Cybersecurity in Process Control, Operations, and Supply Chain

Sandra Parker [a], Zhe Wu [b] and Panagiotis D. Christofides [c,d,1]

[a] Dow, Inc., Midland, MI 48674

[b] Department of Chemical and Biomolecular Engineering, National University of Singapore, 117585, Singapore

[c] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592

[d] Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592

Abstract

With the integration of computation, networking, and physical process components to seamlessly combine hardware and software resources to improve process efficiency, cybersecurity has become increasingly important for reliable process control, process operation, and supply chain management in the chemical process industries. This paper provides an overview of recent works on cybersecurity issues in the area of process control, process operation and supply chain. We start with an overview of recent cyber-attack detection and mitigation works via machine learning (ML) and model predictive control (MPC) to detect and handle intelligent cyber-attacks. Several most common intelligent cyber-attacks in industrial control systems are first presented, followed by machine learning detection methods and resilient control strategies with encryption-decryption tools to achieve secure communication in the sensor-controller and controller-actuator links. Novel control architectures with inherent robustness to prevent cyber-attacks are then presented. We continue with an overview of cybersecurity issues in process operations and supply chains as well as the interface between information technology and operational technology. Finally, we discuss recent efforts on the interface of cybersecurity and process safety and conclude with a discussion of open issues in this emerging research field.

Keywords

Cybersecurity; Machine Learning; Process Control; Process Operation; Process Safety; Supply Chain Management.

Introduction

Over the last two decades, internet communication and wireless networks have been starting to replace or complement existing wired point-to-point communications in traditionally large-scale process operations (e.g., Christofides et al. (2007)). As these new developments bring improved efficiency to the existing system, the heightened concern for unestablished, industrial cybersecurity at all levels has also been rising following cyber-attacks that disrupt standard operations. Due to the connectivity and interaction between the cyber and physical components in chemical processes, operational cybersecurity requires a different strategy from the traditional information technology (IT) approach. This is a consequence of key differences between IT and OT (operational technology): a) OT employs purpose-built technologies and protocols, b) OT systems are typically kept much longer than IT systems where most companies cannot easily perform upgrades or implement changes to the technology, c) upgrades or changes in the OT space generally require plant shutdowns which are costly, and as a result, may lead to equipment running for years, making it difficult for its support, and d) OT is very much concerned with reliability and intellectual property. Despite these differences that raise challenges in implementing cybersecurity solutions in the OT space, recent cyber-attacks have driven the need for developing and implementing novel cybersecurity solutions in the OT space. Most companies and organizations recognize today the need to deploy a combination of traditional IT cybersecurity products and services with tailored operational technology (OT)-specific cybersecurity solutions. The failure to ensure cybersecurity in OT can lead to unsafe and potentially catastrophic consequences in a chemical process operation, causing critical asset damage and human injuries. During the past two decades with the facilitation of technology and processes, the industry has exposed the vulnerabilities of unestablished cybersecurity systems following the rise of cyber-attacks. From 2000 to 2019, a reported 77 cybersecurity-related incidents were uncovered in critical infrastructure in-

[1] Corresponding author. Email: pdc@seas.ucla.edu.

cluding the process industry with a vast majority of attacks on energy and oil production industries (Iaiani et al., 2021). The lack of adequate prevention of cyber-attacks endangers the balance of the economy, environment, and society. For instance, in 2021, the oil pipeline system in the United States, Colonial Pipeline, endured a cyber-attack, which stalled the transportation of oil to much of the eastern United States, causing skyrocketing gas prices (Tsvetanov and Slaria, 2021) and volatile supplies of fuel. In 2015, Ukraine encountered the BlackEnergy malware attack that forced over 200,000 people without power and electricity (Böröcz et al., 2021). The aforementioned examples of cyber-attacks are stark reminders of the repercussions of cyber-attacks and their impact on societal welfare, which are reasons for a greater need for well-established cybersecurity systems. Therefore, the design and implementation of cyber-defense in OT domain that involves industrial control, operation, and supply chain management systems remain an ongoing systems and control engineering research issue of great practical importance.

Chemical and manufacturing industries have adopted firewall isolation, multi-factor authentication, and developed cyber protection protocols over the past decade to improve cybersecurity, particularly in the context of IT tasks. However, with the integration of IT and OT in the framework of Industry 4.0 and the development of intelligent, targeted cyber-attacks that have access to the technical details of the control system and production processes in the plant that aim to modify the operator and control system actions applied to a chemical process, the need for OT task cybersecurity has grown significantly. Earlier efforts to enhance the cybersecurity of the OT space started around 2010 but gained momentum around 2017 by taking advantage of industrial process operation and automation groups. Today, OT cybersecurity is viewed as a key concern across the entire chemical sector and aims to establish cybersecurity standards and raise the level of protection across chemical plants. In particular, to enhance cybersecurity and physical security of process operations, the fundamental cybersecurity research roadmap (a framework, whose key components are summarized in Fig. 1) proposed originally by National Institute of Standards and Technology (2018) (NIST) that has influenced the efforts of many companies including Dow, has proposed a five-step plan to detect and mitigate the impact of cyber-attacks with recovery plans: identify, detect, protect, respond, and recover. However, within this five-step framework, there are many key research questions that need to be considered. Specifically, despite a series of recent efforts over the past five years, designing efficient detection methods and suitably optimal, yet secure, operation control and supply chain strategies for chemical processes in the presence of intelligent cyber-attacks remains an important, fundamental research issue. Furthermore, while the development of most of the existing cyber-attack detection methods still depends partly on human analysis, the increased use of data and the design of stealthy cyber-attacks pose challenges to the development of timely detection methods with high detection accuracy. In the following paragraph, we provide an overview of results on the development of machine learning-based cyber-attack detection schemes as this is a topic central to cybersecurity approaches in the OT space, and it is covered in greater detail later on in the manuscript (please see ”Machine Learning-Based Cyber-Attack Detection” section).

Machine learning, a method of data analysis that can help engineers learn from data, identify patterns, and make decisions with minimal human intervention, has attracted increasing attention and has shown promising potential for use in the detection of cyber-attacks. Over the last decade, machine learning has been widely used in solving classification, regression, and clustering problems due to the rapid development of machine learning algorithms, computing resources/platforms, and many free and open-source software libraries. To detect cyber-attacks, machine learning methods can be utilized to solve classification problems to determine the existence of cyber-attacks in the chemical plant and its control systems using an abundance of industrial process data that is generated by machines and devices under normal operations and under cyber-attacks. Machine-learning methods deployed for cyber-attack detection were presented in a number of works (Tsai et al., 2009; Buczak and Guven, 2015; Ozay et al., 2015). Using various machine-learning classification methods, cyber-attacks on power systems were distinguished from process disturbances in Hink et al. (2014), and a behavior-based intrusion detection algorithm was developed to identify the type of attack (Junejo and Goh, 2016). Similarly, the detection of cyber-attacks in a chemical process was realized via the development of feedforward artificial neural networks in Wu et al. (2018), where compromised signals were rerouted to a secure sensor upon detection. In Shon and Moon (2007), a hybrid approach using support vector machines and genetic algorithms was implemented and compared to existing network intrusion detection systems in industry. An overview of recent research directions for applying supervised and unsupervised machine learning techniques to address the problem of anomaly detection was presented in Omar et al. (2013). Among many machine learning methods, neural network and many of its variances have demonstrated remarkable performance. For instance, a Long Short-Term Memory (LSTM) recurrent neural network (RNN) was used to build a classifier model for the intrusion detection system in Kim et al. (2016). The anomaly detection algorithm outlined in Goh et al. (2017) also used a LSTM network as a predictor to model normal behavior of a water treatment testbed and used the Cumulative Sum (CUSUM) method to identify anomalies. A multi-layer data-driven cyber-attack detection system was proposed in Zhang et al. (2019) where four classification methods including k-nearest-neighbor, decision tree, bootstrap aggregating, and random forest, were used to detect cyber-attacks including man-in-the-middle, denial-of-service, data exfiltration, data tampering, and false data injection attacks based on network and host system data. Many variants of convolutional neural networks with different topologies, parameters, and structures were analyzed for the task of intrusion detection in cybersecurity of network traffic in Vinayakumar et al. (2017), which have shown significant improvement over conventional classifiers. These recent literature contributions have demonstrated the feasibility of machine-learning algorithms in anomaly detection including anomalies caused by cyber-attacks. At any large-scale chemical production plant, a tremendous amount of data is being collected and archived daily in the historian. Using neural-network algorithms, the data can be utilized to train effective detection devices for monitoring and guarding the plant against malicious cyber-attacks.

Besides the detection of cyber-attacks, efforts are made to improve cyber and physical security through a variety of fundamental operation and control methods that address the following aspects: security by design, advanced recovery, advanced threat detection, secure remote access, and combined safety (Fig. 1). This work will discuss recent works within the elements of Fig. 1 in context of cybersecurity of process control and operation systems and supply chains. Specifically, to guarantee the process performance and to mitigate the impact of cyber-attacks, process control systems, e.g., model predictive control (MPC) and economic MPC (EMPC), utilizing encrypted signals may be employed to operate the process with secure remote access in the presence of cyber-attacks. With regard to security by design and advanced recovery, a cyber-secure two-tier control architecture can be developed and integrated with ML-based detectors to enhance process cybersecurity by reconfiguring the control system to stabilize the process at the original steady state upon the detection of a cyber-attack. Additionally, to account for the interactions among control, cybersecurity, and safety systems, the integration of attack detection and control policies as well as combined control and safety systems have been pursued and will be discussed. Finally, directions for future research in the context of cybersecurity of process control, process operation systems, and supply chains will be discussed.

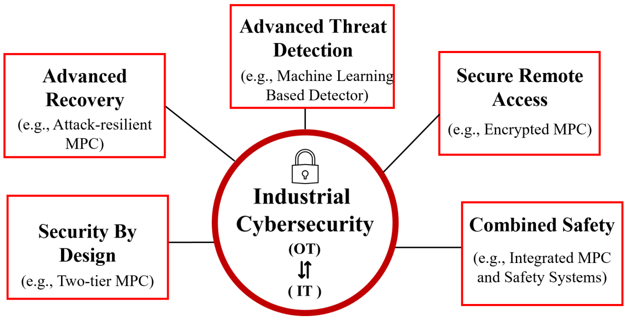


Figure 1: The focus areas of operational technology cybersecurity.

Class of Nonlinear Process Systems

To describe mathematically the various types of cyber-attacks as well as detection and mitigation control methods, we need to introduce a suitable notation, a class of process systems, and specific stabilizability assumptions. Specifically, we consider the class of continuous-time nonlinear systems represented by the following state-space model:

$$\dot{x} = F(x,u,w) := f(x) + g(x)u + h(x)w,\ x(t_0) = x_0 \qquad (1)$$

where the n-dimensional state vector is denoted by $x \in \mathbf{R}^n$ and $u \in \mathbf{R}^k$ denotes the k-dimensional manipulated input vector bounded by $u \in U$. The set U defines the maximum value $u_{\max}$ and the minimum value $u_{\min}$ for input vectors, i.e., $U := \{u_{\min} \leq u \leq u_{\max}\} \subset \mathbf{R}^k$. $w \in W$ is the disturbance vector, where $W := \{w \in \mathbf{R}^q \mid |w| \leq \theta,\ \theta \geq 0\}$. $f(\cdot)$, $g(\cdot)$, and $h(\cdot)$ are sufficiently smooth vector and matrix functions of dimensions $n \times 1$, $n \times k$, and $n \times q$, respectively. We assume that $f(0) = 0$ without loss of generality, and therefore, the origin is a steady-state of Eq. 1. Additionally, we assume there exists a feedback controller that can stabilize the system at the origin. Specifically, we assume there exists a continuously differentiable Lyapunov function $V(x)$ and a Lyapunov-based controller $u = \Phi(x) \in U$ such that the origin of the nominal system ($w(t) \equiv 0$) is rendered asymptotically stable for the states in an open neighborhood D around the origin. The stability region $\Omega_\rho := \{x \in D \mid V(x) \leq \rho\}$, $\rho > 0$ is characterized as a level set of V within D. Throughout this manuscript, $|\cdot|$ is used to denote the Euclidean norm of a vector. Set subtraction is denoted by "$\backslash$", i.e., $A \backslash B := \{x \in \mathbf{R}^n \mid x \in A, x \notin B\}$.

Background and Description of Cyber-Attacks

From the perspective of process control systems as well as process operation and supply chains, cyber-attacks are malicious signals that can compromise actuators, sensors, communication channels between devices, and the operation and control system algorithms. With respect to control system cybersecurity, cyber-attacks modify the control implementation using process and control system information in an attempt to disrupt closed-loop performances. A comprehensive review in Ashibani and Mahmoud (2017) includes an analysis on security issues, requirements, and possible solutions at various layers of the OT architecture. A review of possible weaknesses in corporate networks and in production environments is presented in Asghar et al. (2019). In Amin et al. (2012), a hierarchical attack on automated canal systems was described with various deception attacks in different cyber layers and a field-operational test attack was reported on the Gignac canal system located in Southern France.

Sensor attacks strategically modify the feedback measurements of the attacked states, from which the controller receives and subsequently computes a control action that is different or contrary to its actual optimal value based on the true plant state. Actuator attacks also have access to the plant model and controller design details, which aim to diverge the system away from its ideal operating point. However, instead of altering the sensor measurements, actuator attacks modify the direction and magnitude of the control actions without being detected by sensor monitoring tools. Common detection strategies include designing excitation signals that are superimposed on the control commands to increase the detectability of the attack and developing an input observer to detect attacks as well as estimate the magnitude of the attack (Muniraj and Farhood, 2019). In addition to the detection of actuator attacks, an isolator was developed to identify the affected actuator(s) in the network. As intelligent cyber-attacks are adaptive to the process and control system behavior, we may assume that they are as powerful as having access to the measurement feedback signals (sensor attack), control command signals (actuator attack), or auxiliary information such as the threshold and bias parameters in detection methods such as cumulative sum (CUSUM) (Mohanty et al., 2007; Cárdenas et al., 2011). Being aware of the process and controller behavior, the attacks will therefore have information on the stability region of the process, as well as the existing alarm triggers imposed on the input and output variables. Among sensor cyber-attacks, some common attack types are denial-of-service attacks, replay attacks, and deception attacks – such as min-max, geometric, and surge attacks (Cárdenas et al., 2011). The formulations of the aforementioned three deception and replay attacks are presented below.

1) Min-Max Cyber-attack

Min-max attacks are designed to induce the maximum destabilizing impact within the shortest time without being detected. In order to stay undetectable by classical detection methods such as CUSUM, which detects cyber-attacks by calculating the cumulative sum of the deviation between the expected and measured states based on the process model of Eq. 1, min-max attacks are introduced using the falsified state values furthest from the equilibrium point (minimum or maximum) such that the system does not exit the closed-loop stability region Ω_ρ. In this way, the min-max attacks ensure that the attacked state measurements fed to the control system do not exit the stability region and do not trigger any conventional detection alarms. The min-max attack can be formulated as follows:

$$\bar{x}(t_i) = \min_{x \in \mathbf{R}^\mathbf{n}} / \max_{x \in \mathbf{R}^\mathbf{n}} \{x \mid V(x(t_i)) = \rho\}, \ \ \forall\, i \in [i_0, i_0 + L_a] \quad (2)$$

where ρ defines the level set of the Lyapunov function $V(x)$ that characterizes the stability region Ω_ρ for the system of Eq. 1. $\bar{x}$ is the compromised sensor measurement at each sampling step, i_0 marks the time instant that attack is added, and L_a denotes the time duration of the attack in terms of sampling periods.

2) Replay Cyber-attack

In a replay attack, the attacker first records segments of the system output corresponding to a nominal operating condition where large oscillations occur. The attacker then intercepts and resets the current process state measurements to these pre-recorded values. Replay attacks can be represented by the following equations:

$$\bar{x}(t_i) = x(t_k), \ \forall\, k \in [k_0, k_0 + L_a], \ \ \forall\, i \in [i_0, i_0 + L_a] \quad (3)$$

where $x(t_k)$ is the true plant measurement, L_a represents the length of the attack in terms of sampling periods, and $\bar{x}$ is the series of replay attacks introduced at time t_{i_0} duplicating previous plant measurements that are recorded starting from time t_{k_0}. As previous plant outputs are obtained from legitimate closed-loop measurements and given by secure sensors, these state values are supposedly inside the stability region and the operating envelope. Therefore, by replicating these values and feeding them back to the controller, classical detectors will not be able to recognize the abnormality caused by replay cyber-attacks.

3) Geometric Cyber-attack

Geometric cyber-attacks aim to deteriorate the closed-loop system stability slowly at the beginning, then geometrically increase their impact as time progresses, with their maximum damage achieved at the end of the attack duration. Initially, the attacker adds a small constant β to the true measured output where β is well below the maximum allowable value as defined in a min-max attack. At each subsequent time step, this offset is multiplied by $(1+\alpha)$, where $\alpha \in (0,1)$, until it reaches the maximum allowable attack value. Geometric attacks can be written in the following form:

$$\bar{x}(t_i) = x(t_i) + \beta \times (1+\alpha)^{i-i_0}, \ \ \forall\, i \in [i_0, i_0 + L_a] \quad (4)$$

where $\bar{x}$ is the compromised sensor measurement, β and α are parameters that define the magnitude and speed of the geometric attack.

4) Surge Cyber-attack

Surge attacks act similarly as min-max attacks initially to maximize the disruptive impact for a short period of time; then they are reduced to a lower value by introducing a bounded noise $\eta_l \leq \eta(t_u) \leq \eta_u$ (η_u and η_l are the upper and lower bounds of the noise, respectively) such that the cumulative error between state measurements and their steady-state values will not exceed the threshold defined by some statistic-based detection methods such as CUSUM. The formulation of a surge attack is presented below:

$$\begin{aligned} &\bar{x}(t_i) = \min_{x \in \mathbf{R}^\mathbf{n}} / \max_{x \in \mathbf{R}^\mathbf{n}} \{x \mid V(x(t_i)) = \rho\}, \text{ if } i_0 \leq i \leq i_0 + L_s \\ &\bar{x}(t_i) = x(t_i) + \eta(t_i), \text{ if } i_0 + L_s < i \leq i_0 + L_a \end{aligned} \quad (5)$$

where i_0 is the start time of the attack, L_s is the duration of the initial surge, and L_a is the total duration of the attack in terms of sampling periods. To illustrate the pattern and effect of the four cyber-attack types discussed above, Fig. 2 shows the true concentration values and the cyber-attack-modified sensor values of the concentration when min-max, replay, geometric, and surge attacks target this sensor.

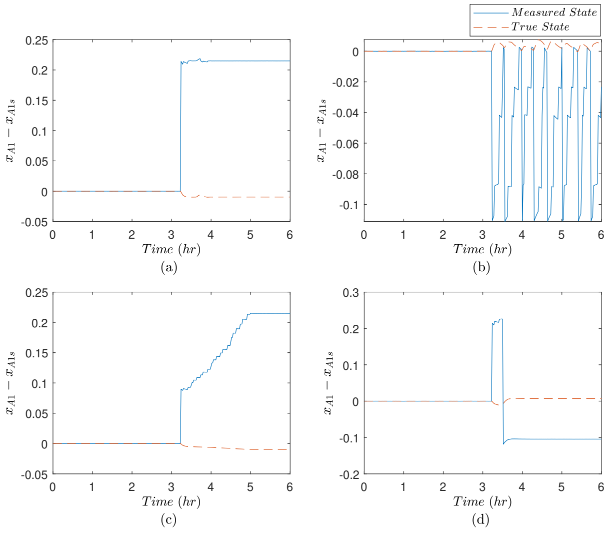


Figure 2: True and measured values of concentration in deviation variable form when (a) min-max, (b) replay, (c) geometric, and (d) surge cyber-attacks are introduced at the sensor.

Machine Learning-Based Cyber-Attack Detection

The first step in the cybersecurity roadmap is to detect and identify cyber-attacks by developing advanced threat detection and protection methods. Cyber-attack detection carried out using data-based approaches, and more specifically, machine-learning methods, have been studied (Huang et al., 2007; Omar et al., 2013; Agrawal and Agrawal, 2015). Machine learning can be utilized to develop detection algorithms based on the time-series data from the dynamic operation of the system of Eq. 1 (Wu et al., 2018). Depending on the training data, the neural networks can be used to distinguish between "attack" and "no attack" (two classes), or to identify the type of attack (multiple classes). While under attack, data collected from individual sensors can also be used to locate the corruption where the neural network model distinguishes between multiple classes with each class representing one problematic sensor. In our study, a feedforward artificial neural network is used for supervised classification. Through a series of nonlinear transformations, each layer in the neural network consists of a series of nonlinear functions of the weighted sum of inputs or neurons (i.e., activation functions), yielding values for the neurons in the subsequent layer from the previous layer.

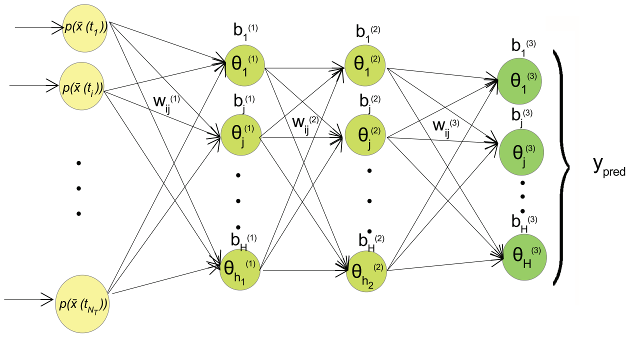


Figure 3: A two-hidden-layer feedforward neural network structure with inputs $p(x)$ being a nonlinear function of state measurements within the detection window N_T, and output being the probability of each class label that indicates the status and/or type of cyber-attack.

The structure of a neural network model with two hidden layers is shown in Fig. 3, with each input unit representing a nonlinear function $p(\cdot)$ of the full state measurements at each sampling time and an output vector representing the probability of each class label. The two-hidden-layer feedforward neural network is mathematically formulated as follows:

$$\theta_j^{(1)} = g_1(\sum_{i=1}^{N_T} w_{ij}^{(1)} p(\bar{x}(t_i)) + b_j^{(1)}) \tag{6a}$$

$$\theta_j^{(2)} = g_2(\sum_{i=1}^{h_1} w_{ij}^{(2)} \theta_i^{(1)} + b_j^{(2)}) \tag{6b}$$

$$\theta_j^{(3)} = g_3(\sum_{i=1}^{h_2} w_{ij}^{(3)} \theta_i^{(2)} + b_j^{(3)}), \;\; y_{pred} = [\theta_1^{(3)}, \theta_2^{(3)}, ..., \theta_H^{(3)}]^T \tag{6c}$$

where $\theta_j^{(l)}$, $j = 1, ..., h_l$, $l = 1,2$ are the neurons in the first ($l = 1$) and second ($l = 2$) hidden layers, respectively. The output node is represented by $\theta_j^{(3)}$, $j = 1, ..., H$, where H is the number of class labels. In general, the number of layers is determined through trial-and-error to achieve the best classification accuracy and computational efficiency. The input node $p(x(t_i))$ receives the state measurement at time t_i, where $i = 1, ..., N_T$ is the length of the time-varying trajectory. $w_{ij}^{(l)}$ and $b_j^{(l)}$ represent the weights connecting neurons i and j in consecutive layers (from $l-1$ to l), and the bias term on the j^{th} neuron in the l^{th} layer, respectively. Based on the information received from the previous layer as well as the optimized biases, weights, and the nonlinear activation function g_l, each layer calculates an output and sends it to the next layer. Examples of the activation functions include the softmax function $g(z_j) = \frac{e^{z_j}}{\sum_{i=1}^{H} e^{z_i}}$, the hyperbolic tangent sigmoid transfer function $g(z) = \frac{2}{1+e^{-2z}} - 1$, and some other common functions such as the sigmoid, radial basis functions, and Rectified Linear Unit (ReLu). The output node y_{pred} computes the probabilities of each class label, from which the class with the highest probability will indicate the status (i.e., no attack or under attack) or the type of cyber-attack that will depend on the requirement of the machine-learning detector.

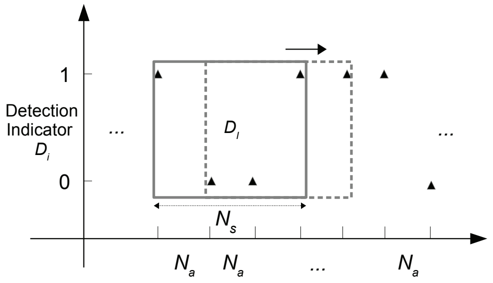


Figure 4: The sliding alarm verification window with detection activated every N_a sampling steps where triangles represent D_i and the window length is N_s.

The classification accuracy of the test dataset is utilized to demonstrate the performance of the neural network since the test dataset is independent of the training dataset and is not used in training the NN model. The classification accuracy (i.e., the test accuracy) of the trained NN model is calculated by the ratio of the number of data samples with correct predicted classes to the total number of data samples in the testing dataset. Additionally, to reduce false alarm rates, a sliding alarm verification window in Fig. 4 is implemented, where the number of positive attack detections $D_i = 1$ within this window needs to surpass a threshold before a cyber-attack alarm is confirmed. The size of this verification window and the threshold value are determined based on the closed-loop evolution of the process as these two parameters have a direct impact on the detection time and alarm rate.

Attack-Resilient MPC Approaches Exploiting Sensor Redundancy

Tracking MPC. Upon the detection of an attack on the sensors providing real-time state measurements to the control system, advanced recovery strategies have been developed to mitigate the impact of attacks. Specifically, one of the most common approaches adopted in industry is to switch to an accurate measurement from redundant, secure sensors. We present the resilient control strategies in the framework of Lyapunov-based MPC that can be represented by the following optimization problem:

$$\mathcal{J} = \min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_t(\tilde{x}(t), u(t))dt \tag{7a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u(t), 0) \tag{7b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{7c}$$

$$u(t) \in U, \ \forall\, t \in [t_k, t_{k+N}) \tag{7d}$$

$$\dot{V}(x(t_k), u(t_k)) \leq \dot{V}(x(t_k), \Phi(x(t_k))), \quad \text{if } V(x(t_k)) > \rho_{min} \tag{7e}$$

$$V(\tilde{x}(t)) \leq \rho_{min}, \ \forall\, t \in [t_k, t_{k+N}), \ \text{if } V(x(t_k)) \leq \rho_{min} \tag{7f}$$

where $\tilde{x}(t)$ is the predicted state trajectory, $S(\Delta)$ is the set of piecewise constant functions with period Δ, and N is the number of sampling periods in the prediction horizon. $\dot{V}(x(t_k), u(t_k))$ represents the time derivative of $V(x)$, i.e., $\frac{\partial V}{\partial x} F(x(t_k), u(t_k), 0)$. $\Phi(x)$ is the stabilizing control law assumed for the nonlinear system of Eq. 1. The cost function $L_t(\tilde{x}(t), u(t))$ satisfies $L_t(0,0) = 0$ and $L_t(\tilde{x}(t), u(t)) > 0$, $\forall(\tilde{x}(t), u(t)) \neq (0,0)$ such that the minimum value of the cost function will be attained at the equilibrium of the system of Eq. 1. We assume that the states of the closed-loop system are measured at each sampling time instance and will be used as the initial condition in the MPC optimization problem of Eq. 7 in the next sampling step. Specifically, based on the measured state $x(t_k)$ at $t = t_k$, the above optimization problem is solved to obtain the optimal solution $u^*(t)$ over the prediction horizon $t \in [t_k, t_{k+N})$. The first control action of $u^*(t)$, i.e., $u^*(t_k)$, is sent to the control actuator to be applied over the next sampling period. Then, at the next sampling time $t_{k+1} := t_k + \Delta$, the optimization problem is solved again, and the horizon will be rolled one sampling time. Specifically, the MPC optimization problem minimizes the objective function of Eq. 7a over the prediction horizon $t \in [t_k,\ t_{k+N})$ subject to the constraints of Eqs. 7b-7f that represent the process model, the state measurement used as the initial condition for MPC at $t = t_k$, the input constraints, and the two Lyapunaov-based constraints for ensuring closed-loop stability, respectively. Once the attack is verified through the sliding alarm window, the MPC of Eq. 7 switches to the state measurement from redundant, secure sensors as the initial condition $x(t_k)$ for Eq. 7c for the remaining time of process operation such that the closed-loop stability is maintained by bounding the state trajectory within Ω_ρ and ultimately driving the state into the terminal set $\Omega_{\rho_{min}}$ around the origin. Note that the back-up sensors are not connected to the online system to ensure they remain secured to any sensor cyber-attacks that have access to sensor measurement through network. In addition to physically isolating the problematic sensors, the impact of sensor attacks can be mitigated by reconstructing tampered state measurements and restoring system stability via machine-learning-based state observers (Wu et al., 2020). An exemplar trajectory under attack-resilient MPC is shown in Fig. 5.

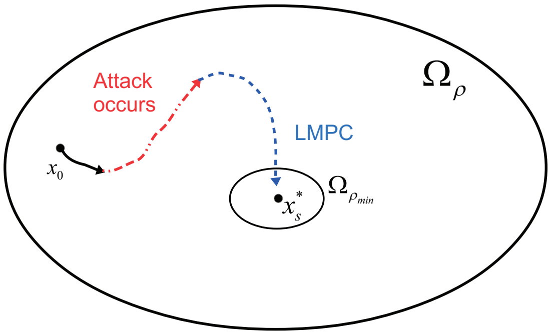


Figure 5: A schematic representing the stability region Ω_ρ and the target set $\Omega_{\rho_{min}}$ around the steady-state x_s^*. The trajectory first moves away from the origin due to cyber-attack and finally reconverges to $\Omega_{\rho_{min}}$ under the MPC of Eq. 7 after the detection of the cyber-attack.

Economic MPC. In addition to utilizing sensor redundancy in the context of tracking MPC, one can develop a similar approach for Economic MPC (EMPC), which is another form of MPC that directly integrates process economic considerations with process control to dynamically optimize process economics through time-varying operation. A number of past works have been developed to address stability, safety, and computational efficiency issues in EMPC (Heidarinejad et al., 2012; Angeli et al., 2011; Müller et al., 2013; Ellis et al., 2014; Wu et al., 2018a). To handle the cyber-attacks that compromise both closed-loop stability and process economic benefits under EMPC, the attack-resilient Lyapunov-based EMPC design, which combines open-loop and closed-loop control, is developed and represented by the following optimization problem:

$$\mathcal{J} = \max_{u' \in S(\Delta)} \int_{t_{N_0}}^{t_{N_0+N_p}} l_e(\tilde{x}(t), u'(t))dt \tag{8a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u(t), 0) \tag{8b}$$

$$u'(t) \in U, \ \forall\, t \in [t_{N_0}, t_{N_0+N_p}) \tag{8c}$$

$$\tilde{x}(t_{N_0}) = \bar{x}(t_{N_0}) \tag{8d}$$

$$V(\tilde{x}(t)) \leq \rho_{secure}, \ \forall\, t \in [t_{N_0}, t_{N_0+N_p}), \quad \text{if } \bar{x}(t_{N_0}) \in \Omega_{\rho_{secure}} \tag{8e}$$

$$\dot{V}(\bar{x}(t_{N_0}), u) \leq \dot{V}(\bar{x}(t_{N_0}), \Phi(\bar{x}(t_{N_0}))), \quad \text{if } \bar{x}(t_{N_0}) \in \Omega_\rho \backslash \Omega_{\rho_{secure}} \tag{8f}$$

where $\Omega_{\rho_{secure}}$ is the set that the process will be operated within such that the system will not immediately lose stability when under malicious cyber-attacks. N_p is the number of sampling periods in one material constraint period, which is the prediction horizon for open-loop control. Since it is common that chemical processes are subject to periodic feed stock constraints, which are specified as part of the input constraint set U, we also require, for example, the quantity of feed materials to be limited within a fixed period of time t_{N_p}. During this period of time (termed material constraint period), the total feed material is constrained to a constant value C, i.e., $\frac{1}{t_{N_p}}\int_{t_0}^{t_{N_p}} u_m(\tau)d\tau = C$, where u_m represents feed material used at every sampling period. Therefore, the material consumption constraint renews every t_{N_p}. If the total operation time is longer than one material constraint period, this material consumption constraint results in cyclic operation of the plant, and consequently, the cyclic behavior of the state-space trajectory. At the start of a new material constraint period, the total consumption limit is renewed, as new feed materials become available to be used again for the next constraint period. In the presence of cyber-attacks, the attack-resilient EMPC is implemented as follows. At time t_k, the EMPC in the open-loop control mode receives the state measurement $x(t_k)$ and computes the optimal trajectory of N_p control action that will be applied in a sample-and-hold manner until the end of this material constraint period. In the case that there are no cyber-attacks or process disturbances, this optimal trajectory of control actions would yield maximum economic benefits while meeting all input and state constraints. While at the closed-loop operation, if the feedback measurement is no longer reliable and cannot be used for closed-loop control, the open-loop control actions that were calculated at the beginning of the material constraint period will be used as a substitute until the end of the material constraint period.

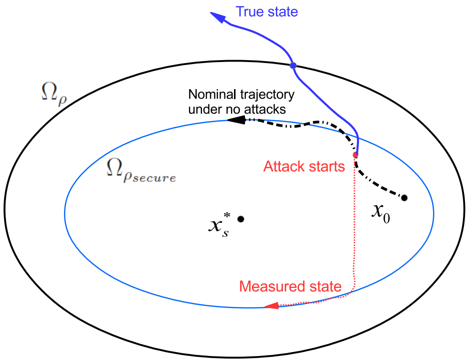


Figure 6: Demonstration of closed-loop operation under EMPC around a secure operating region showing the nominal state trajectory under no attacks and state measurements and true state evolution under a cyber-attack.

At the end of the material constraint period, a cyber-attack detector is activated to determine any occurrence of an attack and the reliability of the control system is reassessed. The detector will provide information on the security status of the feedback measurements over the latest material constraint period. Upon mitigating the impact of a confirmed attack and/or confirming the security of the control system, closed-loop control with secure feedback measurement can be reactivated as a new material constraint when the period starts. The operation of EMPC around a secure operating region is illustrated in Fig. 6 and the attack-resilient strategy of switching from closed-loop to open-loop control is illustrated in Fig. 7.

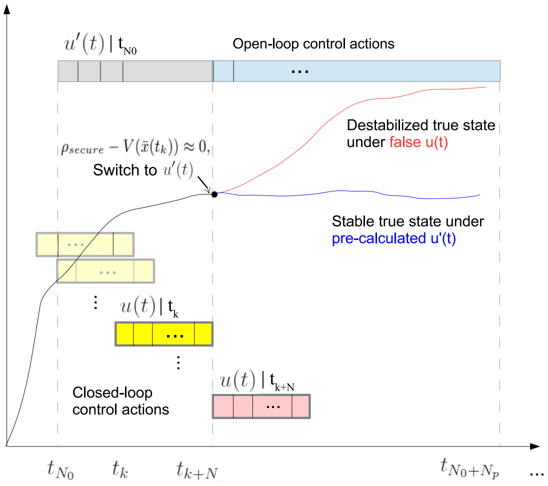

$u'(t) \mid t_{N0}$
Open-loop control actions
...
$\rho_{secure} - V(\bar{x}(t_k)) \approx 0,$
Switch to $u'(t)$
Destabilized true state under false u(t)
Stable true state under pre-calculated u'(t)
...
...
$u(t) \mid t_k$
...
Closed-loop control actions
$u(t) \mid t_{k+N}$
...
t_{N_0}
t_k
t_{k+N}
$t_{N_0+N_p}$
...

Figure 7: Demonstration of attack-resilient EMPC control strategy by switching from closed-loop control actions to pre-calculated open-loop control actions when the state measurements reach the boundary of the secure operating region.

Integrated Attack Detection and Control Policies: Additional Recent Results

A key issue for cyber-attacks in chemical process industries is that they can impact process safety by directly adjusting process states or potentially the equipment condition (Nieman et al., 2020). This motivates a fundamental understanding of the nature of the interactions between the control design and cyber-attacks on various components of the control loop. For example, Durand (2018) elucidated a challenge with attempting to thwart the falsification of sensor measurements using a randomized control law selection. This challenge prevents attacks from causing an issue that may require certain control laws to be used in different regions of state-space, which an attacker can use to provide attacks that are destabilizing. Randomness was further explored in the context of taking advantage of noise in quantum computation for adding randomness to control action selection in Rangan et al. (2022) and for similar reasons, was not able to thwart cyber-attacks on the sensor measurements. However, designing cyberattack detection policies in tandem with control laws can aid in forcing attacks to reveal themselves by setting expectations for what a non-attacked process state trajectory should appear as using the control theory and then by detecting whether the control-theoretic requirements are achieved using the detection policy (in the spirit of other active attack detection policies such as dynamic watermarking (Satchidanandan and Kumar, 2016)).

Integrated attack detection and control policies have been explored in the context of Lyapunov-based economic model predictive control (LEMPC) (Heidarinejad et al., 2012) of nonlinear systems when sensors (Durand and Wegener, 2020; Oyama and Durand, 2020), actuators (Rangan et al., 2022), or sensors and actuators at the same time (Oyama et al., 2022) can be attacked. These policies have considered indicators of attacks such as whether the Lyapunov function is decreasing along the state measurement trajectory, is comparing state predictions with state measurements, or is adding redundancy in state estimates that can be used to provide cross-checking of whether state measurements are correct. These provide different safety guarantees (in the sense that the closed-loop state is maintained within an expected region of state-space at least for some time after an attack) when the sensors are attacked, when the actuators are attacked, or when different detection policies are combined and both sensors and actuators are attacked. The case that sensor measurements are attacked has also been considered for the case that the process dynamics could change at the same time (Oyama et al., 2021; Rangan et al., 2021). Through an extension of the LEMPC-based integrated detection and control policies to this case through a two-tier attack detection policy, safety for at least some time period after an attack on the sensors, process dynamics change, or both can be guaranteed under sufficient conditions. An example of further practical consideration for the cybersecurity of control systems is enabling the evaluation of attacks on sensors, which might be considered in a next-generation manufacturing process, such as in image-based control systems, for which simulations of how replacing or falsifying images used in a level control loop might impact the tank level was explored using the 3D graphics software toolset Blender (Oyama et al., 2022).

Additionally, as discussed in the previous section, achieving process control resiliency to cyber-attacks requires the ability to detect the presence of a cyberattack targeting the process control system. For some classes of cyber-attacks, the ability to detect attacks is impacted by the process control system design (Narasimhan et al., 2022b). To this end, a controller parameter screening methodology was developed to select control parameters that do not mask the impact of cyber-attacks on detection schemes, rendering cyber-attacks detectable by the detection schemes (Narasimhan et al., 2022b). The analysis in Narasimhan et al. (2022b) revealed that the control system design impacted the ability to detect multiplicative attacks with residual-based detection schemes. Additionally, the control system design may also impact cyber-attack identification and mitigation, albeit more work in this direction is needed. While the selection of such controller parameters can enhance the ability to detect attacks, it can also degrade the performance of the attack-free closed-loop system relative to the performance under control parameters selected based on conventional design criteria. To balance this trade-off, an active attack detection methodology that employs the controller parameter switching was developed (Narasimhan et al., 2022a). The detection methodology involves switching between two sets of control parameters. The first parameter set is chosen based on the conventional design criteria and the other based on the ability to detect a range of cyber-attacks. Since switching may excite the process dynamics resulting from the potential of false alarms, a switching condition was presented to minimize false alarms (Narasimhan et al., 2022c).

Encrypted Control

In addition to detection and recovery, another way to enhance the cybersecurity of control systems is to establish secure remote access. Encryption-based control using the encryption of the communication signals (e.g., semi-homomorphic encryption methods) can be developed to ensure secure communication in the sensor-controller and controller-actuator links in the presence of cyber-attacks. Homomorphic Encryption (HE) allows the performing of arithmetic operations such as addition and multiplication in the ciphertext (encrypted message) space such that no decryption on messages is needed in order to perform these operations. Unlike conventional control schemes, encrypted control systems compute encrypted inputs based on encrypted states and encrypted controller parameters without intermediate decryptions by the controller to ensure the confidentiality of safety-critical system states, control actions, and controller parameters in the closed-loop system. Specifically, encryption-based control systems will first encrypt state measurements at the sensor and transmit the ciphertexts to the cloud where the encrypted control actions are computed. Once the actuator receives the encrypted control actions, it decrypts the ciphertexts and applies the control actions in the form of plaintext to the nonlinear system of Eq. 1. Since data remains encrypted during transmission and optimization of control actions, cyber-attacks targeting the communication in the sensor-controller and controller-actuator links are effectively prevented. Paillier encryption, one of the additive homomorphic cryptosystems, has been widely used whose security guarantees rely on a standard cryptographic assumption called Decisional Composity Residuocity (DCR) (Paillier, 1999; Kogiso and Fujita, 2015; Darup et al., 2017, 2021). In Darup et al. (2017), an encrypted explicit MPC scheme was designed using the Paillier cryptosystem for a linear constrained system, where the authors developed the quantized control law as a linear piecewise affine function. The property of homomorphism allows the computing of the encryption of the sum of two signals (i.e., $m_1 + m_2$) given only the encryption of m_1 and m_2 and the public key. It is important to note that Pallier Cryptosystem or any other Partially Homomorphic Encryption (PHE) scheme allows the encrypted evaluation of the control input (using encrypted states and controller parameters) only for a linear control law of the form $u = Kx + b$. Hence, the design of encrypted controllers for nonlinear systems is not straightforward. Specifically, the key of Paillier cryptosystem is generated as follows.

1. Select two random large prime numbers p and q such that $gcd(pq,(p-1)(q-1)) = 1$ where $gcd(i, j)$ refers to the greatest common divisor of $i, j \in \mathbf{N}$;

2. Calculate $M = pq$ and $\lambda = lcm(p-1, q-1)$ where $lcm(\cdot,\cdot)$ denotes least common multiple;

3. Select g as a random integer where $g \in \mathbf{Z}_{M^2} := \{g \in \mathbf{Z} \mid 1 < g < M^2\}$;

4. Ensure that n divides the order of g i.e., $g > M$;

5. Calculate $u = \left(L\left(g^{\lambda} \bmod M^2\right)\right)^{-1} \bmod M$ where $L(x) = \frac{x-1}{M}$ and the inverse refers to modular inverse;

6. If the inverse does not exist, go back to step 3 and change the value of g; if the inverse does exist, the public key (M, g) and the private key (λ, u) are obtained;

Using the keys generated, the data $m \in \mathbf{Z}_M$ (e.g., state measurements x of the nonlinear system of Eq. 1) is encrypted by first selecting a random integer $r \in \mathbf{Z}_M$ and then calculating the ciphertext as $E_M(m,r) = c = g^m \times r^M \bmod M^2$. The decrpytion of a message $c \in \mathbf{Z}_{M^2}$ is calculated by $D_M(c) = m = L(c^\lambda \bmod M^2) \times u \bmod M$. Since the Paillier Encryption allows the addition operations in encrypted form, the sum of plaintext messages $m_1, m_2 \in \mathbf{Z}_M$ such that $m_1 + m_2 \in \mathbf{Z}_M$ can be calculated by the following equation for all $r_1, r_2 \in \mathbf{Z}_M$.

$$\begin{aligned} E_M(m_1+m_2, r_1 r_2) &= E_M(m_1, r_1) E_M(m_2, r_2) \bmod M^2 \\ &= c_1 c_2 \bmod M^2 \end{aligned} \tag{9}$$

It is demonstrated in Eq. 9 that the addition operation can be carried out with the encrypted numbers directly, and therefore, no decryption is needed at this stage. Following the additive homomorphism property, a semi-encrypted product can be computed as follows. Given $m_1, m_2 \in \mathbf{Z}_M$ such that $m_1 m_2 \in \mathbf{Z}_M$, the multiplication of m_1 and m_2 can be written as addition of m_1 with itself for m_2 times. Therefore, using the additive homomorphism property of Eq. 9, the following equation is obtained for all $r \in \mathbf{Z}_M$.

$$E_M(m_1 m_2, r^{m_2}) = E_M(m_1, r)^{m_2} \bmod M^2 = c_1^{m_2} \bmod M^2 \tag{10}$$

Note that the product calculated in Eq. 10 is semi-encrypted since only c_1 is encrypted and m_2 is not. This also explains why Paillier cryptosystem is not a fully homomorphic scheme.

Since the messages/numbers to be encrypted in Paillier cryptosystem are required to be a set of integers, quantization of the signals is needed to map real numbers to integers to encrypt-decrypt the communication signals in the closed-loop system of Eq. 1 (Darup et al., 2017). Specifically, we first map the set of real numbers to the set $\mathbf{Q}_{l_1,d}$ as follows.

$$\begin{aligned} &g_{l_1,d} : \mathbf{R} \to \mathbf{Q}_{l_1,d} \\ &g_{l_1,d}(a) := \arg \min_{q \in \mathbf{Q}_{l_1,d}} |a - q| \end{aligned} \tag{11}$$

where $\mathbf{Q}_{l_1,d}$ is a set of rational numbers between -2^{l_1-d-1} and $2^{l_1-d-1} - 2^{-d}$ separated from each other with a resolution of 2^{-d}, i.e., $\forall q \in \mathbf{Q}$, $\exists \beta \in \{0,1\}^{l_1}$, such that $q = -2^{l_1-d-1}\beta_l + \sum_{i=1}^{l_1-1} 2^{i-d-1}\beta_i$. Subsequently, we map the set of rational numbers to the set of integers $\mathbf{Z}_{2^{l_2}}$ as follows:

$$\begin{aligned} &f_{l_2,d} : \mathbf{Q}_{l_1,d} \to \mathbf{Z}_{2^{l_2}} \\ &f_{l_2}(q) := 2^d q \bmod 2^{l_2} \end{aligned} \tag{12}$$

While the sensor data is encrypted and utilized by the controller to compute control actions without decryption, the control actions need to be decrypted before sending to the actuator to be applied to the system of Eq. 1. Therefore, the inverse operation $f_{l_2,d}^{-1} : \mathbf{Z}_{2^{l_2}} \to \mathbf{Q}_{l_1,d}$ is defined as follows:

$$f_{l_2,d}^{-1}(m) := \frac{1}{2^d} \begin{cases} t - 2^{l_2} & \text{if } t \geq 2^{l_2-1} \\ t & \text{otherwise} \end{cases} \tag{13}$$

While Eq. 13 maps the decrypted inputs back to the rational number space, it can be observed that there will be some error in the input due to the difference between the actual control input and the one mapped to its closest rational number within the set $\mathbf{Q}_{l_1,d}$. Therefore, to address this issue, the control system should be designed to ensure a certain degree of robustness with respect to potential encryption process errors. For example, the quantizations of the state measurements and controller matrices can be modeled as artificial disturbances to the system of Eq. 1 (i.e., $h(x)w$) and accounted for in the design of a robust control scheme.

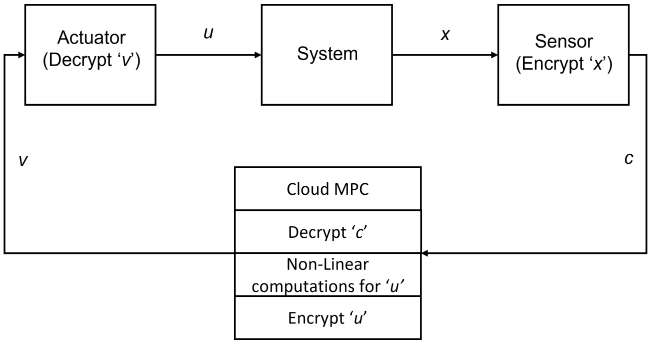


Figure 8: Encrypted control scheme for nonlinear processes.

Darup et al. (2017) describes the encrypted control law evaluation only for a linear system having the control law of the form $u = Kx + b$. This limitation is imposed by the nature of the Partially Homomorphic Cryptosystems which only allow the addition and multiplication operations in the encrypted message space. Thus, in the case of nonlinear systems or nonlinear control laws, it is important to modify our approach. A nonlinear control law can be defined as $u = \Phi(x)$. The sensor measures the states, encrypts them using the Public Key and sends them to the controller establishing a secure communication of the signals. The controller then decrypts the states and performs the nonlinear control law calculations. Once the control action has been computed, the controller then encrypts it (using the Public Key) and sends it to the actuator. At the actuator, the control input is decrypted and the control action is applied to the nonlinear system. We use quantization functions to convert the states and controller parameters to the integer message space in order to prepare them for encryption. This quantization of real numbers induces some loss of data or quantization errors. Thus, in the case of nonlinear systems, it is important to model these quantization errors as disturbances to the system and the controller should be able to handle these disturbances. A schematic of this encrypted control scheme for nonlinear systems is shown in Fig. 8. More work needs to be done in this direction to address the stability, robustness, and performance issues for explicit nonlinear control as well as model predictive control.

Control Architecture Design for Handling Cyber-attacks: Decoupling Stability and Performance Objectives

To enhance the robustness of MPC to cyber-attacks, a two-tier control architecture was designed by Chen et al. (2020b) to allow convenient reconfiguration of the control system to stabilize the process to its operating steady state upon successful detection of cyber-attacks. Specifically, we consider the following class of continuous-time nonlinear systems:

$$\dot{x}(t) = f(x(t), u_c(t), u_a(t)) \tag{14a}$$

$$y_c(t) = h_c(x(t)),\ y_a(t) = h_a(x(t)) \tag{14b}$$

where $x \in \mathbf{R}^{n_x}$ is the state vector, $y_c(t) \in \mathbf{R}^{n_{y_c}}$ represents the vector of state measurements that are sampled continuously (e.g., reactor temperature), and $y_a(t) \in \mathbf{R}^{n_{y_a}}$ represents the vector of networked state measurements that may be sampled asynchronously at $t = t_k$ (e.g., reactor product concentration); u_c and u_a are the manipulated input vectors, which are constrained by $[u_c \in \mathbf{R}^{m_{u_c}}, u_a \in \mathbf{R}^{m_{u_a}}] \in U$. Through y_c and y_a, we assume measurement of the full state vector x can be obtained at t_k. The cyber-secure control architecture integrates a lower-tier control system that uses the dedicated sensor measurements, $y_c(t)$, to ensure stability of the steady-state of the closed-loop system and an upper-tier, high-performance control system (e.g., MPC) that uses both dedicated ($y_c(t)$) and networked ($y_a(t)$) sensor measurements to improve closed-loop performance significantly above what could be achieved with the lower-tier control system.

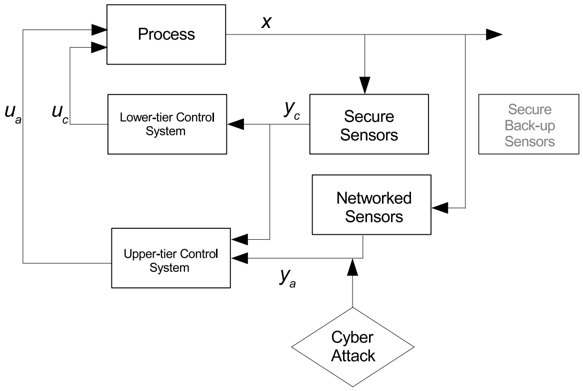
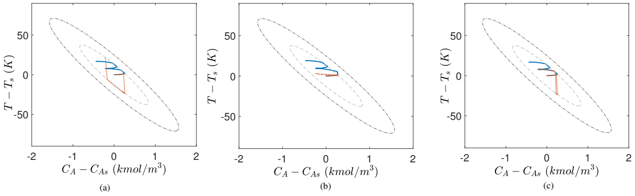


Figure 9: Two-tier control-detector architecture showing lower-tier controllers using continuous secure sensor measurements and an upper-tier MPC using both continuous (secure) and networked (vulnerable to cyber-attacks) sensor measurements, where secure back-up sensors, if available, can be used to replace the compromised networked sensor for upper-tier MPC (Chen et al. (2020b)).

Specifically, we assume that for the lower-tier controller, there exists an explicit feedback controller $u_c(t) = \phi_c(y_c(x)) \in U$ that can stabilize the closed-loop system of Eq. 14 using only the continuous measurements $y_c(t)$. The Lyapunov-based MPC (LMPC) of Eq. 7 can be used as the upper-tier controller to fully utilize the networked (potentially asynchronous) state measurements $y_a(t)$ and to compute $u_a(t)$ that improves the overall closed-loop performance over what can be achieved with $\phi_c(y_c)$ while not jeopardizing the stability properties achieved by $u_a(t)$. Upon detection of an attack on the sensors providing networked asynchronous state measurements to the two-tier control system, the control system reconfiguration logic allows for two mitigation plans. First, the control system can deactivate the upper-tier controller completely and operate the system under the stabilizing lower-tier control system only, which uses cyber-secure, dedicated sensor measurements. Since the lower-tier controllers are capable of driving the process to its operating steady state with secure continuous measurements, the effect of the cyber-attacks is fully eliminated in the closed-loop system in this case and the process is stabilized to the operating steady-state. Second, if a sensor isolation detector is also implemented, it will be activated once a sensor attack is verified. Subsequently, the upper-tier controller can choose to switch the compromised sensor to its redundant back-up sensor with secure readings. By abandoning the corrupted sensor and using its back-up sensor using a secure sensor-controller communication, the upper-tier controller remains functional and is able to drive the process to its steady state with better closed-loop performance. In the extreme case that both continuous and asynchronous sensor measurements are attacked, the upper-tier controller will be shut off and the lower-tier controllers will reroute their continuous measurement signals from the corrupted sensors to their respective secure back-up sensors. The two-tier control design, where the networked sensor measurements, $y_a(t)$, used only by the upper-tier controller may be under potential cyber-attack, is illustrated in Fig. 9. In addition to shutting off the upper-tier control system, the use of encryption of the signals of the upper-tier control system may be employed at the expense of reduced closed-loop performance in order to improve its robustness to signal quantization errors.

Application to a Chemical Process Example

We use a chemical process example as a benchmark to demonstrate the application of integrated data-based attack detectors and cyber-secure MPC schemes that minimize the impact of cyber-attacks on process operation. Specifically, machine learning detectors via feedforward neural network are developed using sensor measurements under nominal and noisy operating conditions in Chen et al. (2020b), and applied online to a simulated reactor-reactor-separator process. Two reactions take place in series ($A \rightarrow B \rightarrow C$) in both CSTRs and the overhead vapor from the flash tank is recycled to the first CSTR. The performance-improvement LMPC receives asynchronous measurements on the mass fractions of A and B in each of the three vessels (x_{A1}, x_{B1}, x_{A2}, x_{B2}, x_{A3}, x_{B3}, all of which can be subject to cyber-attacks), and manipulates the fresh feed flowrate into the second CSTR, F_{20}. Three safety critical PI controllers receive continuous measurements on the temperatures of the three vessels (T_1, T_2, T_3) and manipulate the heat inputs into each vessel Q_1, Q_2, and Q_3, respectively.



(a)

(b)

(c)

Figure 10: State-space plot showing the evolution of true process states (blue trajectories) and attacked state measurements (red trajectories) over two material constraint periods under the resilient LEMPC when (a) min-max, (b) geometric, and (c) surge attacks, targeting the temperature sensor are successfully detected by a NN detector at the end of the first material constraint period, $t = 0.06\ hr$, where the dash-dotted ellipse is the stability region Ω_ρ and the dashed ellipse is $\Omega_{\rho_{secure}}$ (Chen et al. (2020a)).

The process description and parameter values are given in Chen et al. (2020b), and are omitted here. An upper-tier Lyapunov-based MPC, which uses networked sensor measurements to improve closed-loop performance, is coupled with lower-tier cyber-secure explicit feedback controllers to drive a nonlinear multivariable process to its steady state. Although the networked sensor measurements may be vulnerable to cyber-attacks, the two-tier control architecture ensures that the process will stay immune to destabilizing malicious cyber-attacks. Simulation results demonstrate the effectiveness of these detection algorithms in detecting and distinguishing between multiple classes of intelligent cyber-attacks that may occur at different locations of the sensor network. Upon the detection of cyber-attacks, the two-tier control architecture allows convenient reconfiguration of the control system to stabilize the process to its operating steady state. The training and testing accuracy for detecting the presence of an attack, the attack type, or the location of the attack are given in Table 1. Furthermore, a modified Lyapunov-based EMPC using combined closed-loop and open-loop control action implementation schemes was proposed in Chen et al. (2020a) to optimize economic benefits in a time-varying manner while maintaining closed-loop process stability and resiliency against various types of cyber-attacks. Data-based cyber-attack detectors are developed using sensor data via machine-learning methods and these detectors are periodically activated and applied online in the context of process operation. With FNN detectors trained and applied online, the closed-loop state evolution under the resilient EMPC is shown in Fig. 10 where the process is exposed to three types of sensor cyber-attacks (Chen et al., 2020a).

Table 1: Detection accuracies of NN detectors trained under different scenarios of noise level, attack types, and detection purposes (Chen et al. (2020b)).

Scenario	Training (%)	Testing (%)
Nominal, One Attack	99.6	92.2
With Noise, One Attack	99.9	100
With Noise, Two Attacks	98.2	91.4
With Noise, Sensor Isolator	99.6	99.0

Control Architecture Design for Handling Cyber-attacks: Decentralized and distributed control

In addition to constructing control architectures where control systems are structured according to closed-loop stability and performance objectives, decentralized and distributed control systems provide an efficient solution to many challenges of controlling large-scale industrial processes (Christofides et al. (2013)) and may provide certain advantages with respect to robustness to cyber-attacks in comparison with centralized control systems. We will discuss decentralized and distributed control systems in the context of model predictive control. In a decentralized MPC system, no communication is established between the different local controllers, therefore each controller does not have any knowledge on the control actions calculated by the other controllers. While this may lead to reduced closed-loop performance, it may be beneficial in the context of cyber-attacks as the control systems can operate independently. Specifically, for each subsystem, a separate MPC is designed to regulate the states x_j of the subsystem j, $j = 1,...,N_{sys}$, and optimize the respective control actions. Each decentralized MPC j, $j = 1,...,N_{sys}$ can be represented by the following optimization problem:

$$\mathcal{J}_j = \min_{u_{d_j} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}_j(t), u_{d_j}(t))dt \tag{15a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}_j(t) = F_j(\hat{x}(t), u_{d_j}(t), 0) \tag{15b}$$

$$\hat{x}(t) = [\bar{x}_1(t_k) \cdots \bar{x}_{j-1}(t_k)\ \ \tilde{x}_j(t)\ \ \bar{x}_{j+1}(t_k) \cdots \bar{x}_{N_{sys}}(t_k)] \tag{15c}$$

$$u_{d_j}(t) \in U_j,\ \forall\, t \in [t_k, t_{k+N}) \tag{15d}$$

$$\tilde{x}_j(t_k) = \bar{x}_j(t_k) \tag{15e}$$

$$\begin{aligned}&\frac{\partial V(\bar{x}(t_k))}{\partial x_j}(F_j(\bar{x}(t_k), u_{d_j}(t_k)))\\ &\leq \frac{\partial V(\bar{x}(t_k))}{\partial x_j}(F_j(\bar{x}(t_k), \Phi_j(\bar{x}(t_k)))),\ \text{if}\ \bar{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_s}\end{aligned} \tag{15f}$$

$$V(\tilde{x}(t)) \leq \rho_s,\ \forall\, t \in [t_k, t_{k+N}),\ \text{if}\ \bar{x}(t_k) \in \Omega_{\rho_s} \tag{15g}$$

The control actions optimized by MPC j, denoted by u_{d_j}, will be applied to the corresponding control actuators in subsystem j. Note that while full-state feedback measurements could be available to all MPCs, each MPC in the decentralized MPC only has the information of the process dynamics of its respective subsystem.

To achieve better closed-loop control performance compared to decentralized MPC, distributed MPC systems may be developed to take advantage of some level of communication that may be established between the different controllers. Specifically, iterative distributed MPC systems (one of several DMPC architectures discussed in Christofides et al. (2013)) allow signal exchanges between all controllers, thereby allowing each controller to have full knowledge of the predicted state evolution along the prediction horizon and yielding better closed-loop performance via multiple iterations at the cost of more computational time. For example, both controllers communicate with each other in a two-MPC system to cooperatively optimize the control actions. The two controllers solve their respective optimization problems independently in a parallel structure and at the end of each iteration they will exchange solutions with each other. The optimization problem of MPC 1 in an iterative distributed LMPC at iteration $c = 1$ is presented as follows:

$$\mathcal{J} = \min_{u_{d_j} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_j}(t), \Phi_i(\tilde{x}(t)))dt \tag{16a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_j}(t), \Phi_i(\tilde{x}(t)), 0) \tag{16b}$$

$$u_{d_j}(t) \in U_j,\ \forall\, t \in [t_k, t_{k+N}) \tag{16c}$$

$$\tilde{x}(t_k) = \bar{x}(t_k) \tag{16d}$$

$$\begin{aligned}&\frac{\partial V(\bar{x}(t_k))}{\partial x}(F(\bar{x}(t_k), u_{d_j}(t_k), \Phi_i(\bar{x}(t_k))))\\ &\leq \frac{\partial V(\bar{x}(t_k))}{\partial x}(F(\bar{x}(t_k), \Phi(\bar{x}(t_k)))),\ \text{if}\ \bar{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_s}\end{aligned} \tag{16e}$$

$$V(\tilde{x}(t)) \leq \rho_s,\ \forall\, t \in [t_k, t_{k+N}),\ \text{if}\ \bar{x}(t_k) \in \Omega_{\rho_s} \tag{16f}$$

where the variables and constraints are defined following those in the decentralized MPC design. For each control action j corresponding to subsystem j, $i = 1,...,N_{sys}, i \neq j$, which refers to the control actions of all other subsystems except for j. At iteration $c > 1$, after the exchange of the optimized input trajectories $u^*_{d_j}(t), \forall t \in [t_k, t_{k+N})$ between all MPCs $j = 1,...,N_{sys}$, the optimization problem of MPC j is as follows:

$$\mathcal{J} = \min_{u_{d_j} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_j}(t), u^*_{d_i}(t))dt \tag{17a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_j}(t), u^*_{d_i}(t), 0) \tag{17b}$$

$$u_{d_j}(t) \in U_j, \ \forall\, t \in [t_k, t_{k+N}) \tag{17c}$$

$$\tilde{x}(t_k) = \bar{x}(t_k) \tag{17d}$$

$$\frac{\partial V(\bar{x}(t_k))}{\partial x}(F(\bar{x}(t_k), u_{d_j}(t_k), u^*_{d_i}(t_k)) \\ \leq \frac{\partial V(\bar{x}(t_k))}{\partial x}(F(\bar{x}(t_k), \Phi(\bar{x}(t_k)))), \text{ if } \bar{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_s} \tag{17e}$$

$$V(\tilde{x}(t)) \leq \rho_s, \ \forall\, t \in [t_k, t_{k+N}), \text{ if } \bar{x}(t_k) \in \Omega_{\rho_s} \tag{17f}$$

While both distributed and decentralized MPC systems are designed to alleviate the computational complexity for solving large-scale optimization problems for multiple subsystems as opposed to centralized MPC, the vulnerability to cyber intrusions also increases with the expansion of communication networks. The work in Chen et al. (2021) investigates the effect of different types of standard cyber-attacks on the operation of nonlinear processes under centralized, decentralized, and distributed model predictive control systems. The robustness of the decentralized control architecture over distributed and centralized control architectures was analyzed. Considering the inherent structure and operating requirement of both systems, the decentralized control system was found to exhibit greater robustness against potential cyber-attacks at the expense of a small performance loss versus centralized and distributed MPC.

While isolation and handling of actuator faults in nonlinear processes under continuous, synchronous measurements have been studied in Gani et al. (2007); Mhaskar et al. (2008); Ohran et al. (2008); McFall et al. (2008); Ohran et al. (2008), detection and handling of cyber-attacks in cooperative, distributed control architectures for nonlinear processes is a challenging task due to cyber-attack intelligence. Additionally, it cannot be addressed with the aforementioned process monitoring and control methods dealing with the centralized control systems because cyber-attacks may not only affect the sensor measurements going to the controllers but also the inter-controller communication. Therefore, as shown in Fig. 11 (Chen et al. (2021)), a machine-learning-based detector can be developed to detect and isolate cyber-attacks in the context of sequential DMPC. Subsequently, a resilient control strategy can be employed that orchestrates the reconfiguration of the control system. This strategy determines if the MPC algorithms should be reconfigurated or new backup control loops (e.g., switching from distributed MPC to decentralized MPC where there is no communication between the controllers) should be activated in the presence of cyber-attacks in order to preserve closed-loop system stability.

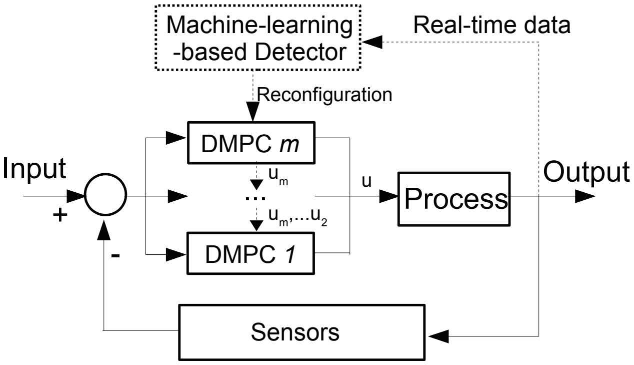


Figure 11: Sequential distributed MPC with machine-learning-based detector.

Application to a Chemical Process Example

A chemical process example of two CSTRs in series with the reaction $A \rightarrow B$ taking place in both reactors is simulated in Chen et al. (2021) to demonstrate the robustness of decentralized control architectures and the effectiveness of the neural-network detection scheme in maintaining the closed-loop stability of the system. The process description and parameters can be found in Chen et al. (2021) and are omitted here. The following Figs. 12-13 from Chen et al. (2021) show the true closed-loop state trajectories under the decentralized control-detector system. The proposed control-detector architecture and detection methodology can be extended to other applications of model predictive control or other methods of advanced control systems, in general.

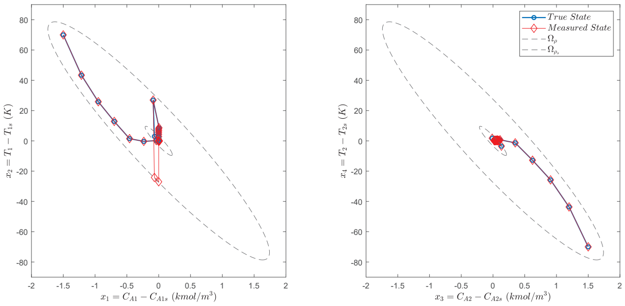


Figure 12: Closed-loop trajectories of true states. The two-CSTR process is operated under the decentralized MPC system when surge attacks are added to the temperature sensor T_1 of the first CSTR at $t = 0.30$ hr and detected by the 2-class FNN detector at $t = 0.32$ hr, after which all sensors are switched to their secured back-up sensors and the true process states are driven back to the ultimate bounded region Ω_{ρ_s} around the operating steady state (Chen et al. (2021)).

Cybersecurity in Operations and Supply Chains

As new technologies such as wireless networks and internet communication bring efficiency to the existing chemical plants, the integration of digitalization in process operations and supply chains is exposing chemical plants to unknown cybersecurity risks. These issues go, of course, beyond chemical plants and influence the operation of all industrial sectors of the economy (e.g., (Sun et al., 2018; Smetana et al., 2021; Perez et al., 2021)). Cyber-attacks targeting operations and supply chains can lead to loss of production, unplanned downtime, quality degradation, and disturbances to cash-to-order processes and the supply chain.

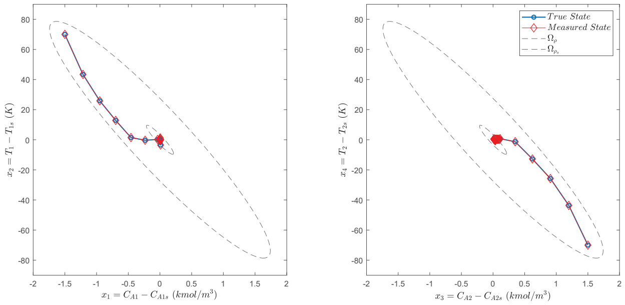


Figure 13: Closed-loop trajectories of true states. The two-CSTR process is operated under the decentralized MPC system when geometric attacks are added to the temperature sensor T_1 of the first CSTR at $t = 0.30\ hr$ and detected by the 2-class FNN detector at $t = 0.35\ hr$, after which all sensors are switched to their secure back-up sensors and the true process states are maintained within the ultimate bounded region Ω_{ρ_s} around the operating steady-state (Chen et al. (2021)).

To enhance the security of plant operations in the OT cyber space, a plant engagement model is typically developed to: 1) assess the current state of cybersecurity, 2) identify and catalog all networked computing devices, and 3) create a plan of improvements. Additionally, conventional IT methods such as anti-virus software, operating system patches, network firewalls and the use of multi-factor authentication for remote access are also utilized to provide another layer of security in process operations. When developing OT security methods for critical plants and manufacturing operations, it should be kept in mind that many chemical plants were designed decades ago with OT networks that are not able to handle cyber-attacks. To ensure secure, safe, and resilient operations, operators should develop a recovery plan to restore plant operations when a cyber-attack occurs and impacts plant operations. Some common practices for operators to proactively integrate cybersecurity into operations include alerts design, operation monitoring, attack identification and investigation, event reporting, log review, event analysis, and incident handling and response.

Similarly, cybersecurity in supply chain cannot be viewed as an IT problem only. A diagram of a supply chain network with common cyber-secure IT and OT approaches is shown in Fig. 14. Since a supply chain includes a large number of sectors such as product design, manufacturing, and distribution via the combination of hardware and software, cloud or local storage, and distribution mechanisms, a cyber-attack on a single supplier may remain undetected for a long time until it leads to chain reaction and eventually compromises the entire network. The cybersecurity risks in supply chain may involve a number of aspects such as sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise. To improve the cybersecurity of supply chain management, companies have adopted a variety of practices such as including security requirements in every contract, automation of manufacturing, testing regimes to reduce the risk of human intervention, validating third-party code and software before using, and limited software access to vendors (Ghadge et al., 2019; Cheung et al., 2021; Sobb et al., 2020).

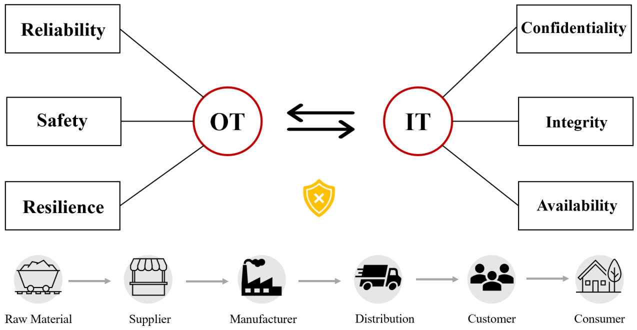


Figure 14: Cyber-secure supply chain with IT and OT integration.

The recent survey article by Enayaty-Ahangar et al. (2020) provides a survey of optimization models and methods for cyberinfrastructure security in the past two decades in which it is demonstrated that various optimization methods such as game theory, mixed integer programming, and linear/nonlinear programming have been widely used to improve cyberinfrastructure security in many ways involving prevention/protection, detection, mitigation, response and recovery from a cyber-threat. In Sun et al. (2018), recent research results on the cybersecurity of a smart grid were discussed and a cyber-power system test-bed was used to demonstrate the impact of attacks and the effectiveness of cybersecurity solutions. More recently, Smetana et al. (2021) introduced the integration of food system technologies with cyber-physical system technologies and pointed out the need for the development of efficient defence mechanisms to address potential cyber-food-safety risks and hazards.

In another recent work, Cheung et al. (2021) provided an overview of research works on cybersecurity in supply chain management. It was pointed out that the measures for enhancing cybersecurity can be classified into three broad categories: precautionary measures, real-time recovery measures, and aftermath measures, which are very similar to the practices introduced for process control systems (i.e., advanced threat detection, security by design, secure remote access, and advanced recovery) and reviewed in the earlier part of this manuscript. Specifically, some common precautionary measures for supply chains are the identification of vulnerabilities in cyberspace, secure access, authentication, data protection, firewall, and gateway development. Machine learning, game theory, Bayesian analysis, and attack path generation and analysis methods have been applied to identify and locate vulnerabilities while blockchain technology has been widely used for data protection and authentication (Kshetri, 2017; Taylor et al., 2020). For example, game theory has been widely used in the supply chain to optimize a defender's strategy by modeling each player's (i.e., attack and defender) behavior and strategies and to capture the interaction between two opposing players. To provide a high-level description of this approach, consider an attacker with a set of N_a potential attacking strategies $\{s_{a,i}\} \in S_a$ and a defender with a set of N_d potential defense strategies $\{s_{d,i}\} \in S_d$, where S_a, S_d are the space of all possible strategies for attacker and defender, respectively, and i represents the strategy index (Colbert et al., 2020). Given an attack strategy i and a defense strategy j, the attacker suffers a cost $C_{a,ij}$ to penetrate the security layer and accomplish its goal and the defender spends a cost $C_{d,ij}$ to apply its strategy. Additionally, given a strategy tuple $\{i, j\}$, it is assumed that the attacker succeeds in attacking the l_{th} system with probability $p_l(s_{a,i}, s_{d,j})$, $l = 1, ..., N$. Assuming the attacker gains a benefit b by successfully attacking a network of N subsystems and both the attacker and defender have complete knowledge of the system, the utility u_a for the attacker can be calculated as follows:

$$u_s(s_{a,i}, s_{d,j}) = b \cdot \Pi_{l=1}^{l=N} p_l(s_{a,i}, s_{d,j}) - C_{a,ij} \tag{18}$$

Similarly, the utility u_d for the defender is as follows:

$$u_d(s_{a,i}, s_{d,j}) = b \cdot [1 - \Pi_{l=1}^{l=N} p_l(s_{a,i}, s_{d,j})] - C_{d,ij} \tag{19}$$

Therefore, for both the attacker and defender, the objective is to select the optimal strategy that maximizes their utilities, for which a number of strategy selection methods have been developed in literature. Interested readers may refer to Zhu et al. (2010); Do et al. (2017); Attiah et al. (2018); Cheung and Bell (2021) for the applications of game theory in cybersecurity. In addition to the optimization-based approaches discussed above, laws, policies, regulations, and standards (e.g., National Institute for Standards and Technology (NIST)) are another important precautionary measure to provide guidelines for companies. With regards to real-time recovery, component isolation and recovery, real-time monitoring as well as communication and interaction between supply chain partners are some common measures to mitigate the impact of cyber-attacks on the supply chain networks. Finally, aftermath measures such as data backup, resilient infrastructure design, and system restoration are needed to ensure full recovery of the network and to refine the precautionary and real-time recovery plans.

Industrial Cybersecurity with IT and OT Integration

Operational technology (OT) cybersecurity has gained increasing attention since 2010. To handle recent cyber events that have driven the need for more regulations and measures to combat cyber-threats in chemical industries, major chemical companies, such as Dow, have developed very significant cybersecurity programs. For example, Dow established its first generation cybersecurity program in 2017 and has greatly improved the program in the following years to keep pace with the evolving threats. While this article has mainly addressed cybersecurity concerns in OT space, it is noted that both IT and OT are utilized in industry to develop cybersecurity solutions to protect software, hardware, infrastructure, people, and data. It is important for process engineers to understand both IT and OT cybersecurity landscapes to be able to develop frameworks for detection and control/learning system design that integrate the best policies from both domains to create workable solutions. On the one hand, the connection to IT network enables constant monitoring of the performance and condition of equipment and systems, and allows the industrial systems to obtain a more detailed view of individual equipment and conduct a more comprehensive analysis of the entire plant through big data. On the other hand, traditional OT systems do not have cybersecurity features such as encryption and authentication systems for secure data access and the equipment with long life cycles in OT systems cannot be regularly updated with patch systems due to stability concerns. Therefore, to allow for digital modernization of chemical industries, advanced cybersecurity solutions with IT and OT integration need to be developed and broadly implemented.

Compared to traditional IT cybersecurity, OT solutions are unique purpose-built technologies and protocols for systems that have been operated much longer than IT systems. Since upgrades or changes in the OT space generally require plant shutdowns which are not easily done, cyber-assessment and cyber-protection packages with minimum disruption to operations should be developed and deployed at high priority plants. Additionally, the International Society of Automation (ISA) has provided a guidance (i.e., IEC 62443) for companies to evaluate the cost of any potential attacks from four aspects: consequences, threats, recovery, and investment in the development of OT cybersecurity solutions.

Cybersecurity and Safety

Since the primary objective of cybersecurity in OT space is to ensure the safe operation of physical assets at all times, we also need to combine safety with control systems to handle cyber-attacks on safety-critical systems that have the potential to cause real harm in the physical world. In addition to the cyber-secure control systems, process safety systems such as alarms systems, emergency shutdown systems, and safety relief devices can provide the last line of defense in the event of an abnormal situation due to cyber-attacks. To prevent the system states from leaving their safety limits prior to the successful detection of cyber-attacks, safety systems can be integrated with control systems to reduce the physical risks of cyber-attacks ranging from simple unplanned downtime in operations to a plant explosion or release of hazardous materials (Wu and Christofides, 2021). Specifically, Safeness Index functions $S(x)$, a function of the (closed-loop) process states that characterizes the "safeness" of a process operation, can be adopted as a safety metric for the activation/deactivation of safety systems (Albalawi et al., 2017; Wu et al., 2018b; Zhang et al., 2019). Safe and unsafe operations can then be evaluated by comparing the value of $S(x)$ with the threshold value that is pre-determined using process first-principles knowledge or past plant data. Additionally, because the Safeness Index function can provide information on both measured and estimated states, its use in the alarm system can help manage the trade-off between measuring fewer states (which may lead to missed alarms) and more states (which leads to instrumentation expenses and possibly more occurrences of alarm overloading).

In addition to integrating process safety metrics into the decision making models of safety systems, integrating the actions of safety systems and control systems may be beneficial as well as pointed out in Wu and Christofides (2021). Specifically, in the traditional process safety paradigm, process variables are stabilized at their set-points by basic process control systems under normal operation; when the control system fails to operate the process in a safe operating region in the presence of disturbances or cyber-attacks, the safety systems (e.g., alarm systems, emergency shutdown systems (ESS), and safety relief devices) are activated to prevent further unsafe operation. However, since the process dynamics is changed after the activation of safety systems (e.g., the opening of a pressure relief valve to prevent high pressure in a chemical reactor), the actions taken by the safety systems should be taken into account in the reconfiguration of control systems. For example, the cyber-secure control system proposed in the previous section can be integrated with safety systems that take actions based on whether $S(x)$ crosses the threshold. We assume secure, redundant sensors or reliable state estimations are available to the control, alarm, emergency shutdown, and relief systems with standard industrial practice. Additionally, the actions taken by the alarm, ESS, and relief systems are assumed to be on-off type actions to simplify the discussion. In the case that safety systems are triggered due to cyber-attacks, the safety-based (lower-tier) control system continues to regulate the process state, while the upper-tier MPC needs to switch to secure, redundant sensors or encrypted secure channels to obtain the the true state, and update the prediction model to account for the change in system dynamics. The safety system will be taken off-line after process states enter the safe operating region, and subsequently, the two-tier control system switches to the initial process model.

Future Research Directions

Actuator cyber-attack detection and handling

Similar to sensor cyber-attacks, actuator cyber-attacks also have access to the plant model and controller design details, aiming to diverge the system away from its ideal operating point. However, instead of altering the sensor measurements, actuator attacks modify the direction and magnitude of the control actions without being detected by sensor monitoring tools. Common detection strategies include active detection methods that design excitation signals to be superimposed on the control commands to increase the detectability of the attack and developing an input observer to detect attacks as well as estimating the magnitude of the attack (Muniraj and Farhood, 2019). Unlike the passive detection methods that use regular operation data to determine if the operation is being affected by a cyberattack, active detection methods that apply some perturbation to the closed-loop process system through the control system can actively probe systems for cyberattacks. Conceivably, active detection methods may ensure that a process is free of a wider range of possible cyberattacks than passive detection methods. Future work developing novel active detection methods and, potentially, extending these methods to aid identification and mitigation may prove fruitful. Furthermore, it is noted that certain actuator attacks are undetectable by an observer-based controller (Ayas and Djouadi, 2016); thus, a machine-learning-based detection method may provide new insights. In addition to the detection of actuator attacks, an isolator may need to be developed to identify the affected actuator(s) in the network. Subsequently, to mitigate the effect of actuator attacks, machine learning methods may be utilized to identify cyber-attack patterns and predict future attack actions. Based on that, a resilient control system may be developed to compensate the effect of attacks without having to shut down the entire plant. Additionally, in the case that a safety-critical actuator is under attack, a controller that can operate the system in the presence of actuator attacks needs to be developed to account for the unavailability of the affected actuators due to a physical intervention of maintenance personnel.

Encrypted control

Since implementing encryption to encrypt-decrypt the communication signals involves the quantization of the signals and calculations using large integers, which may result in significant delays in order to ensure error-free signal encryption-decryption, the encryption-decryption scheme should be tuned to ensure that the calculations can be done with the available computational resources for a specific operating region in the state-space. Once the region of operation size is increased, the computational burden of the encryption-decryption scheme increases as larger deviations from the steady state correspond to larger numbers that need to encrypt using fixed-point operations that are more computationally expensive. This trade-off needs to be carefully studied, and quantitative computational formulas need to be developed to determine how the size of the allowable operating region should be influenced by the presence of potential cyber-attacks such that encryption can be used with allowable computational resources, need to be developed.

Incorporation of domain knowledge in the design of machine-learning-based cyber-attack detectors

Process dynamics and control strategies can be used to determine the most cost-effective and flexible frameworks for providing security to process networks and computing devices. This is important because an overly conservative cybersecurity policy can impede progress toward an efficient next-generation manufacturing framework; better understanding how the physics of the process help to dictate what types of security measures are required is important for preventing the negative impacts of attacks without getting in the way of process adaptability. For example, the machine-learning detector presented above is built using all the input variables available with an attempt to capture all possible relationships between inputs and outputs. However, in the case of large-scale chemical process networks, several issues may arise if taking all inputs into the training of the detector, especially when the outputs are not sensitive (or are fully decoupled) to some of the inputs or process states. In the example of two CSTRs in series, the states of the first CSTR influence the states (and thus, the dynamic behavior) of the second CSTR, but the states of the second CSTR do not influence the states of the first CSTR. This is important information that can be used as specific constraints on the structure of the machine learning detector for the entire two-CSTR system to improve its sensitivity to noise. Second, the detector structure may become complicated in terms of more layers and neurons in order to find a good approximation between all inputs and outputs, which increases the computational burden required for training the detector both off-line and on-line. Motivated by the above, one method for optimizing the detector structure is to perform an input selection (also termed as feature selection in machine learning) to select a subset of relevant features for use in detector construction using direct information of process structural relationships from process-directed graphs. By carrying out an input selection, the detector structure is simplified, which reduces the training times and avoids the burden of dimensionality. Additionally, another approach to improve the performance of the detector in terms of better prediction accuracy and less computation time is to incorporate chemical process structural knowledge in constructing it. Specifically, constraints will be imposed using process-directed graph information on some of the weight parameters in the detector such that the connected inputs, which have no impact on the output variables, exhibit no correlation to the outputs in the training process of the detector.

Decentralized learning for data security and privacy
Improving process data security is another important direction, particularly when this data is being operated upon using control laws or machine learning algorithms, to provide flexibility in manufacturing without concerns for data privacy. Therefore, further advances in techniques and frameworks for promoting privacy are needed to provide tractable solutions for industry. For example, developing a machine-learning-based detector for large-scale distributed systems requires a tremendous volume of data to be collected from all subsystems through various mediums of communication such as Internet and wireless networks, and then processed in a central server or cloud for training. However, as the communication mediums are vulnerable to attackers, the machine-learning-based detector developed in a local server or cloud could be misguided and unable to detect the target cyber-attacks in the presence of data tampering or data manipulation. In addition, as machine learning approaches have been widely used to develop data-driven models for chemical processes that can be incorporated in advanced process control schemes (e.g., MPC), data security and privacy is also of great importance and is gaining increasing attention. While centralized learning can process data and develop machine learning models in a centralized manner for large-scale distributed systems by taking advantage of a high performance computing cluster/cloud, data security and privacy becomes a big issue due to insecure communication links. To alleviate the security concerns, decentralized learning and federated learning methods that distribute a pretrained model to all subsystems, and allow each subsystem to develop and update its own model locally without sharing the raw data with the central server/cloud (AbdulRahman et al., 2020; Li et al., 2020; Ghimire and Rawat, 2022; Khan et al., 2021). The updated model parameters will be sent to the server for model aggregation, and finally, the updated model will be distributed to all subsystems. The idea of decentralized learning has shown its great potential in developing privacy-aware machine learning models, and needs to be further explored in the development of machine-learning-based detectors.

Cybersecurity, safety, operation and control: Engaging vendors
The interface of cybersecurity, safety, operation and control will certainly be explored further in the years to come. Despite the recent efforts to detect and mitigate the impact of cyber-attacks on process control systems, the impact of cyber-attacks on process safety has received very limited attention. How plant operators and control systems should work together to safely handle a cyber-attack with minimal performance loss and without costly plant shut-downs is an important question that needs to be studied. Engaging vendors that design, build, and implement safety and control systems to account directly in their architecture and implementation for cybersecurity concerns as well as monitor and analyze evolving cybersecurity threats should be an important consideration and a potential avenue to bring academic advances on the industrial floor. In this context, it is important that the cybersecurity solutions that are implemented in the OT space can work and cooperate effectively with multiple control system platforms developed by different vendors.

Industrial cases studies
In addition to the simulation studies of chemical reactors discussed in this manuscript, it is also important to investigate the implementation of the machine-learning-based detector and MPC to handle potential cyber-attacks in a variety of chemical process networks and energy systems (for example, gas pipeline networks). Novel detector-controller architectures need to be developed to improve the robustness of the entire pipeline network to cyber-attacks which is a critical need for the existing US pipeline networks. It is particularly important to build case studies using large-scale process simulators and incorporate as many as possible practical concerns based on direct industrial feedback to test the effectiveness and applicability of the methods developed by academics.

Cybersecurity awareness education and training
Cybersecurity concerns and cybersecurity mitigation methods are absent from today's chemical engineering curriculum at both undergraduate and graduate levels. Process control and process design courses as well as chemical engineering labs could be good starting points to introduce cybersecurity issues to raise awareness of cybersecurity concerns among our students who, in their vast majority, go to work in industry. In addition, the organization of short courses and workshops to communicate recent academic advances of cybersecurity approaches to engineers in industry and inform academics of industrial cybersecurity issues should be pursued. It is important to point out that while the present manuscript addresses OT cybersecurity concerns within a chemical process context, cybersecurity issues are present in all industries employing chemical engineers from chemical to pharmaceutical to food and materials industries.

Conclusion

This work presents an overview of recent research results on cybersecurity in process control, process operations, and supply chains. The design and implementation of cyber-defense OT methods including machine-learning-based cyber-attack detection, resilient control strategies, and their integration with MPC, encryption-decryption algorithms, and cyber-secure control architectures were discussed. Chemical process examples were used to demonstrate the efficiency and effectiveness of machine-learning-based detection schemes, and the robustness of attack-resilient MPCs and decentralized MPCs against several most common intelligent cyber-attacks discussed in the open literature. Additionally, an overview of cybersecurity issues in process operations and supply chains was presented, followed by the integration of IT and OT into industrial practices, as well as integrated safety and cybersecurity solutions for safety-critical systems. The paper concluded with a discussion of future directions for academic research, vendor engagement, academia-industry dialogue, and educational needs.

Acknowledgements

We would like to thank Professor Helen Durand (Wayne State University), Professors Matthew Ellis and Nael El-Farra (University of California, Davis), Professor Victor Zavala (University of Wisconsin, Madison), Dr. Scarlett Chen (Google), Mrs. Connie McAda (Dow), and Mr. Atharva Suryavanshi, Mr. Matthew Tom and Mr. Fahim Abdullah (University of California, Los Angeles) for their research results and contributions to this manuscript. We would also like to gratefully acknowledge the financial support from the US National Science Foundation and the US Department of Energy.

References

AbdulRahman, S., H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal 8*, 5476–5497.

Agrawal, S. and J. Agrawal (2015). Survey on anomaly detection using data mining techniques. *Procedia Computer Science 60*, 708–713.

Albalawi, F., H. Durand, and P. D. Christofides (2017). Process operational safety using model predictive control based on a process safeness index. *Computers & Chemical Engineering 104*, 76–88.

Amin, S., X. Litrico, S. Sastry, and A. M. Bayen (2012). Cyber security of water scada systems—part i: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology 21*, 1963–1970.

Angeli, D., R. Amrit, and J. B. Rawlings (2011). On average performance and stability of economic model predictive control. *IEEE Transactions on Automatic Control 57*, 1615–1626.

Asghar, M. R., Q. Hu, and S. Zeadally (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks 165*, 106946.

Ashibani, Y. and Q. H. Mahmoud (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security 68*, 81–97.

Attiah, A., M. Chatterjee, and C. C. Zou (2018). A game theoretic approach to model cyber attack and defense strategies. In *Proceedings of IEEE International Conference on Communications*, Kansas City, MO, pp. 1–7.

Ayas, M. S. and S. M. Djouadi (2016). Undetectable sensor and actuator attacks for observer based controlled cyber-physical systems. In *Proceedings of 2016 IEEE Symposium Series on Computational Intelligence*, Athens, Greece, pp. 1–7.

Böröcz, M. et al. (2021). Critical infrastructure policy in the eu. *Strategic Impact 3*, 46–61.

Buczak, A. L. and E. Guven (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials 18*, 1153–1176.

Cárdenas, A. A., S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry (2011). Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, pp. 355–366.

Chen, S., Z. Wu, and P. D. Christofides (2020a). Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control. *Computers & Chemical Engineering 136*, 106806.

Chen, S., Z. Wu, and P. D. Christofides (2020b). A cyber-secure control-detector architecture for nonlinear processes. *AIChE Journal 66*, e16907.

Chen, S., Z. Wu, and P. D. Christofides (2021). Cyber-security of centralized, decentralized, and distributed control-detector architectures for nonlinear processes. *Chemical Engineering Research and Design 165*, 25–39.

Cheung, K. and M. G. H. Bell (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research 291*, 471–481.

Cheung, K., M. G. H. Bell, and J. Bhattacharjya (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review 146*, 102217.

Christofides, P. D., J. F. Davis, N. H. El-Farra, D. Clark, K. R. D. Harris, and J. N. Gipson (2007). Smart plant operations: Vision, progress and challenges. *AIChE Journal 53*, 2734–2741.

Christofides, P. D., R. Scattolini, D. M. de la Pena, and J. Liu (2013). Distributed model predictive control: A tutorial review and future research directions. *Computers & Chemical Engineering 51*, 21–41.

Colbert, E. J. M., A. Kott, and L. P. Knachel (2020). The game-theoretic model and experimental investigation of cyber wargaming. *The Journal of Defense Modeling and Simulation 17*, 21–38.

Darup, M. S., A. B. Alexandru, D. E. Quevedo, and G. J. Pappas (2021). Encrypted control for networked systems: An illustrative introduction and current challenges. *IEEE Control Systems Magazine 41*, 58–78.

Darup, M. S., A. Redder, I. Shames, F. Farokhi, and D. Quevedo (2017). Towards encrypted mpc for linear constrained systems. *IEEE Control Systems Letters 2*, 195–200.

Do, C. T., N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar (2017). Game theory for cyber security and privacy. *ACM Computing Surveys 50*, 1–37.

Durand, H. (2018). A nonlinear systems framework for cyberattack prevention for chemical process control systems. *Mathematics 6*, 169.

Durand, H. and M. Wegener (2020). Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods. *Mathematics 8*, 499.

Ellis, M., H. Durand, and P. D. Christofides (2014). A tutorial review of economic model predictive control methods. *Journal of Process Control 24*, 1156–1178.

Enayaty-Ahangar, F., L. A. Albert, and E. DuBois (2020). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions 53*, 182–198.

Gani, A., P. Mhaskar, and P. D. Christofides (2007). Fault-tolerant control of a polyethylene reactor. *Journal of Process Control 17*, 439–451.

Ghadge, A., M. Weiß, N. D. Caldwell, and R. Wilding (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal 25*, 223–240.

Ghimire, B. and D. B. Rawat (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal 9*, 8229–8249.

Goh, J., S. Adepu, M. Tan, and Z. S. Lee (2017). Anomaly detection in cyber-physical systems using recurrent neural networks. In *Proceedings of the 18th IEEE International Symposium on High Assurance Systems Engineering*, Singapore, pp. 140–145.

Heidarinejad, M., J. Liu, and P. D. Christofides (2012). Economic model predictive control of nonlinear process systems using lyapunov techniques. *AIChE Journal 58*, 855–870.

Hink, R. C. B., J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan (2014). Machine learning for power system disturbance and cyber-attack discrimination. In *Proceedings of the 7th International Symposium on Resilient Control Systems*, Denver, CO, pp. 1–8.

Huang, L., X. Nguyen, M. Garofalakis, J. M. Hellerstein, M. I. Jordan, A. D. Joseph, and N. Taft (2007). Communication-efficient online detection of network-wide anomalies. In *Proceedings of 26th IEEE International Conference on Computer Communications*, Barcelona, Spain, pp. 134–142.

Iaiani, M., A. Tugnoli, S. Bonvicini, and V. Cozzani (2021). Analysis of cybersecurity-related incidents in the process industry. *Reliability Engineering & System Safety 209*, 107485.

Junejo, K. N. and J. Goh (2016). Behaviour-based attack detection and classification in cyber physical systems using machine learning. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, Xi'an, China, pp. 34–43.

Khan, L. U., W. Saad, Z. Han, E. Hossain, and C. S. Hong (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials 23*, 1759–1799.

Kim, J., J. Kim, H. L. T. Thu, and H. Kim (2016). Long short term memory recurrent neural network classifier for intrusion detection. In *Proceedings of the International Conference on Platform Technology and Service*, Jeju, Korea, pp. 1–5.

Kogiso, K. and T. Fujita (2015). Cyber-security enhancement of networked control systems using homomorphic encryption. In *Proceedings of the 54th IEEE Conference on Decision and Control*, Osaka, Japan, pp. 6836–6843.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy 41*, 1027–1038.

Li, T., A. K. Sahu, A. Talwalkar, and V. Smith (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine 37*, 50–60.

McFall, C. W., A. Bartman, P. D. Christofides, and Y. Cohen (2008). Control and monitoring of a high recovery reverse osmosis desalination process. *Industrial & Engineering Chemistry Research 47*, 6698–6710.

Mhaskar, P., C. McFall, A. Gani, P. D. Christofides, and J. F. Davis (2008). Isolation and handling of actuator faults in nonlinear systems. *Automatica 44*, 53–62.

Mohanty, S. R., A. K. Pradhan, and A. Routray (2007). A cumulative sum-based fault detector for power system relaying application. *IEEE Transactions on Power Delivery 23*, 79–86.

Müller, M. A., D. Angeli, and F. Allgöwer (2013). Economic model predictive control with self-tuning terminal cost. *European Journal of Control 19*, 408–416.

Muniraj, D. and M. Farhood (2019). Detection and mitigation of actuator attacks on small unmanned aircraft systems. *Control Engineering Practice 83*, 188–202.

Narasimhan, S., N. H. El-Farra, and M. J. Ellis (2022a). Active multiplicative cyberattack detection utilizing controller switching for process systems. *Journal of Process Control,* in press.

Narasimhan, S., N. H. El-Farra, and M. J. Ellis (2022b). Detectability-based controller design screening for processes under multiplicative cyberattacks. *AIChE Journal 68*, e17430.

Narasimhan, S., N. H. El-Farra, and M. J. Ellis (2022c). Minimizing false alarms in switching-enabled active multiplicative cyberattack detection. *Submitted*.

National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity (version 1.1). Technical report, National Institute of Standards and Technology.

Nieman, K., H. C. Oyama, M. Wegener, and H. Durand (2020). Predict the impact of cyberattacks on control systems. *Chemical Engineering Progress 116*, 52–57.

Ohran, B. J., D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis (2008). Enhancing data-based fault isolation through nonlinear control. *AIChE Journal 54*, 223–241.

Ohran, B. J., J. Rau, P. D. Christofides, and J. F. Davis (2008). Plantwide fault isolation using nonlinear feedback control. *Industrial & Engineering Chemistry Research 47*, 4220–4229.

Omar, S., A. Ngadi, and H. H. Jebur (2013). Machine learning techniques for anomaly detection: an overview. *International Journal of Computer Applications 79*, 33–41.

Oyama, H. and H. Durand (2020). Integrated cyberattack detection and resilient control strategies using Lyapunov-based economic model predictive control. *AIChE Journal 66*, e17084.

Oyama, H., D. Messina, R. O'Neill, S. Cherney, M. Rahman, K. K. Rangan, G. Gjonaj, and H. Durand (2022). Test methods for image-based information in next-generation manufacturing. In *Proceedings of the IFAC Symposium on Dynamics and Control of Process Systems, including Biosystems*, Busan, Republic of Korea.

Oyama, H., D. Messina, K. K. Rangan, and H. Durand (2022). Lyapunov-based economic model predictive control for detecting and handling actuator and simultaneous sensor/actuator cyberattacks on process control systems. *Frontiers in Chemical Engineering 4*, 810129.

Oyama, H., K. K. Rangan, and H. Durand (2021). Handling of stealthy sensor and actuator cyberattacks on evolving nonlinear process systems. *Journal of Advanced Manufacturing and Processing 3*, e10099.

Ozay, M., I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor (2015). Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems 27*, 1773–1786.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques*, Prague, Czech Republic, pp. 223–238. Springer.

Perez, H. D., S. Amaran, E. Erisen, J. M. Wassick, and I. E. Grossmann (2021). Optimization of extended business processes in digital supply chains using mathematical programming. *Computers & Chemical Engineering 152*, 107323.

Rangan, K. K., J. Abou Halloun, H. Oyama, S. Cherney, I. Azali Assoumani, N. Jairazbhoy, H. Durand, and S. K. Ng (2022). Quantum computing and resilient design perspectives for cybersecurity of feedback systems. In *Proceedings of the IFAC Symposium on Dynamics and Control of Process Systems, including Biosystems*, Busan, Republic of Korea.

Rangan, K. K., H. Oyama, and H. Durand (2021). Integrated cyberattack detection and handling for nonlinear systems with evolving process dynamics under Lyapunov-based economic model predictive control. *Chemical Engineering Research and Design 170*, 147–179.

Rangan, K. K., H. Oyama, and H. Durand (2022). Actuator cyberattack handling using Lyapunov-based economic model predictive control. In *Proceedings of the IFAC Symposium on Dynamics and Control of Process Systems, including Biosystems*, Busan, Republic of Korea.

Satchidanandan, B. and P. R. Kumar (2016). Dynamic watermarking: Active defense of networked cyber-physical systems. *Proceedings of the IEEE 105*, 219–240.

Shon, T. and J. Moon (2007). A hybrid machine learning approach to network anomaly detection. *Information Sciences 177*, 3799–3821.

Smetana, S., K. Aganovic, and V. Heinz (2021). Food supply chains as cyber-physical systems: a path for more sustainable personalized nutrition. *Food Engineering Reviews 13*, 92–103.

Sobb, T., B. Turnbull, and N. Moustafa (2020). Supply chain 4.0: a survey of cyber security challenges, solutions and future directions. *Electronics 9*, 1864.

Sun, C., A. Hahn, and C. Liu (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems 99*, 45–56.

Taylor, P. J., T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. R. Choo (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks 6*, 147–156.

Tsai, C. F., Y. F. Hsu, C. Y. Lin, and W. Y. Lin (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications 36*, 11994–12000.

Tsvetanov, T. and S. Slaria (2021). The effect of the colonial pipeline shutdown on gasoline prices. *Economics Letters 209*, 110122.

Vinayakumar, R., K. P. Soman, and P. Poornachandran (2017). Applying convolutional neural network for network intrusion detection. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, Udupi, India, pp. 1222–1228.

Wu, Z., F. Albalawi, J. Zhang, Z. Zhang, H. Durand, and P. D. Christofides (2018). Detecting and handling cyber-attacks in model predictive control of chemical processes. *Mathematics 6*, 173.

Wu, Z., S. Chen, D. Rincon, and P. D. Christofides (2020). Post cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design 159*, 248–261.

Wu, Z. and P. D. Christofides (2021). *Process Operational Safety and Cybersecurity*. Springer.

Wu, Z., H. Durand, and P. D. Christofides (2018a). Safe economic model predictive control of nonlinear systems. *Systems & Control Letters 118*, 69–76.

Wu, Z., H. Durand, and P. D. Christofides (2018b). Safeness index-based economic model predictive control of stochastic nonlinear systems. *Mathematics 6*, 69.

Zhang, F., H. Kodituwakku, J. W. Hines, and J. Coble (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics 15*, 4362–4369.

Zhang, Z., Z. Wu, D. Rincon, C. Garcia, and P. D. Christofides (2019). Operational safety of chemical processes via safeness-index based MPC: Two large-scale case studies. *Computers & Chemical Engineering 125*, 204–215.

Zhu, Q., H. Tembine, and T. Başar (2010). Network security configurations: A nonzero-sum stochastic game approach. In *Proceedings of the American Control Conference*, Baltimore, Maryland, pp. 1059–1064.