7-31-2019

Process/Equipment Design Implications for Control System Cybersecurity

Helen Durand
Wayne State University, helen.durand@wayne.edu

PROCESS/EQUIPMENT DESIGN IMPLICATIONS FOR CONTROL SYSTEM CYBERSECURITY

Helen Durand *

Wayne State University
Detroit, MI 48202

Abstract

An emerging challenge for process safety is process control system cybersecurity. An attacker could gain control of the process actuators through the control system or communication policies within control loops and potentially drive the process state to unsafe conditions. Cybersecurity has traditionally been handled as an information technology (IT) problem in the process industries. In the literature for cybersecurity specifically of control systems, there has been work aimed at developing control designs that seek to fight cyberattacks by either giving the system appropriate response mechanisms once attacks are detected or seeking to make the attacks difficult to perform. In this work, we begin an exploration into the implications of process and equipment design for enhancing the ability of chemical processes to maintain safe operation during cyberattacks on the process control systems.

Keywords
Process control, process design, cybersecurity, process operational safety.

Introduction

Significant research work with regard to enhancing process operational safety through control design has appeared in recent years (e.g., Albalawi et al. [2018]). In these recent works, safety issues can occur due to a variety of causes, such as large disturbances Zhang et al. [2018]. Safety incidents which can be caused by cyberattacks on control systems have also received focus recently Wu et al. [2018]. Cybersecurity breaches of process control systems at chemical processing facilities could create significant safety hazards for plant workers and residents of communities around such processing facilities. A traditional approach to preventing cyberattacks from causing safety issues at chemical plants is to augment IT defenses (by, for example, employing firewalls and applying software patches) to reduce the ability of attackers to impact process safety. However, IT defenses have limitations and are not guaranteed to prevent cyberattacks from being successful. Solutions which modify the communication/networking channels in control loops so that they are not susceptible to cyberattacks could form a part of the solution; however, the trend in the chemical process industries away from more secure wired communication to wireless communication indicates that cybersecurity solutions which are cumbersome and prevent companies from taking advantage of advances in computing are not the options of interest to industry. Despite the high stakes involved in cyberattacks (i.e., the potential for an attack to cause the deaths of many plant workers and community members), the direction to pursue to make plants cyberattack-resilient within a framework that is attractive to industry is not currently clear. Recent advances with respect to preventing control system cyberattacks from succeeding have focused on cyberattack detection Satchidanandan and Kumar [2017] and also control of systems during attacks Zhu and Başar [2015].

In a recent work Durand [2018], we have defined cyberattack-resilience of a control system in a nonlinear systems framework to mean that there exist no inputs which can drive the closed-loop state out of the set of safe operating conditions. Developing viable processes which meet this definition, if it is possible, will require more than control system advances. In the remainder of this work, we begin an analysis of the role of process and equipment design in realizing operational safety in the face of cyberattacks.

Preliminaries

Notation

The notation $|\cdot|$ signifies the Euclidean norm of a vector. x^T signifies the transpose of a vector x. We define $t_k = k\Delta$, where Δ refers to the sampling period and $k = 0, 1, \ldots$. $diag(x)$ represents a matrix with the components of the vector x on its diagonal.

Class of Systems

We consider classes of process systems of the form:

$$\dot{x} = f(x, u, w) \tag{1}$$

*To whom all correspondence should be addressed, Email: *helen.durand@wayne.edu*.

where $x \in X \subset R^n$ represents the process state vector, $u \in U \subset R^m$ represents the process input vector, and $w \in W \subset R^z$ represents the vector of bounded process disturbances (i.e., $W := \{w \in R^z | \, |w| \leq \theta, \theta > 0\}$). f is a nonlinear, locally Lipschitz vector function of its arguments. We consider that $f(0,0,0) = 0$ and that X is the set of safe states (i.e., if $x \in X$, $\forall \, t \geq 0$, no process incidents occur).

Model Predictive Control

Model predictive control (MPC) is an optimization-based control design which solves the following optimization problem at every sampling time t_k:

$$\min_{u(t) \in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau)) \, d\tau \tag{2a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{2b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2c}$$

$$\tilde{x}(t) \in X, \, \forall \, t \in [t_k, t_{k+N}) \tag{2d}$$

$$u(t) \in U, \, \forall \, t \in [t_k, t_{k+N}) \tag{2e}$$

In Eq. (2), $u(t) \in S(\Delta)$ signifies that the input trajectory is a vector of piecewise-constant inputs held for periods Δ. The stage cost $L_e(x,u)$ is optimized (Eq. (2a)) subject to the nominal ($w \equiv 0$) dynamic model of Eq. (2b), the state measurement of Eq. (2c), the state constraint of Eq. (2d), and the input constraint of Eq. (2e).

On the Role of Design in Preventing Cyberattack Success

In this section, we demonstrate conceptually that the success of cyberattacks on process control systems cannot be fully prevented at the control design level, but that process design, as well as equipment design and selection, have the potential to prevent certain attack types which could jeopardize alternative designs from succeeding. We utilize a numerical example and a process example involving two continuous stirred tank reactors (CSTR's) and a separator to aid in clarifying and drawing several conclusions with respect to the role of design in preventing the success of cyberattacks on process control systems. Throughout this work, we consider cyberattack-resilience to mean that no safety issues occur during a cyberattack (i.e., $x(t) \in X$, $t \geq 0$, even under a cyberattack).

The Inadequacy of Control Laws for Preventing Safety Issues Arising from Cyberattacks

Cyberattacks may target a variety of communication channels within feedback control loops, including the communication between the sensors and controller, and also between the controller and the actuators. Attacks of the latter type bypass controllers in a feedback loop completely and therefore cannot be stopped by adjusting the control system design. In Durand [2018], we explored several different MPC designs with respect to whether they are resilient to cyberattacks in which false state measurement information was provided to the MPC's at each sampling time. A case in which cyberattack-resilience of a control system against sensor measurement falsification is achieved is in the case that the operating steady-state is open-loop stable, such that the open-loop stable input (which is independent of feedback and therefore independent of the process sensors) can be utilized to drive the closed-loop state to the steady-state regardless of whether an attacker can modify the sensor readings or not. The fact that the success of this approach relies on a lack of feedback indicates that it is difficult to conceive of control designs which utilize feedback but do not produce problematic inputs when state measurements are falsified. Another concept that has been explored for utilizing controllers in preventing cyberattacks from being successful has involved controller or instrumentation reconfiguration after an attack is detected. A difficulty with this approach is that detection of the attack, a pre-requisite to switching to a control strategy which maintains safe operation during the attack, requires some expectation of what the attacks will target, so that metrics related to the expected target can be monitored. Given the complexity of large-scale chemical plants and interactions between units, determining all of the types of attack targets may be difficult. In conclusion, there are many methods for evading control-focused efforts for preventing safety issues due to cyberattacks.

The Roles of Process Design and Equipment Design in Preventing Safety Issues Arising from Cyberattacks

Despite that control designs are not expected to be capable of preventing safety incidents in various cyberattack scenarios, appropriate process designs and equipment designs may aid in preventing the success of cyberattacks. At this point, it is not clear how conservative designs may need to be to prevent the success of cyberattacks. In this work, however, we do not focus on design conservatism, but rather on elucidating the manner in which process and equipment designs relate to the success or failure of cyberattacks.

To demonstrate that process designs can play a key role in preventing the success of cyberattacks, consider a vessel in which a runaway reaction could occur (e.g., Zhang et al. [2018]), causing the pressure in the vessel to build up such that an explosion takes place if sufficient cooling is not provided. One could imagine that if the coolant flow rate were a manipulated input, a cyberattacker might seek to gain control of this input and then set it artificially low so that the appropriate cooling is not provided as the reaction takes place. If this were to result in an increase in pressure in the vessel, but the vessel were instrumented with a safety relief valve, the attack may not be able to create an explosion.

With regard to equipment design/selection, the majority of attacks intended to impact process safety which can be conceived are intended to impact process equipment fidelity, including the situation in the above paragraph in which a runaway reaction is initiated with the intent of compromising the reactor vessel. A successful cyberattack on the control system in a uranium enrichment plant in Iran via the Stuxnet worm was also geared toward compromising equipment (it spun centrifuges at the plant at speeds that damaged them Fidler [2011]). One of the challenges with respect to analyzing equipment fidelity for chemical processes under at-

tacks is that there are many mechanisms of failure of equipment Dowling [2013], and equipment is typically designed to withstand expected loading during operation. Cyberattacks may create unexpected loading for which the equipment was not designed; however, determining all of the types of unexpected loading to which equipment might be subjected via rogue control actions can be challenging.

In the following sections, we present a numerical example that illustrates the concept of designing equipment to be cyberattack-resilient. Subsequently, we analyze a chemical process example that suggests initial steps for characterizing whether a process/equipment design inhibits cyberattack success or not.

Cybersecurity and Process Equipment Design: A Numerical Example

In this section, we provide a numerical example to illustrate the concept that equipment designs might be selected to prevent certain cyberattacks from being successful. The example is based on a case study from Durand [in press] in which a continuous stirred tank reactor (CSTR) is followed by a section of process piping that is rigidly fixed on the end that is closest to the CSTR outlet and has a bellows joint on the opposite end, with spring constant k_s. The following dynamic model describes the manner in which the concentration of the reactant A (which is converted to B in the CSTR) and temperature T in the reactor change over time as the values of inlet reactant concentration C_{A0} and heat rate Q are modified:

$$\dot{C}_A = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{-\frac{E}{R_g T}} C_A^2 \tag{3}$$

$$\dot{T} = \frac{F}{V}(T_0 - T) - \frac{\Delta H k_0}{\rho_L C_p} e^{-\frac{E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{4}$$

where F, V, k_0, E, R_g, ΔH, ρ_L, and C_p represent, respectively, the flow rate into and out of the CSTR, the CSTR volume, the pre-exponential constant, the activation energy of the reaction, the ideal gas constant, the enthalpy of reaction, the liquid density, and the heat capacity of the liquid in the CSTR. The values of the parameters can be found in Durand [in press].

The piping element has a yield strength of 270 MPa, a thermal expansion coefficient of 12.5×10^{-6} K^{-1}, a Young's Modulus of 200 GPa, and a cross-sectional area $A = 0.002041$ m^2 Barron and Barron [2012]. A safety factor of 2.7 is used in setting the design stress (which is set to 10^8 Pa and is the value of the stress which it is desired that the stress in the pipe not exceed). Consider that the initial materials selection for the CSTR allows the CSTR to withstand temperatures up to 400 K above the operating steady-state temperature, but that the initial design for the piping uses an unusually stiff bellows joint with $k_s = 5.5 \times 10^7$ N/m. With this bellows joint, the stress in the piping element will exceed the design stress if the temperature of the piping exceeds about 11.8 K above the steady-state value T_s of the temperature of the CSTR outlet. We consider that the piping is insulated such that it could reach these high temperatures if the temperature of the fluid exiting the CSTR exceeds T_s by 11.8 K and remains at that temperature long enough for the pipe temperature to also exceed 11.8 K above T_s. Furthermore, it will yield (exceeding the yield strength will be considered undesirable for the part in this example) if the temperature of the pipe wall exceeds T_s by about 278 K. The controller for the CSTR is an MPC which promotes steady-state operation with bounds on C_{A0} between 0.5 and 7.5 kmol/m^3 and on Q between -5×10^5 and 5×10^5 kJ/h, with a stage cost as follows:

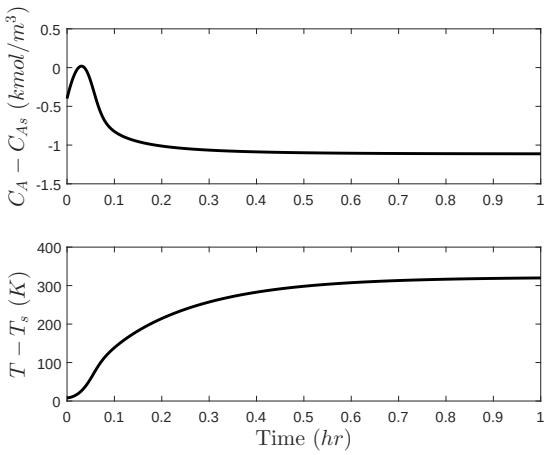

Figure 1. States over one hour of operation for the process of Eqs. (3)-(4) *under EMPC with a sensor attack.*

$$\begin{aligned} L_e =& 100(C_A - C_{As})^2 + (T - T_s)^2 \\ &+ (C_{A0} - C_{A0s})^2 + 10^{-10}(Q - Q_s)^2 \end{aligned} \tag{5}$$

The controller parameters are $N = 10$ and $\Delta = 0.01$ h. The optimization problem of the MPC was solved using MATLAB's function fmincon. The process of Eqs. (3)-(4) is simulated under this controller with an integration step of 10^{-4} h, and in the absence of an attack, the closed-loop state is driven to the steady-state with $C_A = C_{As}$, $T = T_s$, $C_{A0} = C_{A0s}$, and $Q = Q_s$ from an initial condition at $C_A - C_{As} = -0.4$ kmol/m^3 and $T - T_s = 8$ K. If an attack is performed that provides, for example, the same false state measurement at every sampling time for 100 sampling times of $C_A(t_k) = 0.05$ kmol/m^3 and $T(t_k) = 440$ K, then the trajectory in Fig. 1 is obtained. In this case, the temperature of the fluid leaving the CSTR exceeds its steady-state value by 320 K. If the piping element comes to equilibrium with the fluid temperature at this condition, then the stress in the pipe will be beyond that required to cause yielding. This occurs even though the material from which the CSTR itself is made is able to withstand the high temperature in the CSTR.

If the fact that the piping could be compromised by the proposed cyberattack was discovered before construction of the equipment through numerical simulations, one technique for preventing the cyberattack described from causing failure of the piping would be to select a less stiff bellows joint. For example, if the bellows joint was selected to have $k_s = 4.4 \times 10^5$ N/m (noted by Barron and Barron [2012] to be a more typical value of spring bellows constants), the temperature of the pipe would need to be about 39,410 K above T_s,

a case which would never be expected in practice, before the yield strength would be reached. With that spring constant, if an attack is performed on the MPC in which $C_A(t_k) = 0.05$ kmol/m^3 and $T(t_k) = 440$ K at every sampling period, then neither the maximum temperature allowable in the CSTR or in the piping is exceeded in the one hour of operation according to Fig. 1. As a steady-state temperature (different from T_s) appears to have been reached by the end of one hour of operation in Fig. 1, one could conclude that the equipment design is now resilient against the specific cyberattack in which $C_A(t_k) = 0.05$ kmol/m^3 and $T(t_k) = 440$ K at every sampling time.

To determine whether this new equipment design is cyberattack-resilient against any cyberattacks which could be performed, one could begin testing various types of attacks to see whether any of them appears to be capable of compromising the equipment. For example, if instead an attack is performed in which $T(t_k) = 430$ K, then the temperature at the CSTR outlet becomes 547 K above its steady-state value after 1 h of operation. This temperature is now lower than the temperature at which the piping element would exceed the yield strength, but is now higher than the temperature which could cause failure of the CSTR. Though one could again modify the equipment design to prevent failure of the CSTR in this attack scenario (perhaps modifying the material from which the CSTR is constructed), the process of trying an attack, assessing the outcome, and modifying equipment accordingly is not straightforward. It lacks a systematic methodology for generating attack scenarios to be used in testing the equipment fidelity. It may be difficult to postulate every possible attack and how it may impact equipment, as attacks may be of various types (e.g., they may not only be those in which the sensor measurement is fixed at every sampling time, but may change between sampling times and operate a process in a dynamic fashion). This means that even material failure mechanisms which are related to dynamic behavior (e.g., fatigue) may also need to be considered.

This example has been numerically constructed (with some liberty taken in selecting equipment designs and allowable maximum temperatures in the equipment that would not be expected to be appropriate in practice) to illustrate the concept that equipment designs can play a role in the success of cyberattacks, and that clever equipment designs may prevent some attacks that would otherwise compromise equipment from being able to do so. It also clarifies that: 1) determining how attacks might impact equipment may be difficult given the many different failure mechanisms of materials and the many different types of attacks which could be performed to make the various failure mechanisms relevant and 2) at a large-scale plant with connected units and coupled process dynamics, attacks might be deployed which modify inputs to one unit to seek to cause failure in another that is, perhaps, downstream (this is shown in the case of the first attack examine above, where when $k_s = 5.5 \times 10^7$ N/m, the changes in the manipulated inputs which directly impact the states of the process fluid in the CSTR are utilized not to cause failure of the CSTR, but to impact the downstream piping). The fact that some level of analysis of the ability of the equipment to withstand cyberattacks is demonstrated to be achievable in this example suggests that that the potential of equipment or process designs to withstand cyberattacks may be a worthwhile consideration during process hazard analysis.

Cyberattacks and Process Design: A Chemical Process Example

In the process example in this section, we move from investigating the impacts of equipment design on cybersecurity to investigating the impacts of process design. To do so, we consider the process example from Lao et al. [2013] in which two CSTR's in series are followed by a flash drum. CSTR's 1 and 2 (Vessels 1 and 2, respectively) receive fresh feed of the reactant A at concentrations C_{A10} and C_{A20} at flow rates F_{10} and F_{20}, respectively. The first CSTR also receives a recycle stream of condensed vapor from the overhead of the flash drum (Vessel 3) at flow rate F_r. The product stream F_3 is the liquid condensed in the flash drum. Heat is supplied or removed from CSTR 1, CSTR 2, and the flash drum at rates Q_1, Q_2, and Q_3, respectively. The model equations and parameters are those in Lao et al. [2013], with a slight change to the equations representing the concentrations C_{Ar}, C_{Br}, and C_{Cr} of species A, B, and C in the recycle stream (where B is the desired product produced from A, and C is an undesired byproduct) as follows:

$$C_{jr} = \frac{\alpha_j C_{j3}}{K_d},\ j = A, B, C, D \tag{6}$$

where D is an inert material, α_j is the relative volatility of species j at the conditions in the flash drum, and C_{ji}, $i = 1, 2, 3$, is the concentration of species j in the liquid in Vessel i. K_d is computed as follows:

$$K_d = [\sum_{j=A}^{C} \frac{\alpha_j C_{j3}}{\rho_M}] + \alpha_D \frac{\rho - \sum_{j=A}^{C} C_{j3} MW_j}{M_{WD}\rho_M} \tag{7}$$

where

$$\rho_M = \frac{\rho - [\sum_{j=A}^{C} C_{j3} M_{Wj}]}{M_{WD}} + [\sum_{j=A}^{C} C_{j3}] \tag{8}$$

where ρ is the density of the liquid in the flash drum, ρ_M is the molar density (assumed for ease of modeling to be the same for the liquid and vapor) in the flash drum, and M_{Wj} is the molecular weight of species j. Two steady-states of the process will be of interest in the studies below for the state vector $\bar{x} = [T_1\ C_{A1}\ C_{B1}\ C_{C1}\ T_2\ C_{A2}\ C_{B2}\ C_{C2}\ T_3\ C_{A3}\ C_{B3}\ C_{C3}]^T$, where T_i is the temperature in Vessel i: an open-loop unstable steady-state $\bar{x}_u = [370.22\ 3.29\ 0.17\ 0.042\ 435.32\ 2.74\ 0.45\ 0.11\ 435.15\ 2.88\ 0.50\ 0.12]^T$ and an open-loop stable steady-state $\bar{x}_s = [300.97\ 3.55\ 0.0035\ 0.00050\ 300.78\ 3.32\ 0.0029\ 0.00041\ 300.61\ 3.50\ 0.0033\ 0.00044]^T$ (stability or instability was assumed from open-loop simulations). The steady-state values of the process manipulated inputs Q_1, Q_2, Q_3, and $\Delta F_{20} = (F_{20} - 5)$ m^3/h are zero. The CSTR is operated under an MPC where the lower and upper bounds on each heat rate input are -1×10^6 and 1×10^6 kJ/h,

respectively, and the upper and lower bounds on ΔF_{20} are -5 and 5 m^3/h. The stage cost is

$$L_e = 10^5((\bar{x} - \bar{x}_q)P(\bar{x} - \bar{x}_q)^T + 5 \times 10^{-12}Q_1^2 + 5 \times 10^{-12}Q_2^2 + 5 \times 10^{-12}Q_3^2 + 100\Delta F_{20}^2) \quad (9)$$

where q is either u or s, depending on whether the process is to be operated around the stable or unstable steady-state, and $P = diag(20, 10^3, 10^3, 10^3, 10, 10^3, 10^3, 10^3, 10, 10^3, 10^3, 10^3)$. The process model is integrated with an integration step size of 10^{-5} h. It is operated for one hour with $N = 6$ and $\Delta = 0.005$ h. The MATLAB function fmincon is utilized in solving the optimization problem.

We now analyze how two attacks on this process play out differently to gain insights into how design impacts cybersecurity. Fig. 2 shows the results when an MPC which incorporates a model of the three-unit process in Eq. (2b) and has $q = u$ in Eq. (9) is used to control the process with recycle when it is initialized from $x_I = \bar{x}_q + [10\ 0.5\ -0.001\ -0.0001\ -10\ 0.5\ -0.001\ -0.0001\ 10\ 0.5\ -0.001\ -0.0001]^T$ with $q = u$, but the false state measurement x_{F1} provided at every sampling time is $\bar{x}_u$. By providing the MPC with a state measurement corresponding to the operating steady-state, the MPC is tricked into computing the steady-state control action, as this is the control action that we would like it to compute if, in reality, the process state is at the steady-state. Because the steady-state at which we would like to stabilize the closed-loop state is open-loop unstable, when the inputs are fixed at the steady-state values by the MPC but the process state is not at $\bar{x}_u$, the closed-loop state does not approach $\bar{x}_u$ but instead approaches a different (stable) steady-state with problematically high temperatures in the various units. The steady-state input provided by the MPC is thus insufficient for driving the closed-loop state back to $\bar{x}_u$ during the attack. An important point about this attack is that despite the fact that the system dynamics in this case are more complex than those in, for example, Eqs. (3)-(4), due to the multiple interconnected units and recycle, applying the steady-state input corresponding to an open-loop unstable steady-state when the closed-loop state is not initialized at that steady-state is an easy-to-recognize attack strategy. It is also easy to figure out how to achieve with the control design at hand, because it is well-known that an MPC designed to track a steady-state will compute the steady-state input if the state measurement is at the steady-state. This implies: 1) there may be some attacks which can be readily identified during certain hazard assessments if criteria for recognizing these attacks (e.g., false state measurements which lead to open-loop unstable steady-state control inputs being applied to a process when it is off the steady-state) are developed, and then the process can be protected against such attacks via strategies in process/equipment design or detection/controller reconfiguration and 2) the fact that the process dynamics are coupled, large-scale, or complex does not necessarily mean that it is difficult for an attacker to locate a method for successfully bringing the plant to an unsafe condition.

Now consider that this same process is operated around the stable steady-state (i.e., $q = s$ in the above problem formulation). In this case, the same type of cyberattack (i.e., $\bar{x}_s$ is the falsified input at every sampling time) does not succeed in causing a safety concern, because it causes the MPC to compute open-loop stable inputs that drive the closed-loop state to the open-loop stable steady-state. From a nonlinear systems perspective, if there are multiple steady-states (as in this example) for a given set of inputs, the set of initial states around $\bar{x}_s$ from which the steady-state input might be applied and the closed-loop state would be driven to the origin is not R^n. This suggests a (computationally-laborious) mechanism for anticipating some of the conditions which might be set up under a cyberattack on the process state measurements that maintains these falsified sensor values constant throughout the time of the attack. Specifically, for MPC, a characteristic of attacks that present the same falsified state measurement at every sampling time is that the MPC will compute the same input at every sampling time. To analyze whether there exist significant concerns with respect to a process and/or equipment design being susceptible to a cyberattack, a technique that could be attempted would be to discretize the input space between the input bounds as well as the state space and then determine, for each point in the state-space, all steady-states which can be found to be associated with each input combination in the input space. Subsequently, the worst-case scenarios revealed by this analysis could be analyzed to determine whether they indicate that problematic conditions are likely to occur or not, and if so, how equipment or process design might be adjusted to modify that. Despite the fact that this technique does not explore dynamic behavior which may be set up by cyberattacks and that it is likely to be computationally intractable with full process models, it suggests the beginnings of a systematic approach to characterizing whether a process is cyberattack-resilient.

The analysis with respect to the two cyberattacks on the CSTR-CSTR-flash drum process as detailed above also provides insight into how cyberattacks should and should not be understood. For example, the heat inputs applied at every sampling time in Fig. 2 are zero, and yet the temperatures in

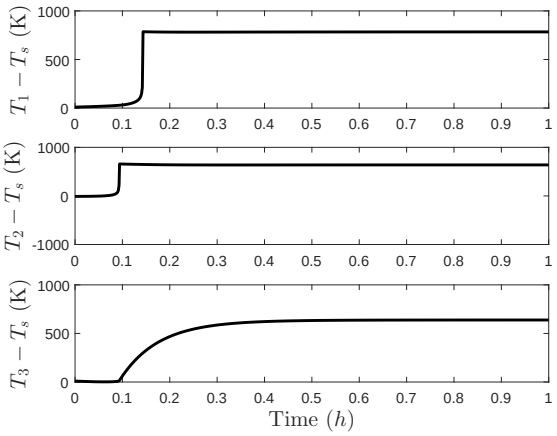

Figure 2. T_1, T_2, and T_3 over 1 h of operation for the 2 CSTR-flash drum process under a cyberattacked EMPC provided the false state measurement x_{F1}.

every vessel increased significantly because the initial condition was one in which the reactant A was present in the two CSTR's and converted to the products with no heat removed from the vessel as the exothermic reactions took place. The reason that that cyberattack succeeds is a combination of the initial condition and how the inputs applied from the process condition drive it to an unsafe operating condition by taking advantage of the physics of the process. The manner in which attacks succeed is not the result only of the inputs which the attacker applies (e.g., it is not necessarily true that Q_1 must become large for T_1 to become large), but of the direction in which these inputs drive the process given the process state when the actions begin to be applied. As noted in Durand [2018], the results of attacks may be difficult to predict in many cases, as the results would be state trajectories for coupled nonlinear systems under various input trajectories.

An important question which remains to be addressed for the example above is how the design might be modified in light of the realization that a cyberattack could be easily performed on the system. Part of the reason why the cyberattack can be easily performed is that the desired operating conditions correspond to an unstable steady-state for the system. The steady-state is unstable due to the process dynamics. An interesting future research direction could be exploring techniques for modifying designs while maintaining the operating steady-state as a process steady-state (but perhaps modifying its stability). One could also consider adding safety systems Ahooyi et al. [2016] which are physically activated when the conditions of the process reach certain values, before an unsafe but stable steady-state is reached, essentially using a strategy which switches the process dynamics automatically when the inputs are not as expected, in an attempt to cause the modified dynamics to prevent the safety issues. Selecting equipment that results in tighter input bounds might also be an option. It would be expected that equipment with more significant limitations (i.e., smaller ranges of allowable inputs) would prevent the worst-case scenarios from deviating too much from the steady-state conditions. However, small ranges for the allowable inputs may negatively impact the ability of the control system to be flexible and to reject disturbances. In summary, techniques are needed for considering designs and changes in designs within a dynamic systems framework.

Conclusions

This work presented preliminary results in the direction of seeking to understand the extent to which cybersecurity of process control systems might be understood as a process and equipment design problem. The task of designing cyberattack-resilient systems for the process industries is challenging, and the solution is not likely to come from control design. It remains to be seen whether process and equipment design may provide a solution in many cases or if, like inherent safety Kletz and Amyotte [2010], it may be deemed a consideration for design rather than a condition of design if it requires significant conservatism that reduces the economic attractiveness of processes. Motivated by the fact that cyberattacks introduce transients even into processes which might otherwise be operated at steady-state, an interesting future direction could be to explore whether there may exist novel process and equipment designs that are not necessarily developed for a steady-state paradigm and which may allow for greater economic benefits with cyberattack-resilience beyond what can be achieved in traditional paradigms. It may also be interesting to consider the extent to which design-based cyberattack-resilience considerations might be extended to make processes resilient (from a process safety perspective) to actuator and sensor faults, as the techniques for developing resilience that have been described above are independent of sensor measurements and are related only to whether the actuator outputs are within their bounds, and not to the exact value that they take within their bounds.

Acknowledgments

Financial support from Wayne State University is gratefully acknowledged.

References

T. M. Ahooyi, M. Soroush, J. E. Arbogast, W. D. Seider, and U. G. Oktem. Model-predictive safety system for proactive detection of operation hazards. *AIChE Journal*, 62:2024–2042, 2016.

F. Albalawi, H. Durand, and P. D. Christofides. Process operational safety via model predictive control: Recent results and future research directions. *Computers & Chemical Engineering*, 114: 171–190, 2018.

R. F. Barron and B. R. Barron. *Design for Thermal Stresses*. John Wiley & Sons, Hoboken, New Jersey, 2012.

N. E. Dowling. *Mechanical Behavior of Materials: Engineering Methods for Deformation, Fracture, and Fatigue*. Pearson, Boston, Massachusetts, fourth edition, 2013.

H. Durand. A nonlinear systems framework for cyberattack prevention for chemical process control systems. *Mathematics*, 6: 44 pages, 2018.

H. Durand. On accounting for equipment-control interactions in economic model predictive control via process state constraints. *Chemical Engineering Research and Design*, in press.

D. P. Fidler. Was Stuxnet an act of war? Decoding a cyberattack. *IEEE Security & Privacy*, 9:56–59, 2011.

T. A. Kletz and P. Amyotte. *Process Plants: A Handbook for Inherently Safer Design*. CRC Press, 2010.

L. Lao, M. Ellis, and P. D. Christofides. Proactive fault-tolerant model predictive control. *AIChE Journal*, 59:2810–2820, 2013.

B. Satchidanandan and P. R. Kumar. Dynamic watermarking: Active defense of networked cyberphysical systems. *Proceedings of the IEEE*, 105:219–240, 2017.

Z. Wu, F. Albalawi, J. Zhang, Z. Zhang, H. Durand, and P. D. Christofides. Detecting and handling cyber-attacks in model predictive control of chemical processes. *Mathematics*, 6:22 pages, 2018.

Z. Zhang, Z. Wu, H. Durand, F. Albalawi, and P. D. Christofides. On integration of feedback control and safety systems: Analyzing two chemical process applications. *Chemical Engineering Research and Design*, 132:616–626, 2018.

Q. Zhu and T. Başar. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, 35:46–65, 2015.