Target

HAI

Scenario

Description

Controller

Variable

Point

20.07

21.03

22.04

23.05

Long-term (LT) attack that decrease or

AP41

P1-FC

SP1-LT

P1_B3005

increase SP value of P1-FC continuously for

more than 10 minutes and restores to normal.

Decrease or increase CV value of P1-LC.

CV1

P1_LCV01D

Restore to normal.

P1-LC

AP42

PV1

P1_LIT01

Attempt to repeat previous sensor value.

PV2

P1_FT03

Attempt to maintain previous sensor value.

Long-term (LT) attack that decrease or

AP43

P1-LC

CV1-LT

P1_LCV01D

increase CV value of P1-LC continuously for

more than 10 minutes and restores to normal.

Decrease or increase CV value of P1-LC.

CV1-LT

P1_LCV01D

AP44

P1-LC

Restore to normal.

PV1-LT

P1_LIT01

Attempt to repeat previous sensor value.

Decrease or increase SP value of P1-TC.

AP45

P1-TC

SP1

P1_B4002

Restore as a form of a trapezoidal profile while

hiding SP changes in HMI.

Decrease or increase CV value of P1-CC.

CV1

P1_PP04

AP46

P1-CC

Restore to normal.

PV1

P1_TIT03

Attempt to repeat previous sensor value.

Long-term (LT) attack that decrease or

AP47

P2-TC

SP2-LT

P2_VTR02

increase SP value of P2-TC continuously for

more than 10 minutes and restores to normal.

TOTAL

14

25

37

37

ATTACK SCENARIOS TARGETING INTERNAL POINTS

Attack scenarios targeting internal points modulate the algorithm function used inside the control logic. The boiler DCS of the HAI testbed employs various algorithm functions, and we developed attack scenarios that target the artificial I/O, arithmetic, and monitor functions.

Artificial I/O function: This function is used to initialize an algorithm function with internal parameters. An attacker can tamper the output of the algorithm function when the process is initialized by modulating the internal parameters.

Arithmetic function: This function is utilized to generate calibration curves for sensor inputs or control command outputs. An attacker can degrade the performance of a sensor or controller by changing calibration tuning parameters.

Monitor function: This function monitors whether the input signal crosses the high/low threshold. An attacker can change the threshold to cause over-detection or no-detection of anomalies.

A trigger-type attack, in which an attack only occurs in a specific situation, can be implemented if the internal parameters of the algorithm function are changed. The artificial I/O function can modulate the output of the control signal associated with the algorithm function into an arbitrary value at initialization. The arithmetic function triggers an attack only when the input value reaches the area affected by the calibration adjustment parameter. The monitor function triggers an attack only when