Chapter 13
Cyber-Attack Detection for a Crude Oil Distillation Column

H. M. Sabbir Ahmad, Nader Meskin, and Mohammad Noorizadeh

13.1 Introduction

13.1.1 Preliminary

Due to the continuous development of technology, an increasing number of electronic devices are being developed with networking features suitable for connecting to industrial networks. This technological evolution has also made its way to Industrial Control Systems (ICSs) where an increasing number of monitoring and controlling devices have been connected to computer networks facilitating the supervisory level monitoring and control. Evolution in computing and internet technology has encouraged increasing number of ICS to be linked to cyber-world giving rise to a new class of systems called Cyber-Physical System (CPS) which provides several economic and performance-enhancing benefits. However, it also makes ICS more vulnerable to cyber-attacks. The effect of cyber-attacks differs in cyber-physical critical ICS compared to traditional ICT systems as they can cause damage to physical infrastructure posing threats to human health and environment. The complex CPS infrastructure more than ever requires the development of novel security solutions, as these systems are continuously targeted by attacks and intrusions by intelligent adversaries. Some typical examples of attacks in real systems are the Stuxnet worm attack, multiple recent power blackouts in Brazil, and the SQL Slammer worm attack on the Davis–Besse nuclear plant, to name a few (Pasqualetti et al. 2012; Nourian

H. M. S. Ahmad · N. Meskin (✉) · M. Noorizadeh
Qatar University, Doha, Qatar
e-mail: nader.meskin@qu.edu.qa

H. M. S. Ahmad
e-mail: ha1607441@student.qu.edu.qa

M. Noorizadeh
e-mail: m.noorizadeh@qu.edu.qa

M. Abbaszadeh and A. Zemouche (eds.), *Security and Resilience in Cyber-Physical Systems*, https://doi.org/10.1007/978-3-030-97166-3_13

and Madnick 2018; Pasqualetti et al. 2015), further justifying the need to address cyber-security for ICS.

Extensive research has been conducted on security issues from the prospective of network and communication technologies to securely defend network performance against adversaries. These research works have mainly concentrated on designing methodologies to secure communication networks in CPS ignoring interactions between the cyber and physical domain. Traditionally, cyber-security for ICS has been dealt by IT engineers from the prospective of network security. Such approaches primarily aim to secure the communication network to protect the IT infrastructure without considering the physical behavior of the plant and how the ICS is affected by cyber-attack. ICS are characterized by feedback closed-loop control architecture and aim to optimize the system control performance, such as reducing state estimation errors, stabilizing an unstable plant, and enhancing the robustness against uncertainties and noise. Therefore, it is important to guarantee the resiliency of cyber-physical ICS subject to multiple types of malicious attacks. This chapter focuses on the development of cyber-attack detection technique for a Cyber- Physical Distillation Column.

13.1.2 Cyber-Security of Distillation Column

Cyber-security of CPS has become a hot topic of research lately with focus on a wide range of physical plants. In Kundur et al. (2011), Manandhar et al. (2014), He et al. (2017), Kurt et al. (2019), cyber-security for smart grid has been studied and in Abokifa et al. (2019), the effect of cyber-attacks on water distribution systems is investigated. In Li et al. (2019), Kravchik and Shabtai (2018), Lin et al. (2018), Adepu and Mathur (2021), Elnour et al. (2020), different techniques for detecting attacks on a cyber-physical Reverse Osmosis Water Treatment Plant are presented. In Noorizadeh et al. (2021), a hybrid testbed is developed for Tennessee Eastman process and different data-driven detection algorithms are developed and tested. In Elnour et al. (2021), the security of Smart Buildings has been studied. To the best of the author's knowledge, cyber-security for a Crude Oil Distillation Column (DC) is only considered in Sabbir Ahmad and Meskin (2020) where the system dynamics simulated using Aspen Plus Dyanmics was integrated with Simulink and an observer-based attack detection scheme was implemented and validated using computer simulation in Simulink. In this study, first a detailed dynamical model of the DC is presented and a HIL testbed is designed for a cyber-physical DC using hardware from Siemens. Finally, an online real-time distributed detection scheme is proposed based on Unscented Kalman Filter (UKF) scheme implemented directly on PLCs.

In Taqvi et al. (2016), Minh and Pumwa (2012a), George and Francis (2015), Kathel and Jana (2010), Zou et al. (2017), Bendib et al. (2015), Radulescu et al. (2007), Weerachaipichasgul et al. (2010), a set of equations collectively called MESH equations are presented to describe the internal dynamics of a distillation column.

In Taqvi et al. (2017), the column model is described in terms of the relationship between the inputs and outputs which are generated using data from Aspen Plus Dynamics. In Minh and Pumwa (2012a), George and Francis (2015), Kathel and Jana (2010), Zou et al. (2017), a binary continuous distillation column is simulated with the assumption that the molar hold up in each tray including the condenser and reflux drum remains constant and there is negligible vapor holdup in each tray. This assumption neglects the dynamics of liquid and vapor flow rates inside the column due to tray hydraulics which have significant time constants impacting the dynamic performance of the model. In Bendib et al. (2015), the MESH equations are presented without any description for liquid and vapor flow rates dynamics inside the column. The crude feed is considered as a pseudo-binary mixture with a constant relative volatility in Minh and Pumwa (2012a), George and Francis (2015), Kathel and Jana (2010), Zou et al. (2017), Bendib et al. (2015) which is not the case in reality as the volatility varies with temperature and pressure. Finally, the fundamental limitation of using input–output relationship for distillation column simulation is that the internal dynamics which contains information on individual trays inside the column is ignored. Such information can be extremely valuable in several ways, one of which is temperature inferential output product quality measurement. The purity of output product stream can be determined using off-line analyzers which is indeed time-consuming. Time inferential measurement is fast and provides an efficient way of controlling the quality of the products from a distillation column.

As part of this study, the DC plant presented in Minh and Pumwa (2012a, b) is considered and the presented data to design the column in Aspen Plus is used to generate the steady-state data. Then, in order to improve the model accuracy, the DC plant is transported into Aspen Plus Dynamics to observe the effect of various column parameters to include them in the mathematical model. Finally, using the steady-state data, the dynamical model is simulated in real-time using MESH equations given in Minh and Pumwa (2012a, b) inside Simulink environment.

Next, a hybrid Hardware-In-the-Loop (HIL) ICS testbed is developed and implemented for the DC plant using industrial automation hardware from Siemens to make the study resembles a practical ICS. The hybrid HIL testbed contains three layers: (I) Field layer, (II) Control layer, and (III) Supervisory layer, and PROFINET as an industrial communication protocol is used for communication between I/O modules and PLCs. Different types of attack on ICS sensors and actuator such as false data injection attack (Lv et al. 2019; Zhang et al. 2017) (scaling attack, bias injection attack, etc.), Denial of Service (DoS) attack (Meraj et al. 2015), replay attack (AlDairi and Tawalbeh 2017) are emulated inside the testbed using their mathematical representation.

Finally, an online distributed attack detection method for the DC plant is developed and implemented in real-time on the testbed PLCs. The proposed detection algorithm is based on state estimation using UKF. There are various nonlinear state estimators available. As part of this study, three factors are considered while choosing UKF, namely, convergence, implementation simplicity (the estimators are implemented inside the PLCs which have limited mathematical library tool set), and computational complexity (PLCs have limited computational ability). Based on these criteria, UKF is chosen as it is able to provide full system state estimation based on the systems inputs and outputs in the presence of process and measurement noise which provided the main motivation for the choice of this algorithm. Computationally, the algorithm primarily involves basic linear mathematical operations (addition, subtraction, and multiplication) which could be easily implemented inside the PLCs. The fundamental idea is that during normal operation, the estimated measurements will coincide with the actual measurements, while in the presence of any attack, there will be deviation between the estimated and actual measurements. Hence, by computing the residuals corresponding to the difference between the actual and estimated measurements and comparing them with a given threshold, attacks can be successfully detected. Various formulated attack scenarios are emulated inside the testbed and performance of the proposed detection scheme is demonstrated.

This chapter includes seven sections. In Sect. 13.2, the mathematical model and the control system of the DC plant are presented and the details of the developed hybrid testbed are discussed in Sect. 13.3. Next, the mathematical models of various attacks used in this study are provided in Sect. 13.4 and the proposed attack detection algorithm is presented in Sect. 13.5. The results corresponding to different attack scenarios injected in the developed testbed are given in Sect. 13.6. Finally, the summary of the chapter is presented in the conclusion section.

13.2 Distillation Column Design and Modeling

A continuous binary distillation splits a crude feed into two fractions, which are collected from the top and bottom sections of the crude tower. The raw crude is fed to the binary column at the feed section and the column can be divided into two sections, namely, rectifying and stripping section. The rectifying section is located at the top just above the feed and the bottom section is called the stripping section. The original crude feedstock is passed through a preheater which heats the feed to a certain temperature in order to convert it into a two phase fluid before feeding to the distillation column. Inside the column, the temperature gradient causes the relatively volatile lighter components to vaporize and rise to the top of the column, and the less volatile heavier components fall down to the bottom section of the column. The vapor at the top is cooled down by a condenser and collected at the reflux drum where a portion of it is extracted out as distillate and the remaining cooled liquid (known as reflux) is fed back to the column. Similarly, the liquid at the column base is collected in reboiler drum where a portion of it is extracted out as bottoms product and the remaining portion is vaporized by the reboiler and fed back to the column.

13.2.1 Plant Data

The considered DC model is based on a real petroleum project presented in Minh and Pumwa (2012a, b). The plant operates for 24 h and 365 d over a year during which it processes 130,000 tons of raw condensate. Figure 13.1 illustrates the flowsheet of the binary distillation column considered in this work. The plant operating specification is to maintain the product quality within desired range; the purity of the distillate has

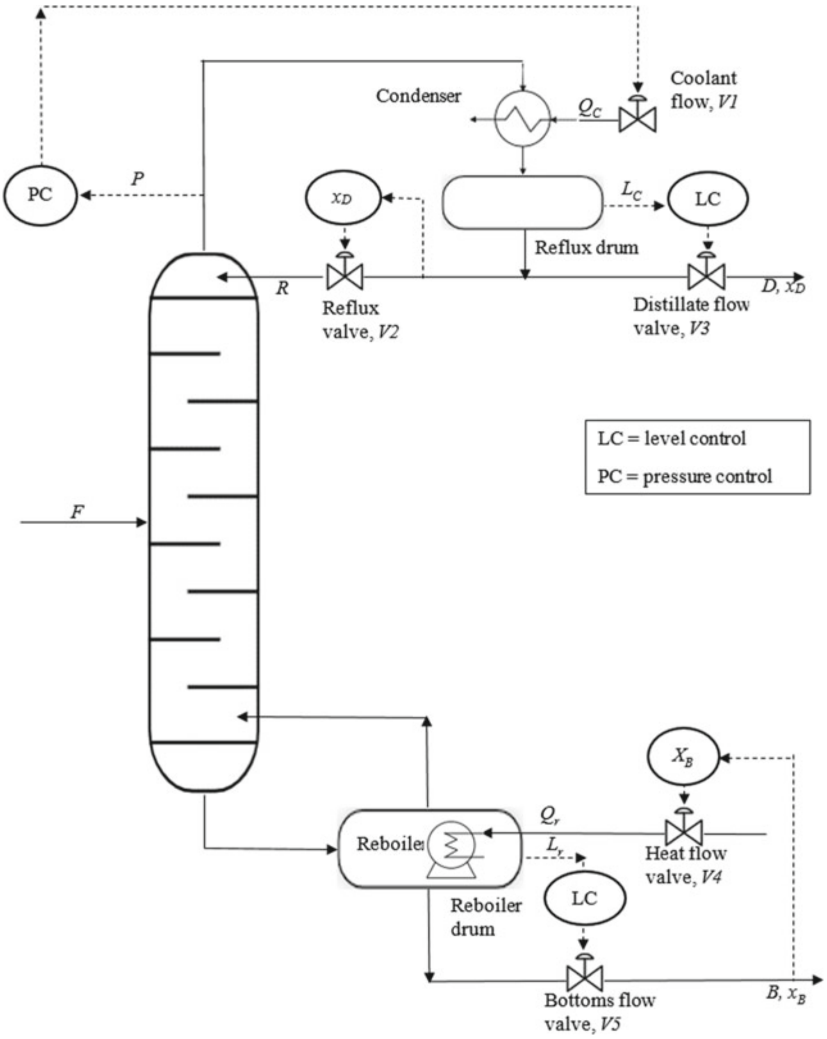

Fig. 13.1 Flowsheet of a binary distillation column, ©2020 IEEE. Reprinted, with permission, from Sabbir Ahmad and Meskin (2020)

Table 13.1 Raw condensate composition

Component	Mole fraction	Component	Mole fraction (%)
Propane	0.00	n-C11H24	1.94
Normal Butane	19.00	n-C12H26	2.02
Iso-Butane	26.65	Cyclopentane	1.61
Iso-Pentane	20.95	Methylclopentane	2.02
Normal Pentane	10.05	Benzene	1.61
Hexane	7.26	Toulen	0.00
Heptane	3.23	O-xylene	0.00
Octane	1.21	E-benzen	0.00
Nonane	0.00	124-Mbenzen	0.00
Normal Decane	0.00		

Table 13.2 Properties of pseudo components

Properties	Ligas	Napthas
Molar weight	54.5–55.6	84.1–86.3
Liquid density (kg/m^3)	570–575	725–735
Feed composition (vol%)	48–52	48–52

to be higher than or equal to 98% and the impurity of the bottoms has to be equal or less than 2%.

Table 13.1 presents the nominal composition of the raw condensate and the actual composition of the raw condensate generally fluctuates around their nominal values. Although the liquid feed consists of multiple components, however, since the aim is to use a binary distillation column, a pseudo-binary mixture is considered consisting of Ligas (iso-butane, n-butane, and propane) and Napthas (iso-pentane, n- pentane, and heavier components). There are 14 trays inside the column with the topmost tray is numbered as the first layer. The properties of the pseudo components are allowed to fluctuate within the range shown in Table 13.2 based on the fluctuation in the condensate composition. Before feeding to the column, the raw crude is passed through a preheater to convert it into two phases which are vapor and liquid phase and fed to trays 7 and 8, respectively.

13.2.2 Distillation Column Design

The column is designed using Redfrac model available in ASPEN Plus where two degrees of freedom are considered for the column design and distillate rate (kmole/hr)

Table 13.3 Column design parameters used in Aspen Plus

Parameter	Value	Parameter	Value
Feed temperature (°C)	118	Feed pressure (atm)	4.6
Condenser pressure (bar)	4	Stage pressure drop (bar)	0.075
Distillate rate (kmole/hr)	93	Reflux rate (kmole/hr)	350
Vapor feed stage	7	Vapor feed rate	185.827
		(kmole/hr)	
Liquid feed stage	8	Liquid feed rate	16.937
		(kmole/hr)	
Ligas concentration	0.513	Ligas concentration	0.127
In vapor feed		In liquid feed	

and reflux rate (kmole/hr) are the two parameters selected for the column design. Table 13.3 presents the data used in ASPEN Plus for the column design.

13.2.3 Dynamic Model of the Distillation Column

The dynamics of the nth tray using mass and balance equations can be written as

$$\frac{\mathrm{d}M_n}{\mathrm{d}t} = L_{n-1} - L_n + V_{n+1} - V_n \tag{13.1}$$

$$\frac{\mathrm{d}(M_n x_{n,i})}{\mathrm{d}t} = L_{n-1}x_{n-1,i} - L_n x_{n,i} + V_{n+1}y_{n+1,i} - V_n\, y_{n,i}, \tag{13.2}$$

where M_n is the liquid hold up (kmole) in the nth tray inside the column, L_n and h_n denote the flow rate (kmole/hr) of the liquid flowing down the nth tray and the amount of heat energy that is passed with the liquid from the nth tray, respectively, V_n and H_n denote the vapor flow rate (kmole/hr) at the nth tray and the energy carried by the vapor, respectively, and $x_{n,i}$ and $y_{n,i}$ denote the liquid and vapor mole fraction of the ith component in tray n, respectively, where

$$\sum_{i=1}^{C} x_{n,i} = 1\,;\ \sum_{i=1}^{C} y_{n,i} = 1, \tag{13.3}$$

with C as the number of components in the feed. Since, it is assumed the feed to be a pseudo-binary mixture, we have $C = 2$ and it is only necessary to consider the molar concentration dynamics of the lighter component based on the summation condition.

By differentiating (13.2) and substituting (13.1), it follows that

$$\frac{\mathrm{d}(x_{n,i})}{\mathrm{d}t} = \frac{L_{n-1}x_{n-1,i} + V_{n+1}y_{n+1,i} - (L_{n-1} + V_{n+1})x_{n,i} + V_n(y_{n,i} - x_{n,i})}{M_n}. \tag{13.4}$$

The column is numbered from top as $n = 1$ for the reflux drum, $n = 2$ for the first tray, $n = f$ for the feed tray, $n = N + 1$ for the bottom tray, and $n = N + 2$ for the reboiler with total of 14 trays inside the column, i.e., $N = 14$.

In order to perform a dynamic simulation to observe the dynamics of the tray hydraulics, the model from Aspen Plus is transported to Aspen Plus Dynamics. It is indeed necessary to include this dynamics since the time constants associated with liquid and vapor flow rates are quite large which will affect the overall response time of the system. Hence, the effect of tray hydraulics is included (as continuous system states) to the liquid and vapor flow rates across every tray in the column by introducing a time constant as follows:

$$dL_n(s) = \frac{1}{\tau_{L_n}s + 1}dL(s) \tag{13.5}$$

$$dV_n(s) = \frac{1}{\tau_{v_n}s + 1}dV(s), \tag{13.6}$$

where $dL = L - L^{\text{nominal}}$, $dL_n = L_n - L_n^{\text{nominal}}$, $dV = V - V^{\text{nominal}}$, and $dV_n = V_n - V_n^{\text{nominal}}$. L_n^{nominal} and V_n^{nominal} are the nominal liquid and vapor flow rates for the nth tray inside the column which have been acquired from Aspen Plus. The time constants are determined from Aspen Plus Dynamics. The initial molar holdup in each tray has been computed using the Francise–Wier formula presented in Wijn (1999). The following assumptions are considered here

- The relative volatility is constant across each tray of the column. This implies that the vapor–liquid equilibrium relationship for the nth tray can be expressed as

$$y_n = \frac{\alpha x_n}{1 + (\alpha - 1)x_n}.$$

- The overhead vapor is totally condensed in a condenser.
- The pressure remains constant at the top of the column and the differential pressure between trays remains constant.
- The holdup of vapor is negligible throughout the system.

The overall model of the DC plant is expressed as follows:

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}(t), \boldsymbol{u}(t)) + \boldsymbol{w}(t) \tag{13.7}$$

$$\boldsymbol{y}(t) = \begin{bmatrix} x_1(t) \\ x_{16}(t) \end{bmatrix} + \boldsymbol{v}(t), \tag{13.8}$$

where

$$x(t) = [x_1(t), x_2(t), \ldots, x_{16}(t), M_1(t), M_2(t), \ldots, M_{16}(t),\\ L_2(t), L_3(t), \ldots, L_{15}(t), V_2(t), V_3(t), \ldots, V_{15}(t)]^T$$

is the state variable of the system, where for brevity, the subscript i is dropped from $x_{n,i}$ due to having only two components in DC, $u(t) = [L_1(t), V_{16}(t)]^T$ is the control input signal, and w and v are the process and measurement noise vector, respectively which have been modeled as Gaussian white noise.

13.2.4 Control of Distillation Column

13.2.4.1 Control Requirement for Distillation Column

In order to control a binary DC plant, at first, it is essential to determine its degree of freedom (DoF). DoF of a process is the number of independent variables that must be specified in order to define the process completely. Consequently, the desired control of a process will be achieved when and only when all degrees of freedom have been specified. Among several available approaches, one of the simple approaches to determine the DoF for a DC plant is to count the number of valves. There are four control valves as shown in Fig. 13.1, one on each of the following streams: distillate, reflux, bottoms, and reboiler vapor, and hence this column has four degrees of freedom. The feed stream is considered being set by the upstream process and consequently it is considered to be a constant. Inventories in any process must be always controlled, and the inventory loops involve liquid levels and pressures. The column has been designed in Aspen Plus to operate under constant pressure at the top of the column with a constant differential pressure between the trays and this implies that the liquid level in the reflux drum and the liquid level in the column base must be controlled. Hence, by considering the two variables that must be allocated for controlling the liquid level in the reflux drum and column base, there exist two remaining degrees of freedom. Thus, there are two and only two additional variables that can (and must) be manipulated to maintain the product quality of distillate and bottoms product.

Generally, a column is designed to operate in the steady state at the values determined from design calculations during normal operation and a column remains at energy and material balance (described by MESH equations) during the steady-state operation. Material balance infers that the sum of products entering the column must be equal (approximately) to the sum of products leaving the column, and energy balance implies that the heat input to the column must be equal (approximately) to heat removed from the system. A column is said to be "stable" when it is under energy and material balance.

Table 13.4 Manipulated and controlled variable pairs for the binary distillation column

Controlled variables	Manipulated variables	Control valve (Fig. 13.1)
Purity of distillate	Reflux flow rate	Reflux flow V_2
Liquid level in reflux drum	Distillate flow rate	Distillate flow V_3
Impurity in bottoms	Reboiler duty	Heat flow V_4
Liquid level in column base	Bottoms flow rate	Bottom flow V_5

The column dynamics arises from the control loops, i.e., if value of a control variable fluctuates from its desired value then the corresponding manipulated variable is adjusted to bring the control variable back to its desired value. Such changes in value of control variables may occur due to various reasons including change in properties of the feed within the range mentioned in Table 13.2.

13.2.4.2 Controller Design for Distillation Column

As mentioned previously, the proposed DC in Fig. 13.1 has four control and four controlled variables. Table 13.4 summarizes the control variables selected to control each of the four controlled variables. The PID controllers for distillation and bottoms product composition control is tuned using model-based PID tuning tools available from MATLAB. A PID controller contains a proportional, integral, and derivative term associated with each is a constant gain, that takes into account tracking error to achieve error convergence. The PID controller is given as

$$u(t) = K_p e(t) + K_i \int e(t)dt + K_d \frac{\mathrm{de(t)}}{\mathrm{d}t}, \tag{13.9}$$

where $e(t) = y(t) - y_d(t)$, $y(t)$ is the output and $y_d(t)$ is the set-point.

The levels of the reflux drum and column base are maintained constant by adjusting the distillate and bottoms product flow, respectively, using the feed-forward control as

$$D(t) = V_{14}(t) - L_{\text{refluxflow}}(t), \tag{13.10}$$

$$B(t) = L_1(t) - V_{\text{vaporflow}}(t), \tag{13.11}$$

where $V_{14}(t)$ and $L_1(t)$ represent the vapor (kmole/hr) flowing out of tray 14 into the condenser and liquid (kmole/hr) flowing from tray 1 to the reboiler, respectively, $D(t)$ corresponds to the distillate flow rate (kmole/hr) and $B(t)$ corresponds to the bottoms product flow rate (kmole/hr).

13.3 Testbed Design

The hybrid testbed is designed to implement an ICS for the DC by integrating industrially used hardware in the simulation loop to make the study practically viable. The control objective of the DC plant is to maintain the purity of the distillate from the rectifying section and the bottoms product from the stripping section. Therefore, the DC has two outputs which are controlled using the two inputs which are the reflux flow rate (kmole/hr) and the vapor flow rate (kmole/hr) from the reboiler. The developed hybrid testbed contains two control PLCs: one for the rectifying section regulating the quality of the distillate and the second for the stripping section regulating the bottoms impurity level.

As part of this study, a three-level hybrid HIL Cyber-Physical ICS testbed is designed for the DC as shown in Figs. 13.2 and 13.3. The DC dynamics is simulated in real-time in a PC using Simulink and a data acquisition board (DAQ) is used to generate the measurements as well as receiving the valves commands from the controller. The field layer (Level 0) of the testbed is implemented using ESP-200 Distributed I/O modules from Siemens which are connected to DAQ. The control layer (Level 1) is implemented using Siemens S7-1500 PLCs which are interfaced to the Distributed I/Os using PROFINET which is an industrially used communication network. In addition, the second layer has a supervisory engineering station for supervisory monitoring an control. Finally, a cloud server is included in the testbed in the third layer (Level 2) for remote logging and online monitoring of the testbed. The link between simulator and the ICS is established using Humosoft MF634 DAQ

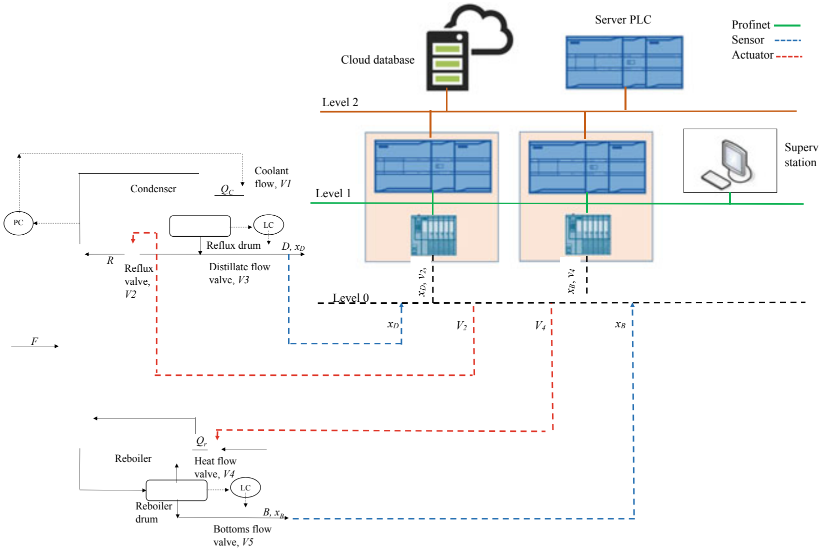

Fig. 13.2 Block level diagram of the DC testbed

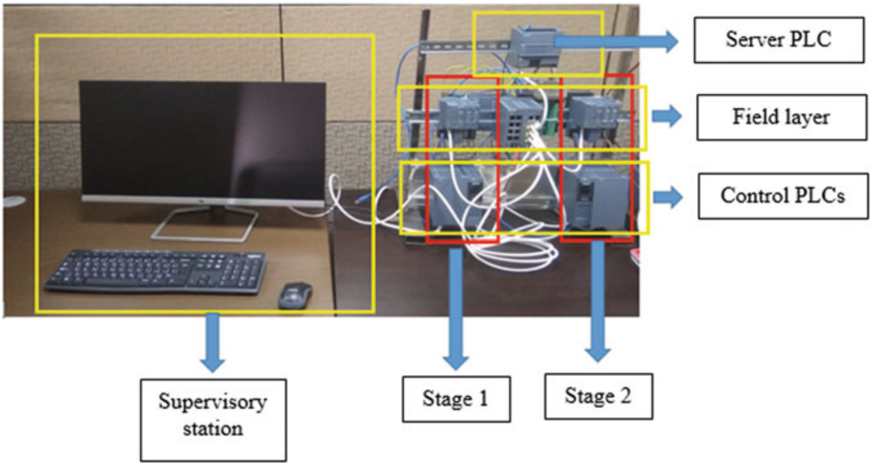

Fig. 13.3 The developed cyber-physical DC testbed

card which is used to extract the sensor measurements and manage the actuator inputs as voltages, and feed them to the distributed I/O modules.

The simulation sampling time for the DC plant simulator in MATLAB/Simulink is set to 3.6 s and the PLC monitors and updates the sensors and actuators every 3.6 s. The control firmware has been implemented in the PLC using an interrupt routine which is set to time-out every 3.6 s to service the feedback control loops in order to fulfill the control objective.

13.4 Attack Modeling

Industrial control systems (ICS) for any physical plant consist of a number of control loops that are responsible for controlling various parameters related to the plant. Each control loop fundamentally contains a controller, sensors, and actuators. Our study assumes that the attacker has managed to sneak through the IT security infrastructure to the control systems operating the plant and is capable of launching attacks on these systems, i.e., sensors and actuators. This is the worst attack scenario possible on the ICS. Figure 13.4 presents a diagram of a networked CPS under attack that has been considered as part of this study.

For any arbitrary attack of time period T_{ai}, let $\psi_i(t)$ and $\hat{\psi}_i(t)$ correspond to the healthy and corrupt data due to attack on the ith sensor/actuator ICS resource. In this case, the attack models can be expressed as follows:

1. **Scaling attack** (Sridhar and Govindarasu 2014): A scaling function is used to generate a false data injection attack whereby the channel data during attack is scaled by a constant factor as expressed below

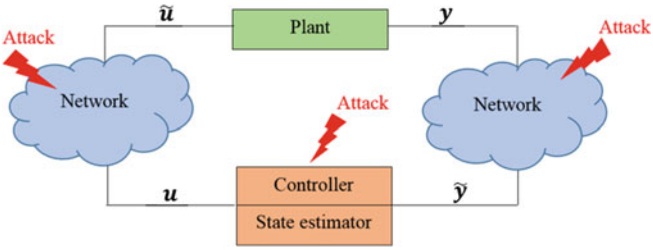

Fig. 13.4 Block level illustration of ICS of Cyber-Physical System under attack, ©2020 IEEE. Reprinted, with permission, from Sabbir Ahmad and Meskin (2020)

$$\hat{\psi}_i(t) = \begin{cases} \psi_i(t), & t \notin T_{ai} \\ \lambda_s \psi_i(t), & t \in T_{ai} \end{cases}, \tag{13.12}$$

where $\lambda_s \in \mathbb{R}$ is a constant.

2. **Bias Injection attack:** In this attack, the true sensor/actuator measurements are modified by adding a constant bias denoted by λ_b, as follows:

$$\hat{\psi}_i(t) = \begin{cases} \psi_i(t), & t \notin T_{ai} \\ \psi_i(t) + \lambda_b, & t \in T_{ai} \end{cases}, \tag{13.13}$$

where $\lambda_b \in \mathbb{R}$ is a constant.

3. **Ramp attack** (Sridhar and Govindarasu 2014): As part of this attack, the true sensor/actuator readings of the targeted resource are modified by adding a ramp function which gradually increases/decreases with time based on the gradient of ramp denoted by λ_r as follows:

$$\hat{\psi}_i(t) = \begin{cases} \psi_i(t), & t \notin T_{ai} \\ \psi_i(t) + \lambda_r t, & t \in T_{ai} \end{cases}. \tag{13.14}$$

4. **Replay attack** (Mo et al. 2015): The replay attack has two stages. At first, the adversary gathers sensor/actuator readings by disclosing the data from the targeted ICS resources. Subsequently, the attacker replays this collected data to the targeted ICS resources.
Stage 1 ($0 \leq t < T_I$): disclosure of resource

$$I_t = I_{t-1} \cup \begin{bmatrix} \gamma_u & 0 \\ 0 & \gamma_y \end{bmatrix} \begin{bmatrix} u(t) \\ y(t) \end{bmatrix}, \tag{13.15}$$

where γ_u and γ_y are the binary incidence matrices mapping the actuator and sensor data channels to the corresponding data gathered by the adversary, T_I is the length of gathering information for the replay attack, and the collected data is stored in I_k.
Stage 2 ($T_I \leq t < 2T_I$): disruption of resource

$$\begin{bmatrix} \boldsymbol{u}(t) \\ \boldsymbol{y}(t) \end{bmatrix} = I_{t-n}. \tag{13.16}$$

5. **DoS attack:** The DoS attack can be launched by jamming the communication channels, flooding packets in the network, and compromising devices to prevent data transfer, etc. As the lack of available sensor/actuator data, the DoS attack can be modeled as follows:

$$\hat{\psi}_i(t) = \begin{cases} \psi_i(t) & t \notin T_{ai} \\ (1 - D_{\mathrm{s}}(t))\psi_i(t) + D_{\mathrm{s}}(t)\psi_i(t - t_n) & t \in T_{ai}, \end{cases} \tag{13.17}$$

   where $D_{\mathrm{s}}(t)$ is a binary index and takes a value of 1 to resemble a scenario when a packet is denied and 0 for the normal operation. To encompass energy limitations, it is assumed that, within the attack time horizon T_{ai}, the targeted resource can send at most M data packets, while the attacker can launch DoS attack at most N times where $N < M$. In (13.17), t_n is the number of consecutive packets which are jammed by the attacker and hence can take values from $k_n = \{1, 2, 3, \ldots, N\}$. The attack model sends the last available packet during the DoS attack. DoS attack is able to make the data channels unavailable by jamming the disruption resources.
6. **Bounded random attack** (Manandhar et al. 2014; Sridhar and Govindarasu 2014): This attack involves the addition of randomly generated attack values to the sensor/actuator signal as follows:

$$\hat{\psi}_i(t) = \begin{cases} \psi_i(t) & t \notin T_{ai} \\ \psi_i(t) + \; N(0, \sigma^2) & t \in T_{ai} \; and \; |\sigma| < \rho, \end{cases} \tag{13.18}$$

   where $\rho \in \mathbb{R}$.

It should be noted that the above-presented attack models are applicable for targeting both sensors and actuators.

13.5 Attack Detection Algorithm

13.5.1 UKF Based Attack Detection

The proposed detection method is based on state estimation which is implemented using UKF. A UKF is a state estimation algorithm that estimates the system states based on the system measurements and control inputs in the presence of Gaussian process and measurement noise. The proposed detection scheme is based on the idea of comparing the system measurements against the estimates from UKF and computing the residuals for every measurement upon which a threshold is applied to detect cyber-intrusions.

The proposed column has two control inputs and output measurements which are the reflux flow rate (kmole/hr) and vapor flow rate (kmole/hr), and distillate purity and bottoms impurity concentrations, respectively. Each tray has four associated states which are the molar holdup in the tray, molar concentration of distillate, liquid and vapor flow rate for that particular tray. Additionally, the condenser and reboiler each have two states which are the molar holdup and molar concentration of the distillate and bottoms product. As there are 14 trays besides the condenser and reboiler, hence in total there are 60 states. The system 13.7 is decomposed by separating the rectifying and stripping section dynamics of the column. Hence, the rectifying section dynamics is given as follows:

$$\begin{aligned} \dot{\boldsymbol{x}}_r(t) &= \boldsymbol{f}_\mathbf{1}(x_r(t), x_s(t), u(t)) + \boldsymbol{w}_r(t) \\ y_r(t) &= x_1(t) + v_r(t) \end{aligned} \tag{13.19}$$

and the dynamics of the stripping section is given as follows:

$$\begin{aligned} \dot{\boldsymbol{x}}_s(t) &= \boldsymbol{f}_2(x_s(t), x_r(t), u(t)) + \boldsymbol{w}_s(t) \\ y_s(t) &= x_{16}(t) + v_s(t), \end{aligned} \tag{13.20}$$

where

$$\begin{aligned} \boldsymbol{x}_r(t) = [&x_1(t), x_2(t), \ldots, x_8(t), M_1(t), M_2(t), \ldots, M_8(t), \\ &L_2(t), L_3(t), \ldots, L_8(t), V_2(t), V_3(t), \ldots, V_8(t)]^T \\ \boldsymbol{x}_s(t) = [&x_9(t), x_{10}(t), \ldots, x_{16}(t), M_9(t), M_{10}(t), \ldots, M_{16}(t), \\ &L_9(t), L_{10}(t), \ldots, L_{15}(t), V_9(t), V_{10}(t), \ldots, V_{15}(t)]^T, \end{aligned}$$

$x_r(t)$ and $x_s(t)$, and $y_r(t)$ and $y_s(t)$ correspond to the states and outputs, for the rectifying and stripping section, respectively. The continuous states of the rectifying and stripping section include the liquid molar concentration of the lighter components in every tray along with the liquid and vapor flow rate dynamics for every tray inside each section. $f_1(\cdot)$ an $f_2(\cdot)$ represent the vector fields describing the state dynamics for the rectifying and stripping section, respectively, $x_i(t)$, $M_i(t)$, $L_i(t)$ and $V_i(t)$ denote the molar concentration, molar holdup, liquid and vapor flow rate for the ith tray in the column, and $w_r(t)$, $w_s(t)$, $v_r(t)$, and $v_s(t)$ represent the Gaussian white process and measurement noise, for the rectifying and stripping section, respectively.

The distributed scheme is implemented using two UKF, one for the rectifying section and one for the stripping section on their respective control PLC which interact with each other for estimating the overall system states. Based on the estimated state, each PLC computes residuals for its sensor measurements for each of which a threshold is applied for attack detection. Figure 13.5 shows a block diagram of the proposed detection scheme.

As the given model is continuous-time hence Eulers discretization is applied to derive the discrete-time model of the rectifying and stripping section of the column.

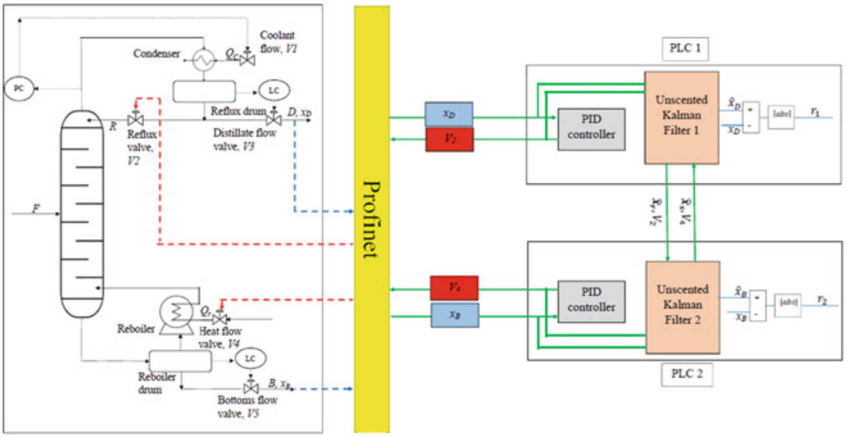

Fig. 13.5 Block level illustration of the detection scheme

The two main steps for implementing UKF for a discrete-time system are given below.

Prediction step:

$$
\begin{aligned}
\boldsymbol{X}^a_{k-1} &= \hat{\boldsymbol{x}}^a_{k-1} \pm \sqrt{(\Delta + \lambda) P^a_{k-1}} \\
\boldsymbol{X}^x_{k|k-1} &= f(\boldsymbol{X}^x_{k-1}, \boldsymbol{X}^w_{k-1}) \\
\hat{\boldsymbol{x}}_{k|k-1} &= \sum_{i=0}^{2\Delta} W_i^{(m)} \boldsymbol{X}^x_{i,k|k-1} \\
P_{k|k-1} &= \sum_{i=0}^{2\Delta} W_i^{(c)} [\boldsymbol{X}^x_{i,k|k-1} - \hat{\boldsymbol{x}}_{k|k-1}][\boldsymbol{X}^x_{i,k|k-1} - \hat{\boldsymbol{x}}_{k|k-1}]^T .
\end{aligned}
$$

Update step:

$$
\begin{aligned}
\boldsymbol{Y}_{k|k-1} &= h(\boldsymbol{X}^x_{k|k-1}, \boldsymbol{X}^v_{k-1}) \\
\hat{\boldsymbol{y}}_k &= \sum_{i=0}^{2\Delta} W_i^{(m)} \boldsymbol{Y}_{i,k|k-1} \\
P_{\tilde{\boldsymbol{y}}_k, \tilde{\boldsymbol{y}}_{k-1}} &= \sum_{i=0}^{2\Delta} W_i^{(c)} [\boldsymbol{Y}_{i,k|k-1} - \hat{\boldsymbol{y}}_k][\boldsymbol{Y}_{i,k|k-1} - \hat{\boldsymbol{y}}_k]^T \\
P_{\boldsymbol{x}_k, \boldsymbol{y}_k} &= \sum_{i=0}^{2\Delta} W_i^{(c)} [\boldsymbol{X}^x_{i,k|k-1} - \hat{\boldsymbol{x}}_{k|k-1}][\boldsymbol{Y}_{i,k|k-1} - \hat{\boldsymbol{y}}_k]^T \\
K &= P_{\boldsymbol{x}_k, \boldsymbol{y}_k} P^{-1}_{\tilde{\boldsymbol{y}}_k, \tilde{\boldsymbol{y}}_k}
\end{aligned}
$$

$$\begin{aligned}\hat{\boldsymbol{x}}_k &= \hat{\boldsymbol{x}}_{k|k-1} + K(\boldsymbol{y}_k - \hat{\boldsymbol{y}}_k)\\ P_k &= P_{k|k-1} - K P_{\tilde{\boldsymbol{y}}_k,\tilde{\boldsymbol{y}}_k} K^T,\end{aligned}$$

where $\boldsymbol{x}^a = [\boldsymbol{x}^T \ \ \boldsymbol{w}^T \ \ \boldsymbol{v}^T]^T$, $\boldsymbol{X}^a = [(\boldsymbol{X}^x)^T \ \ (\boldsymbol{X}^w)^T \ \ (\boldsymbol{X}^v)^T]^T$, $W_0^{(m)} = \lambda/(\Delta + \lambda)$, $W_i^{(m)} = W_i^{(c)} = 1/\{2(\Delta + \lambda)\}, i = 1, \ldots, 2\Delta, \lambda = \alpha^2(\Delta + K) - \Delta$ is the composite scaling parameter, Δ is the dimension of augmented state, $\hat{\boldsymbol{x}}_k$ is the mean state estimate, $\hat{\boldsymbol{y}}_k$ is the mean output estimate, P_k is the covariance matrix, $\boldsymbol{X}_i, i = 1, \ldots, 2\Delta$, are the sigma points, $P_k^a = \text{diag}(P_k, P_w, P_a)$, and P_w, P_v are the covariance of process and measurement noise, respectively. The parameter α determines the spread of the sigma points around $\hat{\boldsymbol{x}}_k$ and is usually set to a positive value (between 0 and 1) and K is a secondary scaling parameter which is usually set to 0.

The residuals which are used for detection are defined as follows:

$$r_1 = \left| x_D - \hat{x}_D \right| \tag{13.21}$$

$$r_2 = \left| x_B - \hat{x}_B \right|, \tag{13.22}$$

where x_D, x_B, $\hat{x}_D$, and $\hat{x}_B$ correspond to the distillate purity and bottoms impurity measurement (i.e., x_1, x_{16}), and estimated distillate purity and bottoms impurity (i.e., $\hat{x}_1, \hat{x}_{16}$), respectively, and r_1 and r_2 denote the residual in distillate purity estimation and bottoms impurity estimation, respectively. The value of the residuals is chosen based on the specification of the measured parameters, i.e., product purity requirement with the aim of detecting the attack as early as possible to limit the potential damage on the product qualities due to an attack without triggering false alarms.

13.5.2 Detector Design

Fundamentally, the detection algorithm is implemented using moving window-based monitoring, whereby at each time-instant the window is shifted by one sample. The time-instant is set as the same as the update frequency of the UKF filter (T_s) as 3.6 s. The window length is defined as the number of samples corresponding to a residual that has to be monitored. The window length for this study has been set to ten samples, i.e., 36 s. The length of the window is set as such to reduce the number of false alarms without missing any true positive attack events. A Boolean flag is allocated to each residual at every time-instant indicating the outcome from comparing the residual against a predefined threshold. If the residual exceeds the threshold the flag is set to False and vice versa. In the proposed window-based monitoring, at every time-instant a decision status is assigned to each residual based on the evaluation of the flags in the window. The decision status is binary, and can be either "Healthy (0)" or "Abnormal (1)" which is determined based on the percentage of the flag in each window with given value. In our study, the status is set as Abnormal (1) if 60% of the flags inside the window are set as False. The detection algorithm is implemented inside the PLC as shown in Fig. 13.5.

13.6 Results

This section presents the results of the various attack cases that are used to validate the proposed detection scheme. For all attack cases, the threshold for the residuals defined in (13.21) and (13.22) is set to 0.02 and 0.01, respectively.

13.6.1 Attack on Distillate Purity Measurement

During this attack, the distillate purity is scaled up by 5% with the aim of violating the product quality specification of the distillate. The result for this attack is presented in Fig. 13.6. The attack is detected within 36 s by the residual corresponding to the distillate purity. This is achieved as the UKF is able to estimate the distillate purity correctly in the event of the attack as illustrated in the figure. Besides that the presented results confirm that the scheme successfully detects the attack before the product quality specification is violated.

13.6.2 Attack on Bottoms Impurity Measurement

In this case, the bottoms impurity measurement is targeted using a ramp attack with $\lambda_{\mathrm{r}} = 1.8 \times 10^{-6}$. Figure 13.7 presents the results corresponding to this attack and as can be seen, the attack is successfully detected in 36 s by r_2 before the bottoms impurity requirement could be violated. Principally, in the event of a sensor attack, a discrepancy arises between the estimator output estimate and the actual measurement as illustrated in Fig. 13.7 that facilitates the attack detection. Additionally, the difference between the estimated and actual bottoms impurity during the normal operation is due to the fact that the actual measurements contain noise which is filtered out by the UKF.

13.6.3 Attack on Reflux Flow Rate

The attack is injected by scaling the actual reflux rate down by 20%. In the event of an actuator attack, as both the correct sensor and actuator data is available to the control PLC, hence it is able to detect the attack by monitoring the system measurements which changes abnormally due to the attack as illustrated in Fig. 13.8. From these

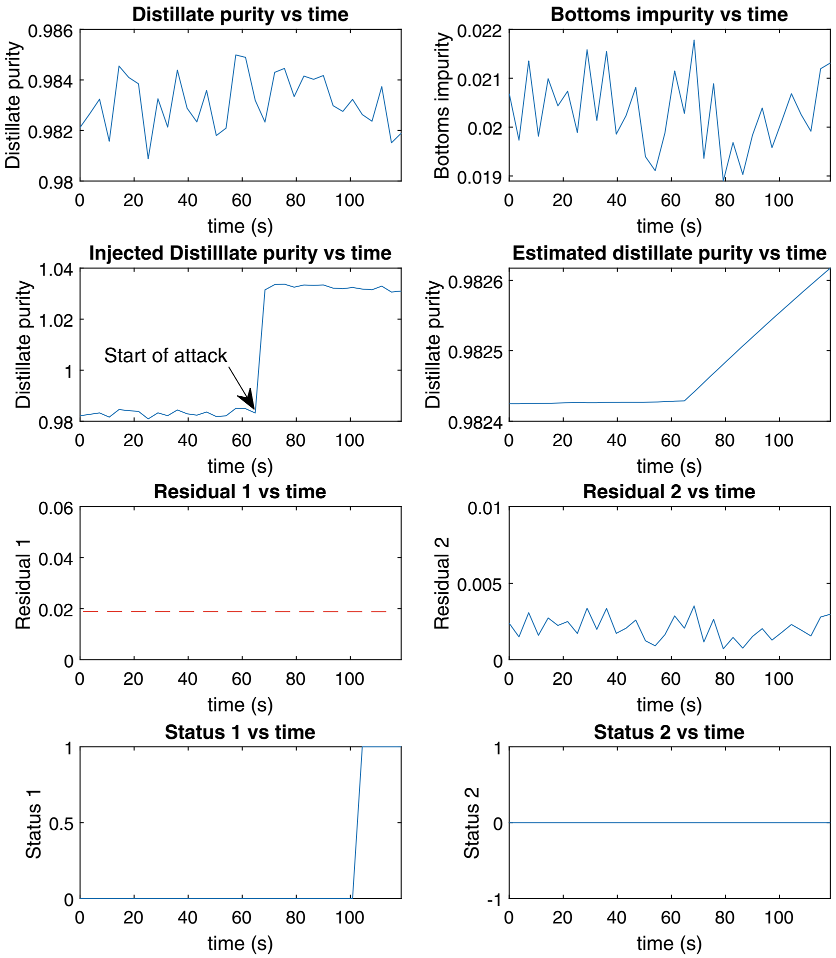

Fig. 13.6 Results illustrating the effect of attack on the distillate purity measurement

results, it can be seen that the attack is successfully detected by both residuals; however, r_1 detected the attack earlier in 1.5 h. As a result of this attack, the distillate product quality requirement is violated.

13.6.4 Attack Case Summary

Besides the presented cases, Table 13.5 summarizes the results for various other attack cases considered as part of this study. The main noticeable observation is the difference between the sensor and actuator attacks detection times where the

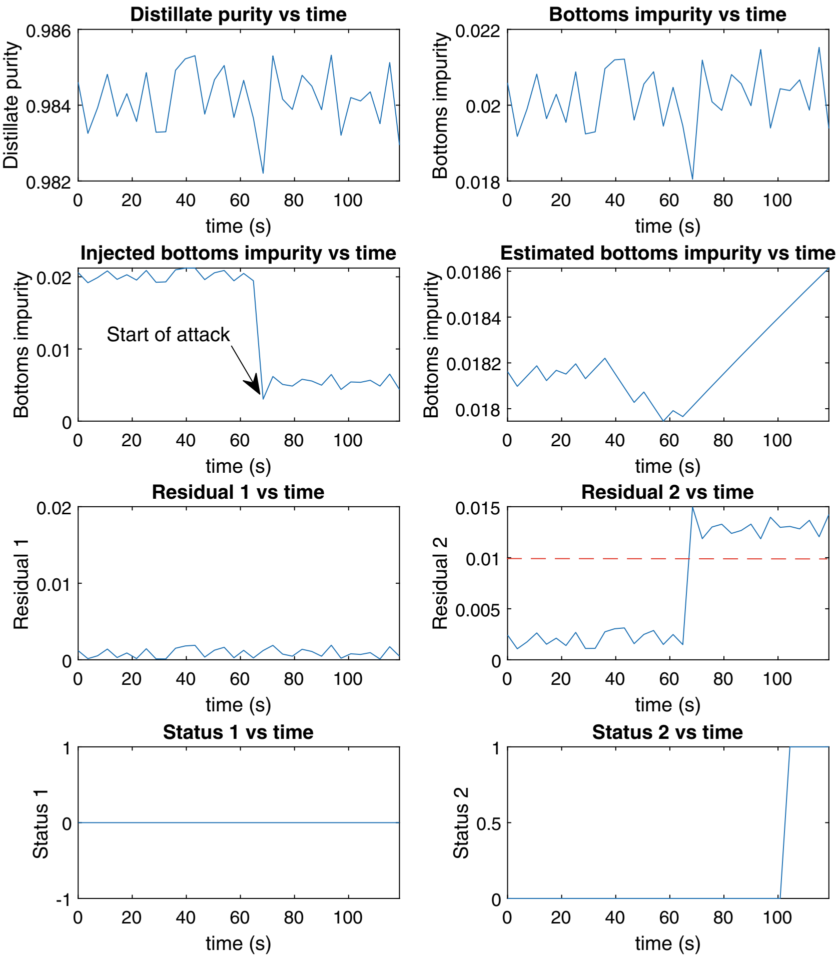

Fig. 13.7 Results illustrating the effect of attack on the bottoms impurity measurement

actuator attacks take longer to be detected. This is due to the fact that the sensor attack directly manipulates a variable of the residual functions, whereas in the case of actuator attacks, the attack is detected using the change in the product quality which takes longer to be appear as the system is relatively slow.

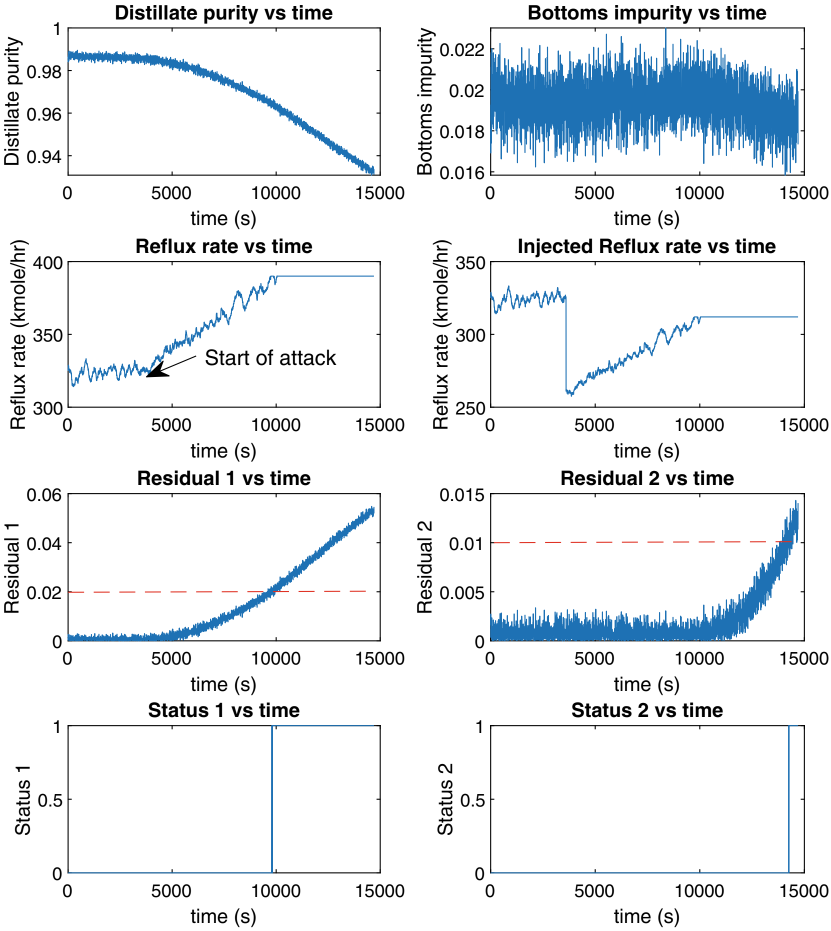

Fig. 13.8 Results illustrating the effect of attack on the reflux flow rate

13.7 Conclusion and Future Work

This chapter addresses the cyber-security of a cyber-physical DC plant by proposing an attack detection technique. A dynamical model of the DC plant is developed which allows for performing simulation study without the necessity of having a physical column. Following that, a hybrid HIL ICS testbed is proposed for the DC plant implemented using industrial hardware from Siemens. A PLC-based online distributed detection scheme is developed based on state estimation using Unscented Kalman Filter and successfully validated for various attack scenarios formulated using the presented attack models. In the proposed model, it is assumed that the column pressure at the top remains constant which is not the case in reality. A feedback control loop is generally used to maintain constant column pressure by

Table 13.5 Summary of detection results for various sensor and actuator attacks

Attack type	Attack name	Targeted resource	Detection time (s)
Sensor attack	Bias injection	Distillate purity	36
		Bottoms impurity	36
	DoS attack	Distillate purity	48
		Bottoms impurity	68
Actuator attack	Replay attack	Reflux rate	4320
		Vapor flow rate	3885
	Constant value attack	Reflux rate	3655
		Vapor flow rate	5139
	Random attack	Reflux rate	4481
		Vapor flow rate	3593

adjusting the condenser duty cycle. Thus, the existing model can be extended by incorporating the column pressure dynamics and an additional feedback control loop can be added to enhance the practicality of the study. As part of this study, a continuous binary DC is considered while there exist other types of columns that are found in industry, e.g., batch distillation column, multi-component distillation column. Hence, further studies can be done to tackle cyber-security for the other distillation column configurations. Furthermore, distillation column is a part of crude processing and there exist various chemical and physical processes both upstream and downstream that is used to convert the raw crude into commercial product. These processes can be included in the future study to make it industrially more feasible.

Acknowledgements This publication was made possible by the Graduate Sponsorship Research Award (GSRA) award (GSRA4-2- 0518-17083) from the Qatar National Research Fund (QNRF), a member of the Qatar Foundation. The authors would also like to acknowledge the financial support received from NATO under the Emerging Security Challenges Division program.

References

A.A. Abokifa, K. Haddad, C. Lo, P. Biswas, Real-time identification of cyber-physical attacks on water distribution systems via machine learning-based anomaly detection techniques. J. Water Resour. Plan. Manag. **145**(1), 04018089 (2019)

S. Adepu, A. Mathur, Distributed attack detection in a water treatment plant: method and case study. IEEE Trans. Dependable Secure Comput. **18**(1), 86–99 (2021)

S.H.M. Ahmad, N. Meskin, Cyber attack detection for a nonlinear binary crude oil distillation column, in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (2020), pp. 212–218

A. AlDairi, L. Tawalbeh, Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput. Sci. **109**, 1086–1091 (2017). 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16–19 May 2017, Madeira, Portugal

R. Bendib, H. Bentarzi, Y. Zennir, Investigation of the effect of design aspects on dynamic control of a binary distillation column, in *2015 4th International Conference on Electrical Engineering (ICEE)* (2015), pp. 1–5

M. Elnour, N. Meskin, R. Jain, A dual-isolation-forests-based attack detection framework for industrial control systems. IEEE Access 1 (2020)

M. Elnour, N. Meskin, R. Jain, Application of data-driven attack detection framework for secure operation in smart buildings. Sustain. Cities Soc. **69**, 102816 (2021)

A. George, R.M. Francis, Model reference adaptive control of binary distillation column composition using MIT adaptive mechanism. Int. J. Eng. Res. Technol. **4** (2015)

Y. He, G.J. Mendis, J. Wei, Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid **8**(5), 2505–2516 (2017)

P. Kathel, A.K. Jana, Dynamic simulation and nonlinear control of a rigorous batch reactive distillation. ISA Trans. **49**(1), 130–137 (2010)

M. Kravchik, A. Shabtai, Anomaly detection; industrial control systems; convolutional neural networks. CoRR (2018), arXiv:abs/1806.08110

D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, K. Butler-Purry, Towards modelling the impact of cyber attacks on a smart grid. Int. J. Secur. Netw. **6**, 2–13 (2011)

M.N. Kurt, O. Ogundijo, C. Li, X. Wang, Online cyber-attack detection in smart grid: a reinforcement learning approach. IEEE Trans. Smart Grid **10**(5), 5174–5185 (2019)

D. Li, D. Chen, L. Shi, B. Jin, J. Goh, S. Ng, MAD-GAN: multivariate anomaly detection for time series data with generative adversarial networks. CoRR (2019), arXiv:abs/1901.04997

Q. Lin, S. Adepu, S. Verwer, A. Mathur, Tabor: a graphical model-based approach for anomaly detection in industrial control systems, in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security, ASIACCS '18* (Association for Computing Machinery, New York, NY, USA, 2018), pp. 525–536

M. Lv, W. Yu, Y. Lv, J. Cao, W. Huang, An integral sliding mode observer for cps cyber security attack detection. Chaos: Interdiscip. J. Nonlinear Sci. **29**, 043120 (2019)

K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. **1**(4), 370–379 (2014)

T. Meraj, S. Sharmin, A. Mahmud, Studying the impacts of cyber-attack on smart grid, in *2015 2nd International Conference on Electrical Information and Communication Technologies (EICT)* (2015), pp. 461–466

V.T. Minh, J. Pumwa, Modeling and adaptive control simulation for a distillation column, in *2012 UKSim 14th International Conference on Computer Modelling and Simulation* (2012a), pp. 61–65

V. Minh, J. Pumwa, Modeling and control simulation for a condensate distillation column (2012b)

Y. Mo, S. Weerakkody, B. Sinopoli, Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Syst. Mag. **35**(1), 93–109 (2015)

M. Noorizadeh, M. Shakerpour, N. Meskin, D. Unal, K. Khorasani, A cyber-security methodology for a cyber-physical industrial control system testbed. IEEE Access **9**, 16 239–16 253 (2021)

A. Nourian, S. Madnick, A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. IEEE Trans. Dependable Secure Comput. **15**(1), 2–13 (2018)

F. Pasqualetti, F. Dorfler, F. Bullo, Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control **58**, 2715–2729 (2012)

F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. IEEE Control Syst. Mag. **35**(1), 110–127 (2015). (Feb)

G. Radulescu, N. Paraschiv, A. Kienle, An original approach for the dynamic simulation of a crude oil distillation plant 2: setting-up and testing the simulator. Revista de Chimie **58** (2007)

S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)

S.A. Taqvi, L.D. Tufa, S. Muhadizir, Optimization and dynamics of distillation column using aspen plus$\circ R$. Procedia Eng. **148**, 978–984 (2016). Proceeding of 4th International Conference on Process Engineering and Advanced Materials (ICPEAM 2016)

S.A. Taqvi, L.D. Tufa, H. Zabiri, S. Mahadzir, A.S. Maulud, F. Uddin, Rigorous dynamic modelling and identification of distillation column using aspen plus, in *2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC)* (2017), pp. 262–267

W. Weerachaipichasgul, P. Kittisupakorn, A. Saengchan, K. Konakom, I.M. Mujtaba, Batch distillation control improvement by novel model predictive control. J. Ind. Eng. Chem. **16**(2), 305–313 (2010)

E. Wijn, Weir flow and liquid height on sieve and valve trays. Chem. Eng. J. **73**(3), 191–204 (1999)

T. Zhang, Y. Wang, X. Liang, Z. Zhuang, W. Xu, Cyber attacks in cyber-physical power systems: a case study with GPRS-based SCADA systems, in *2017 29th Chinese Control And Decision Conference (CCDC)* (2017), pp. 6847–6852

Z. Zou, Z. Wang, L. Meng, M. Yu, D. Zhao, N. Guo, Modelling and advanced control of a binary batch distillation pilot plant. Chin. Autom. Congr. (CAC) **2017**, 2836–2841 (2017)