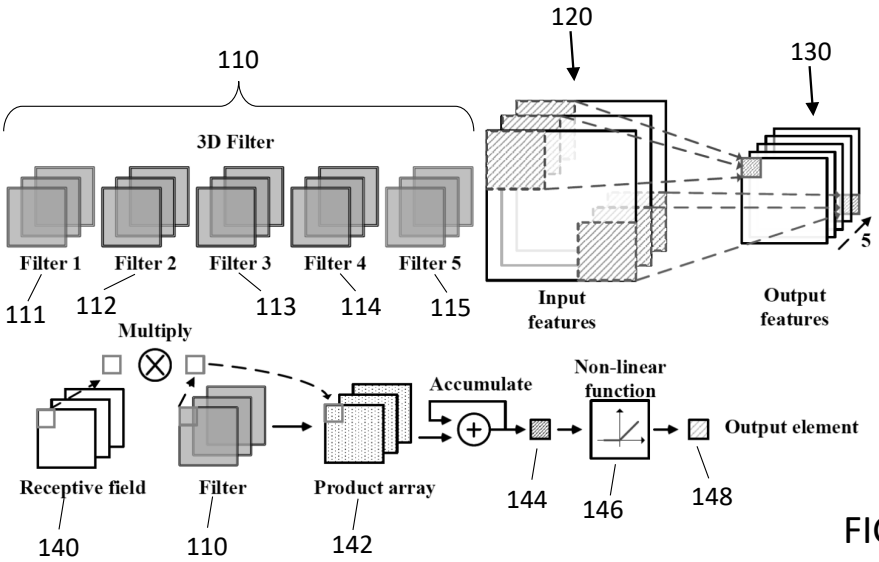

110
120
130
3D Filter
Filter 1
Filter 2
Filter 3
Filter 4
Filter 5
111
112
113
114
115
Input features
Output features
5
Multiply
Accumulate
Non-linear function
Output element
Receptive field
Filter
Product array
140
110
142
144
146
148

FIG.1

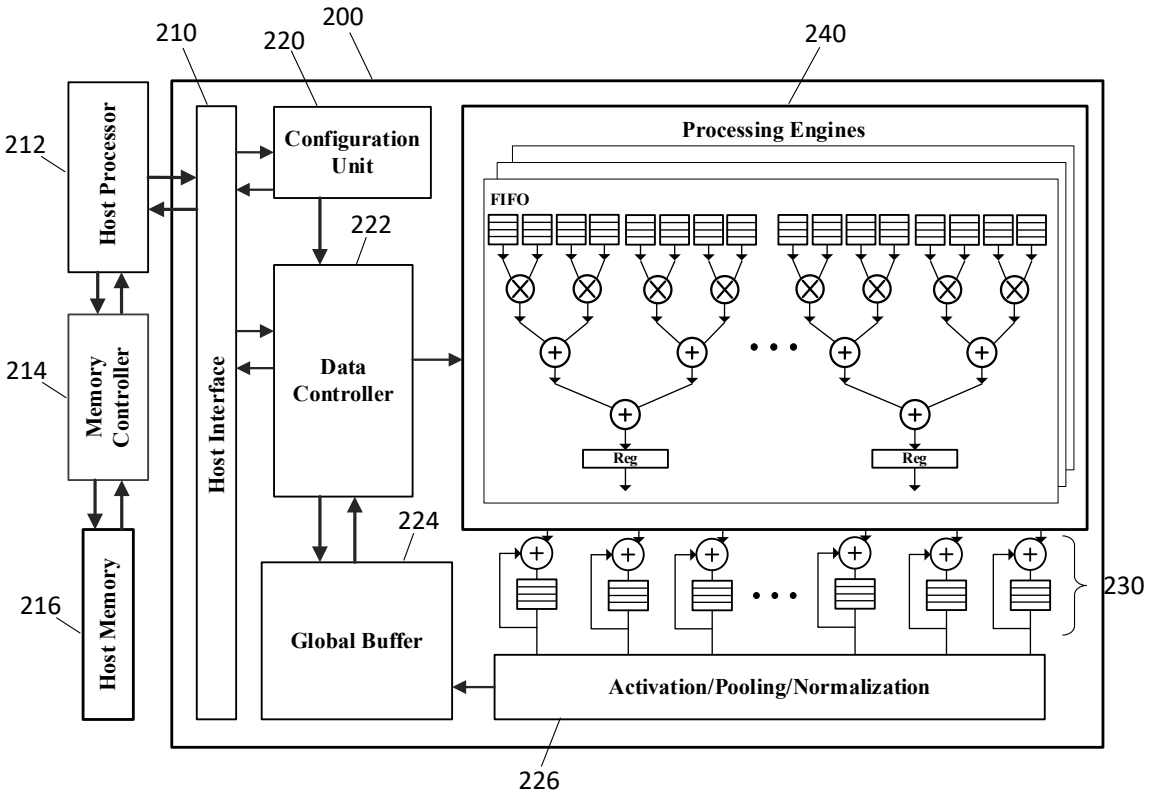

200
210
220
240
212
Host Processor
Configuration Unit
Processing Engines
FIFO
222
214
Memory Controller
Host Interface
Data Controller
Reg
224
216
Host Memory
Global Buffer
230
Activation/Pooling/Normalization
226

FIG.2

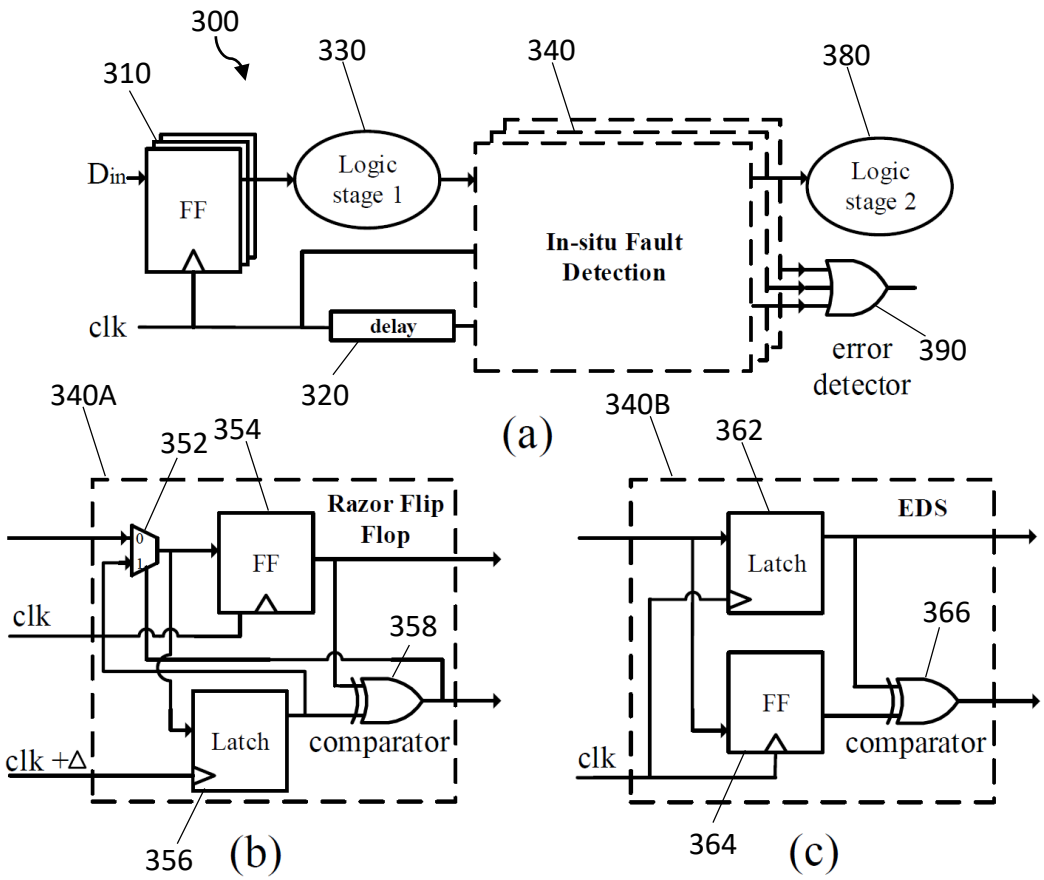

300
310
330
340
380
Din
FF
Logic stage 1
In-situ Fault Detection
Logic stage 2
clk
delay
320
error detector
390
(a)
340A
352
354
Razor Flip Flop
FF
clk
358
Latch
comparator
clk +Δ
356
(b)
340B
362
EDS
Latch
366
FF
comparator
clk
364
(c)

FIG.3

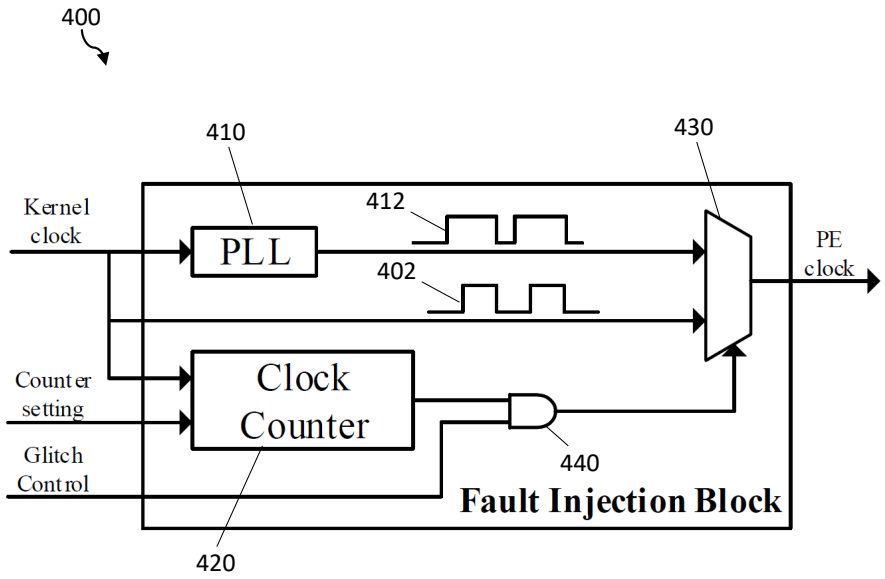

400
410
430
Kernel clock
PLL
412
402
PE clock
Counter setting
Clock Counter
Glitch Control
440
Fault Injection Block
420

FIG.4

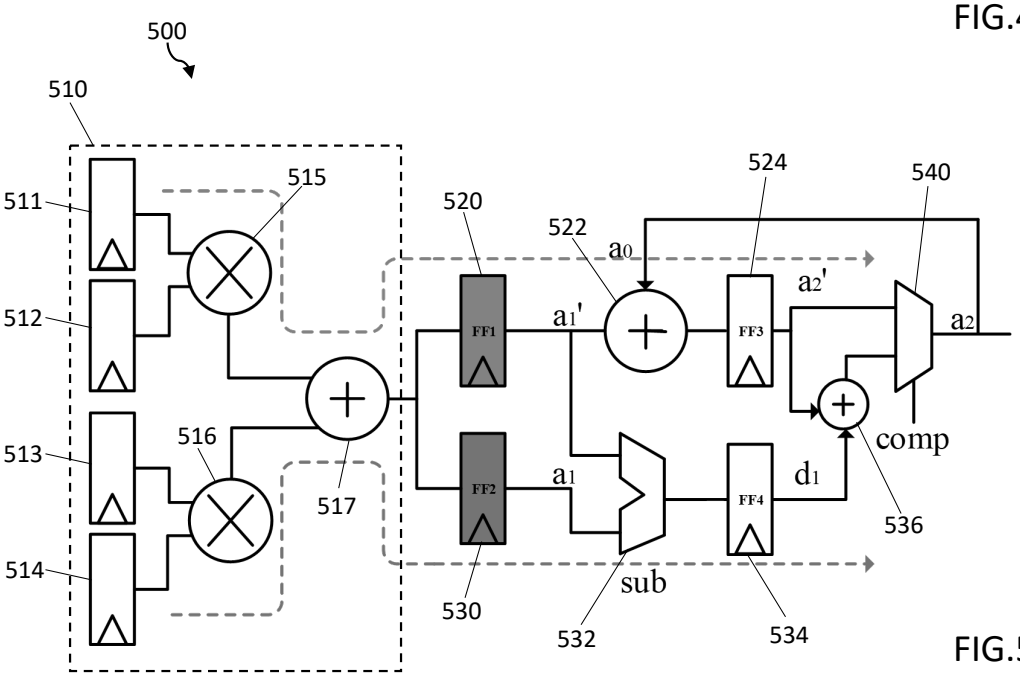

500
510
511
512
513
514
515
516
517
520
522
524
540
FF1
FF2
FF3
FF4
a0
a1'
a2'
a2
a1
d1
comp
sub
530
532
534
536

FIG.5

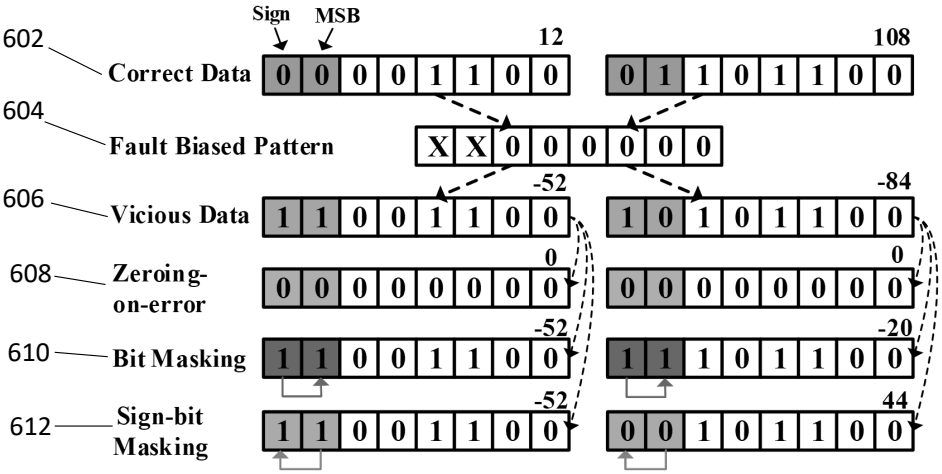

Sign
MSB
602
Correct Data
12
108
604
Fault Biased Pattern
606
Vicious Data
-52
-84
608
Zeroing-on-error
0
610
Bit Masking
-20
612
Sign-bit Masking
44

FIG.6

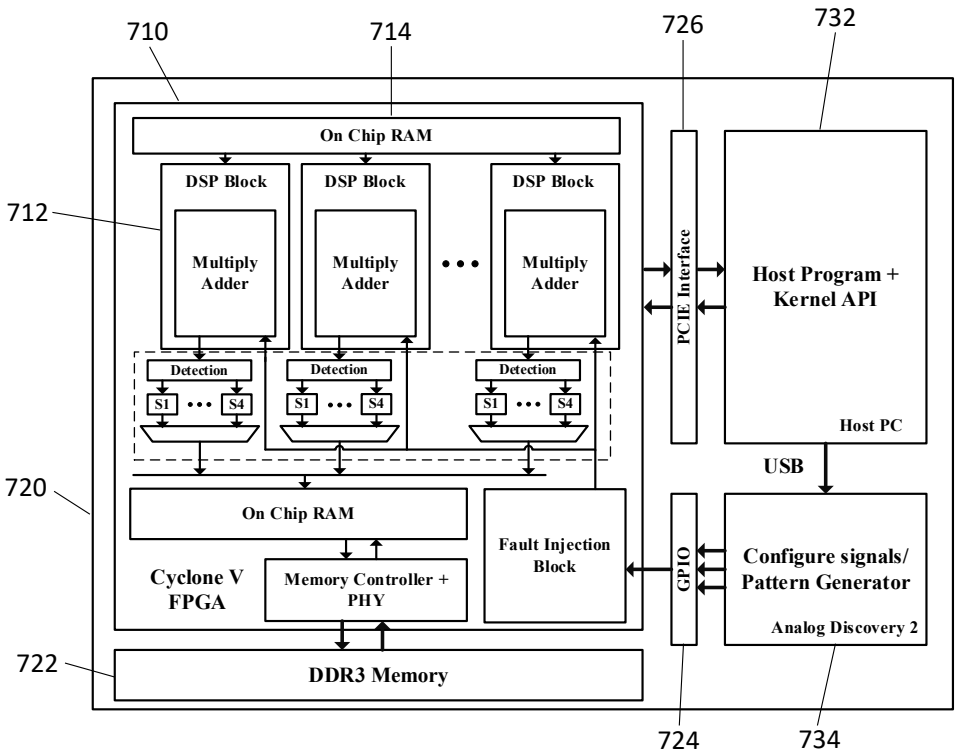

710
714
726
732
712
On Chip RAM
DSP Block
Multiply Adder
Detection
S1
S4
PCIE Interface
Host Program + Kernel API
Host PC
USB
720
On Chip RAM
Cyclone V FPGA
Memory Controller + PHY
Fault Injection Block
GPIO
Configure signals/ Pattern Generator
Analog Discovery 2
722
DDR3 Memory
724
734

FIG.7

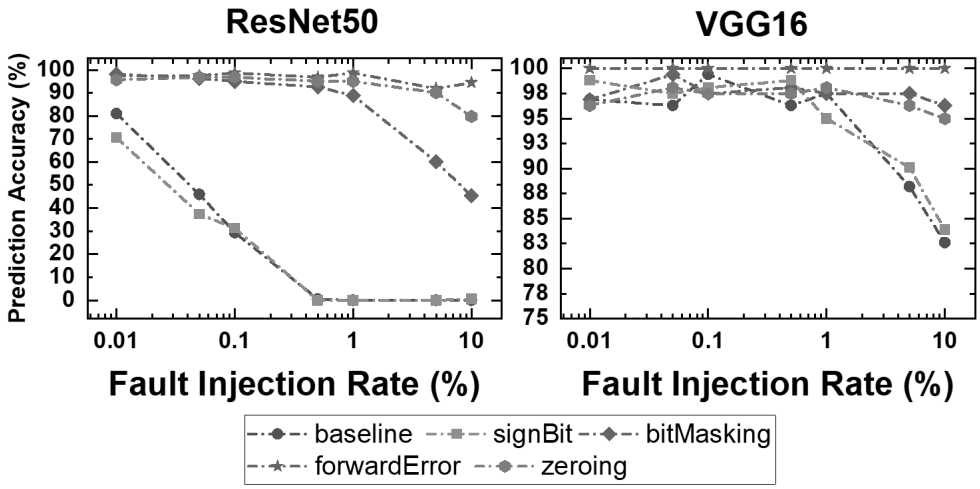

ResNet50
VGG16
Prediction Accuracy (%)
Fault Injection Rate (%)
Fault Injection Rate (%)
baseline
signBit
bitMasking
forwardError
zeroing

FIG.8

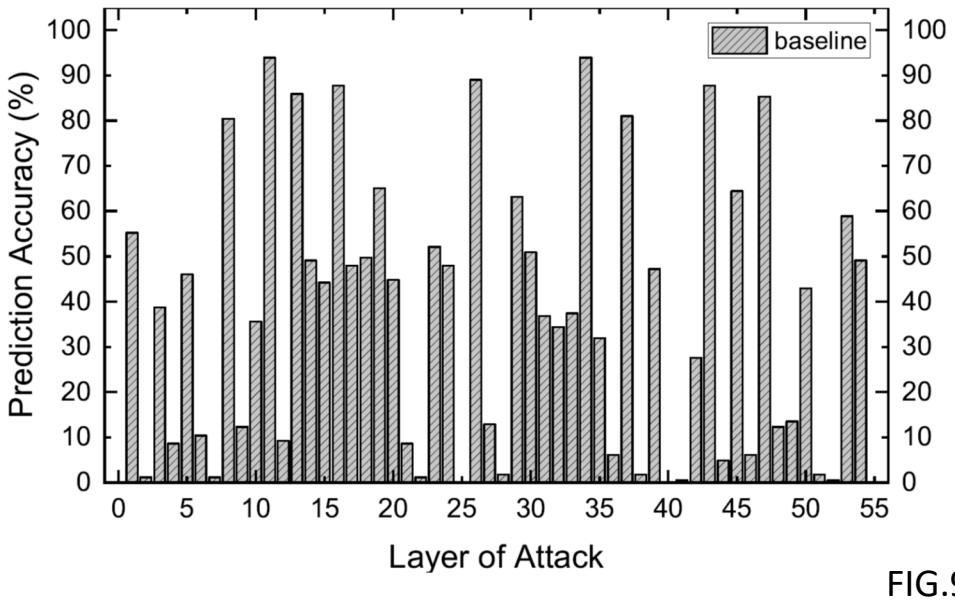

baseline
Prediction Accuracy (%)
Layer of Attack

FIG.9