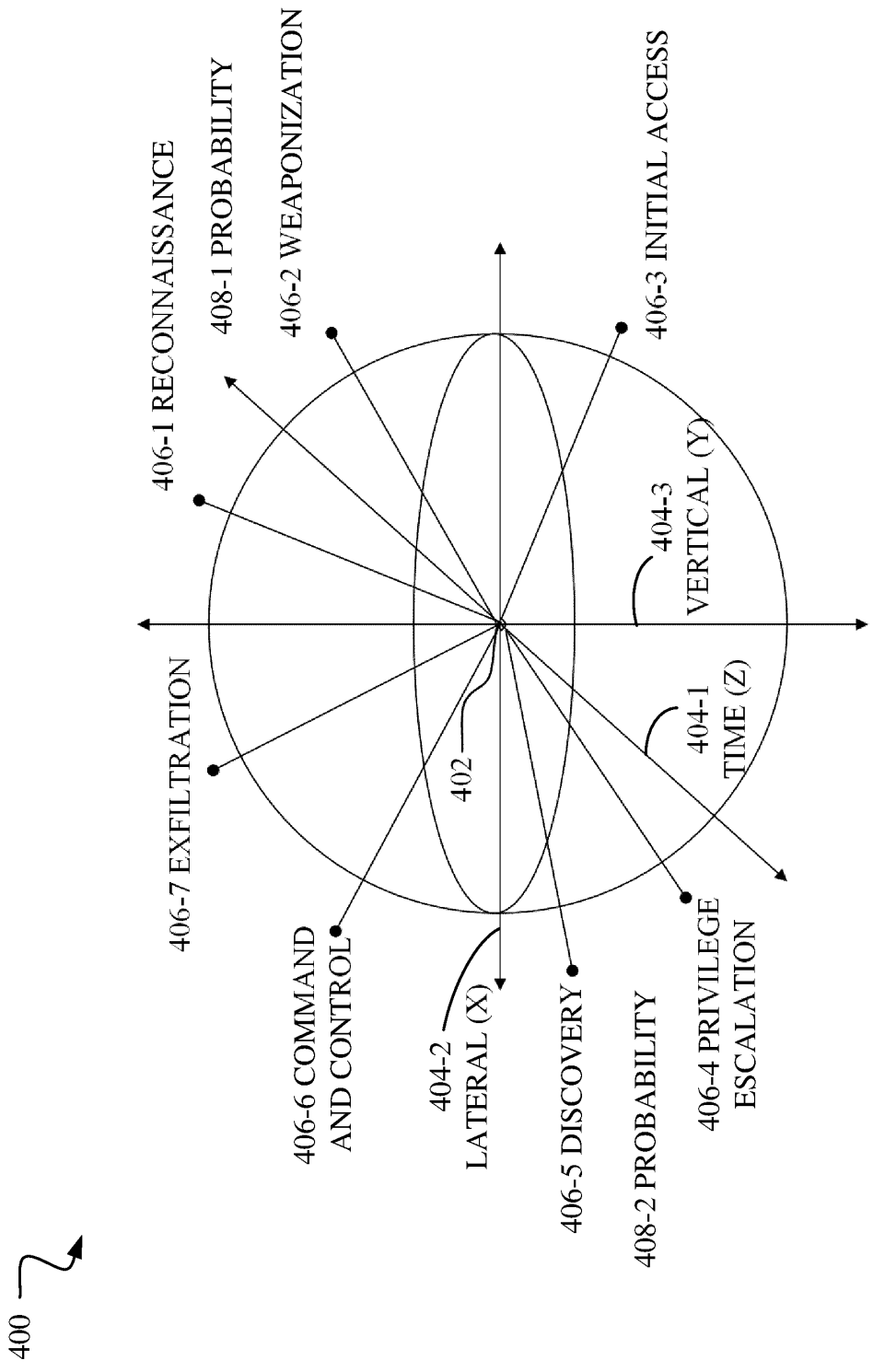

400
406-1 RECONNAISSANCE
408-1 PROBABILITY
406-2 WEAPONIZATION
406-3 INITIAL ACCESS
404-3
VERTICAL (Y)
404-1
TIME (Z)
402
406-7 EXFILTRATION
406-6 COMMAND
AND CONTROL
404-2
LATERAL (X)
406-5 DISCOVERY
408-2 PROBABILITY
406-4 PRIVILEGE
ESCALATION

FIG. 4

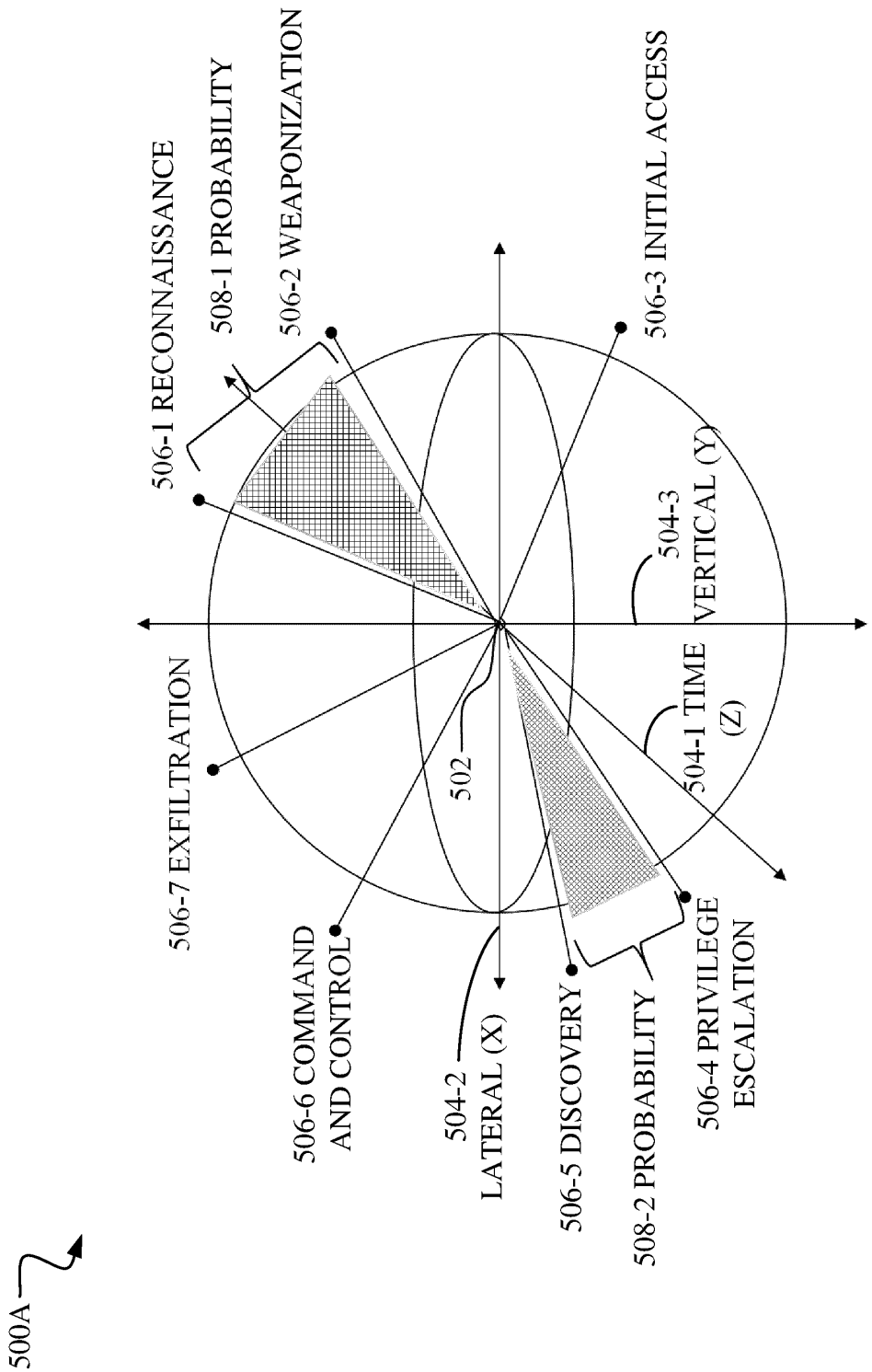

500A
506-1 RECONNAISSANCE
508-1 PROBABILITY
506-2 WEAPONIZATION
506-3 INITIAL ACCESS
504-3 VERTICAL (Y)
504-1 TIME (Z)
502
504-2 LATERAL (X)
506-7 EXFILTRATION
506-6 COMMAND AND CONTROL
506-5 DISCOVERY
508-2 PROBABILITY
506-4 PRIVILEGE ESCALATION

FIG. 5A

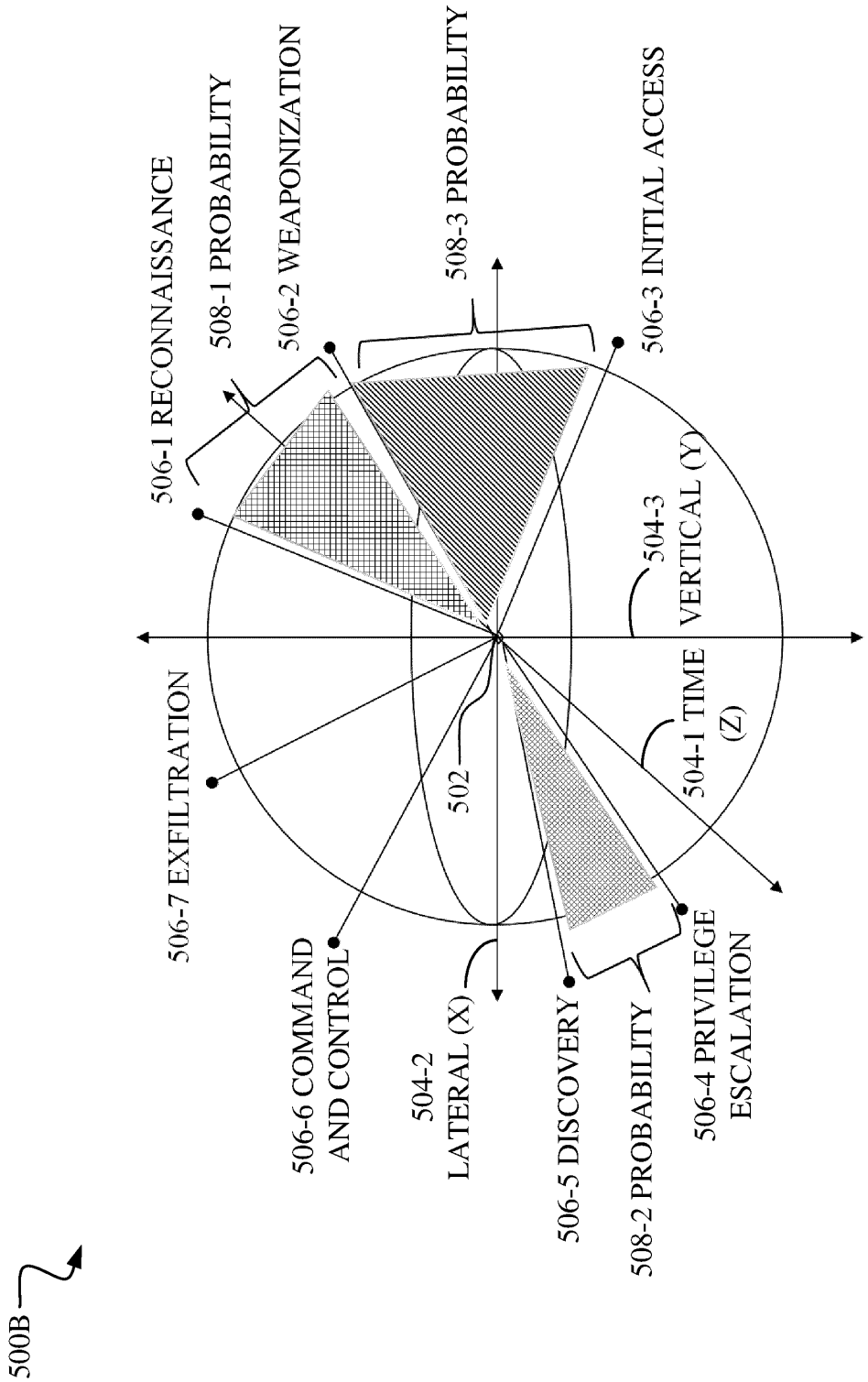

500B
506-1 RECONNAISSANCE
508-1 PROBABILITY
506-2 WEAPONIZATION
508-3 PROBABILITY
506-3 INITIAL ACCESS
504-3
VERTICAL (Y)
504-1 TIME
(Z)
502
504-2
LATERAL (X)
506-7 EXFILTRATION
506-6 COMMAND
AND CONTROL
506-5 DISCOVERY
508-2 PROBABILITY
506-4 PRIVILEGE
ESCALATION

FIG. 5B

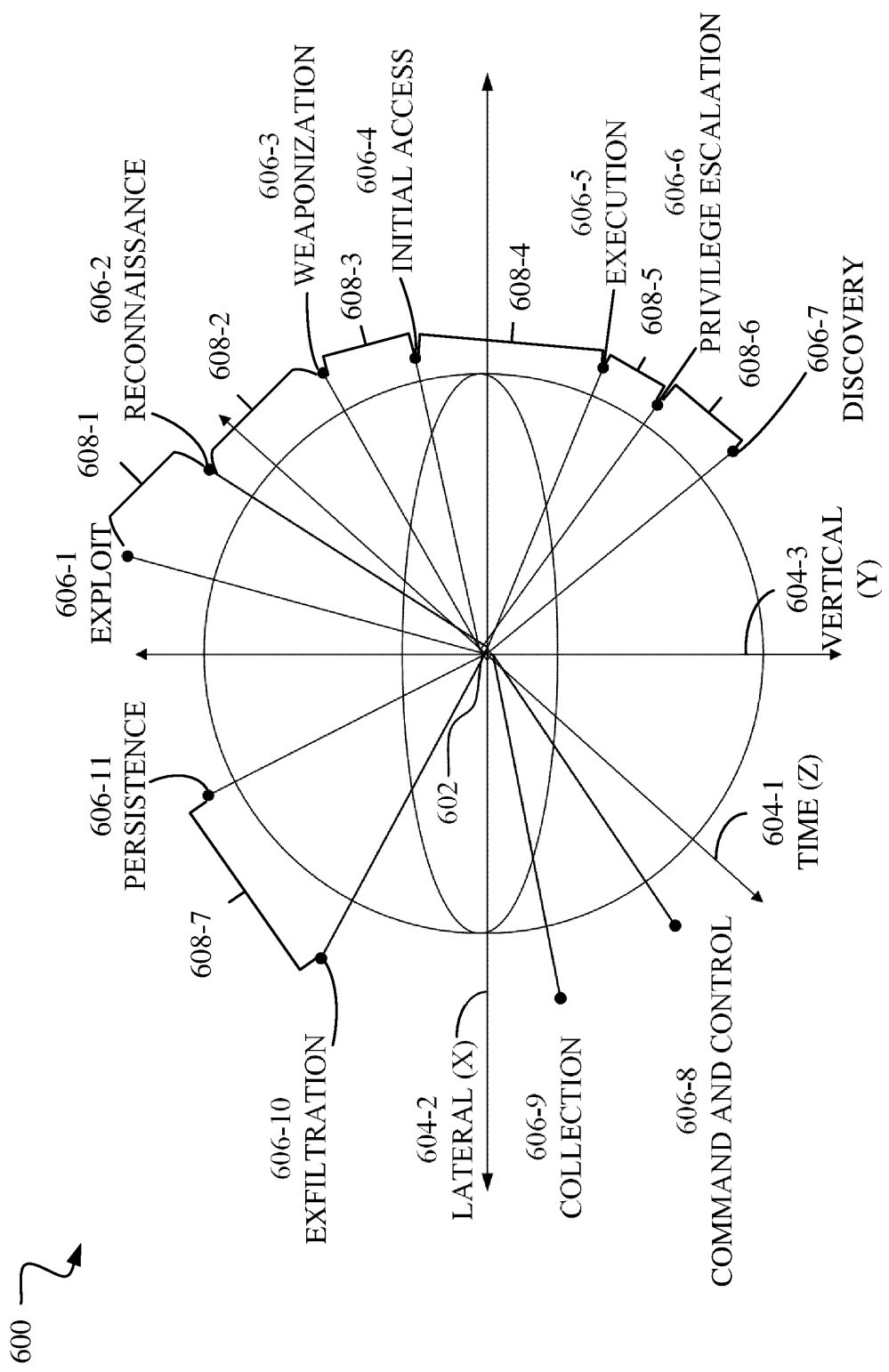

600
606-1
EXPLOIT
608-1
606-2
RECONNAISSANCE
608-2
606-3
WEAPONIZATION
608-3
606-4
INITIAL ACCESS
608-4
606-5
EXECUTION
608-5
606-6
PRIVILEGE ESCALATION
608-6
606-7
DISCOVERY
604-3
VERTICAL
(Y)
604-1
TIME (Z)
606-8
COMMAND AND CONTROL
606-9
COLLECTION
604-2
LATERAL (X)
606-10
EXFILTRATION
608-7
606-11
PERSISTENCE
602

FIG. 6

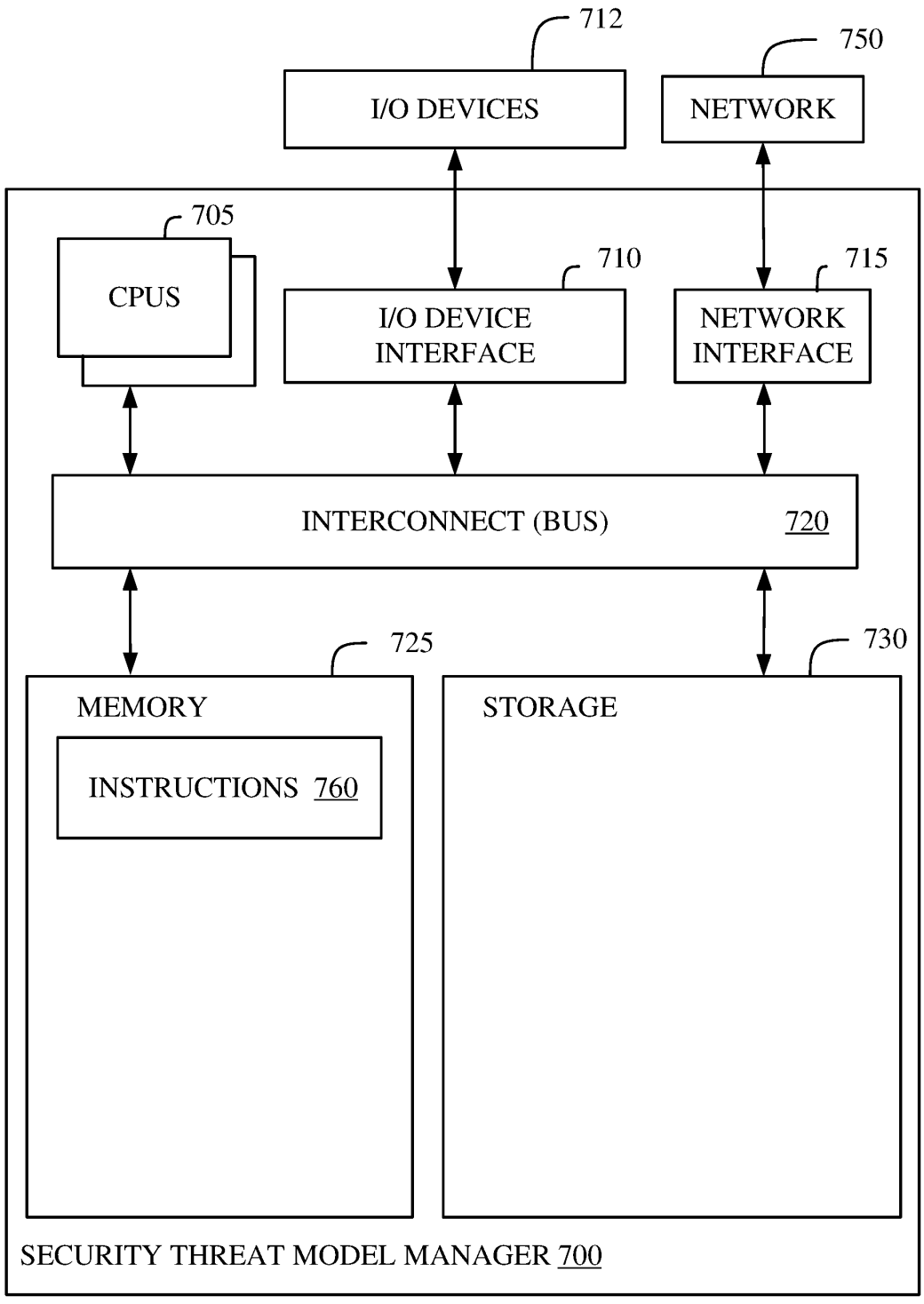

712
I/O DEVICES
750
NETWORK
705
CPUS
710
I/O DEVICE INTERFACE
715
NETWORK INTERFACE
INTERCONNECT (BUS) 720
725
MEMORY
INSTRUCTIONS 760
730
STORAGE
SECURITY THREAT MODEL MANAGER 700

**FIG. 7**

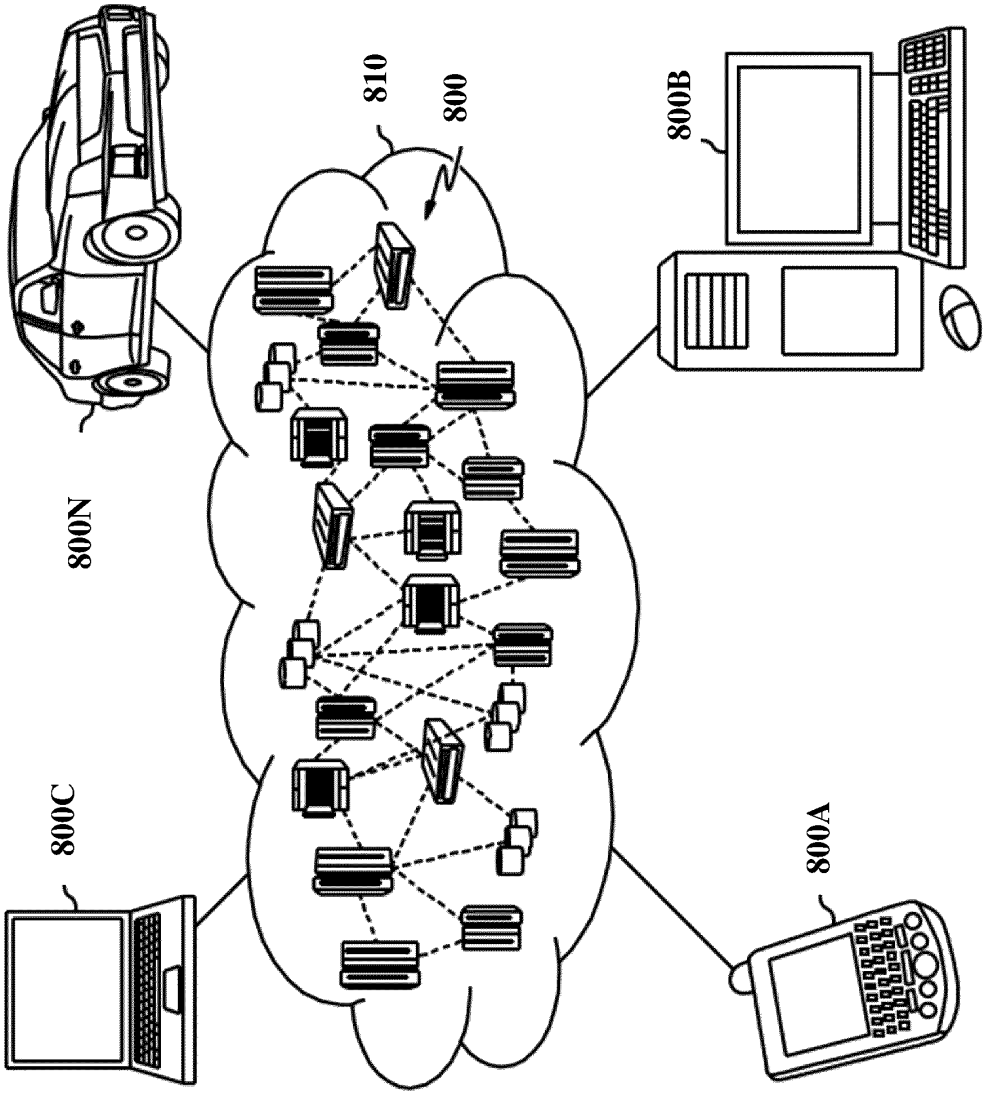



FIG. 8

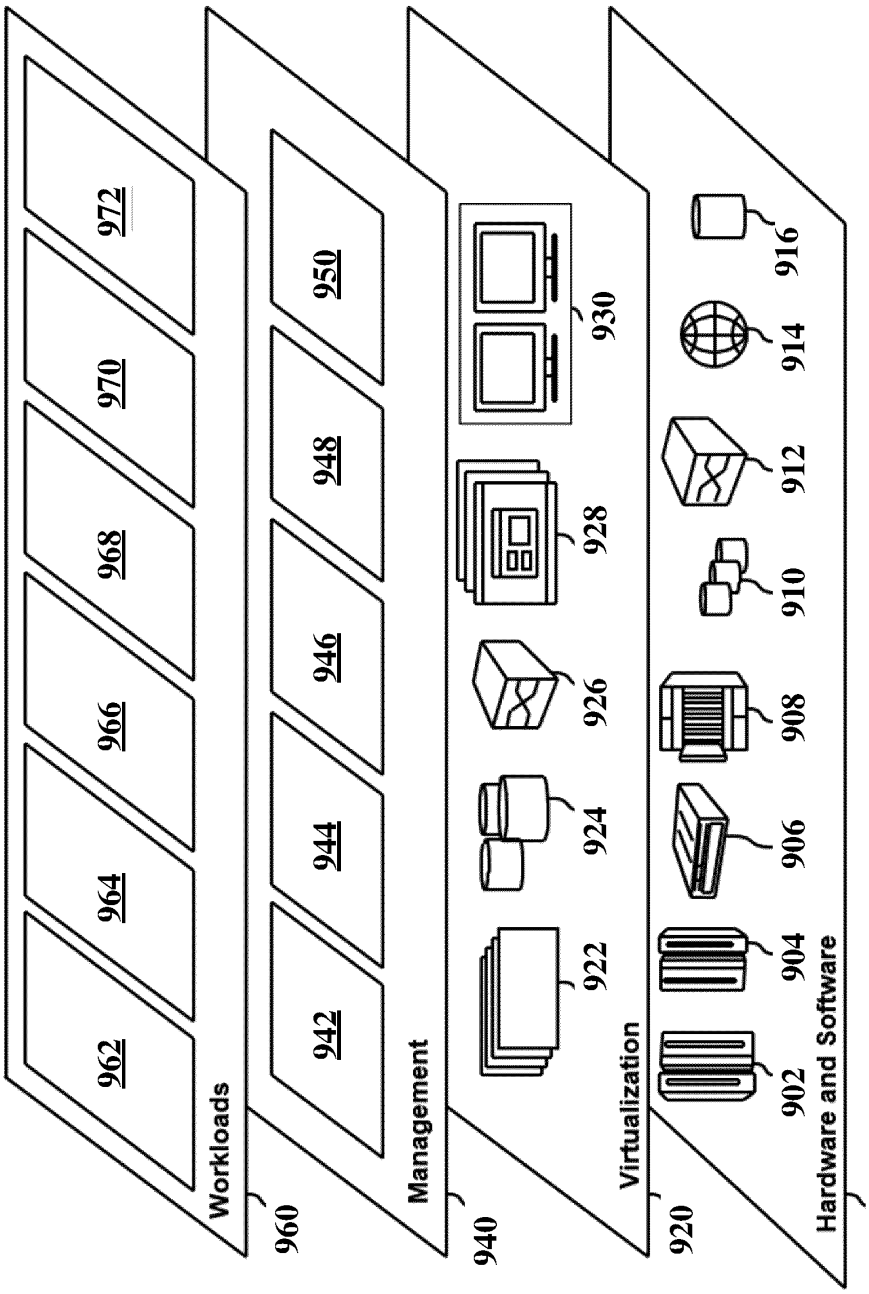

Workloads
960
962
964
966
968
970
972
Management
940
942
944
946
948
950
Virtualization
920
922
924
926
928
930
Hardware and Software
900
902
904
906
908
910
912
914
916

FIG. 9