ATTACK SCENARIOS

All attack scenarios in the viewpoint of a feedback control scheme were configured based on four types of variables, namely the setpoints (SPs), process variables (PVs), control variables (CVs), and control parameters (CPs). An attacker can control all variables by indirectly manipulating any algorithm

blocks in the embedded controllers such as the setpoint algorithm, PID controller, signal conditioner and others. Thus, an attacker can ultimately achieve a stealthy attack on the control device.

OWS

Set-Points (SPs)

70 92

Attacker

Operator

Control Parameters (CPs)

EWS

Maintanance

SP attacks

Controller

Set-point algorithm

CP attacks

PID controller

CV/PV attacks

Signal conditioner

Control Variables (CVs)

Process Variables (PVs)

Actuators

Sensors

Boiler, Turbine, Water-treatment Process

FIGURE 14. ATTACK MODEL BASED ON A PROCESS CONTROL LOOP(PCL).

The variables and parameters of the process control loop (PCL) are represented as "points" on the control device. A point is a variable allocated in memory for data access. I/O points are used for external peripheral device connection, whereas internal points are used for internal variables. The SP, PV, and CV variables of PCL correspond to I/O points. These points exchange information through hard-wired connections with external devices such as OWS and remote I/O. The internal points are only accessible to EWS that corresponds to CPs of PCL.

Normal Behaviors

During normal operation, it is assumed that the operator operates the control facility in a routine manner via the HMI, and that the simulator variables associated with power generation in the HIL simulator are changed. The operator monitors the PV values given by the current sensor displayed on

the HMI, and adjusts the SPs of the various control devices to operate the system.

HMI operation task scheduler was used to periodically set the SPs and HIL simulator variables to random or predefined values within the normal range to simulate a benign scenario. The normal ranges of SP values in which the entire process was stable were determined by experimentally changing the value of each SP.

The four controllers (P1-PC, P1-LC, P1-FC, and P1-TC) and two simulation models (steam turbine power generator and pump-storage hydropower generator) were automatically operated several times

a day. These were initiated with a random delay, and a random value or predefined value within the normal operational range was reached. All SP values were recorded to learn the system features