BF Backtracking

back to the Bug in the Improper Operation

back to the Improper Operation

back to Improper Operand$_{2j}$

back to Improper Operand$_{np-2}$

from the Failure back to Improper Operand$_{np-1}$

Improper Operation

Improper Operand$_{2j}$

Improper Operand$_{3k}$

Improper Operand$_{np}$

Exploitable Error

Improper State$_1$

(operation $_1$,
operand $_{11}$, ...
operand $_{1ii}$, ...)

Improper State$_2$

(operation $_2$,
operand $_{2j}$, ...)

...

Improper State$_n$

(operation $_n$, ...
operand $_{np}$, ...)

Failure

Initial State − caused by the Bug

Final State − results in an Exploitable Error

Transition State − caused by a Fault

Failure − caused by exploitation of the Final Error