MODEL-PREDICTIVE SAFETY SYSTEM FOR PREDICTIVE DETECTION OF OPERATION HAZARDS

Masoud Soroush[1*], Taha Mohseni Ahooyi[2], Jeffrey E. Arbogast[3] and Warren D. Seider[4]

[1]Drexel University, Philadelphia, PA 19104
[2]Temple University, Philadelphia, PA 19122
[3]American Air Liquide, Newark, DE 19702
[4]University of Pennsylvania, Philadelphia, PA 19104

Abstract

This paper highlights the capability and potential of a recently-introduced method of designing model-predictive safety (MPS) systems (Mohseni Ahooyi et al., 2016). For the first time, the method proposed a systematic utilization of process models to generate *predictive* alarm signals (alerts) for the detection of present and future operation hazards (OHs) in real time. An MPS system uses a process model to project in real-time the process operability status and to generate alarm signal(s) indicating the presence of a current or future OH. It triggers alarm(s) in real time when the process is unable to satisfy an operability constraint over a moving time-horizon into the future. Unlike typical existing functional safety systems that generate *reactive*, *non-interacting* alarm signal(s) when a process variable exceeds a threshold, an MPS system generates *predictive* alarm signals that systematically account for process *nonlinearities* and *interactions*, and alert the process personnel to imminent and potential, present and future OHs. Although the method uses the concepts of moving-horizon, model-based prediction and state estimation, it does not deal with control at all. The performance of the system is shown using a polymerization reactor example.

Keywords

Model-predictive safety system, Predictive alerts, Process safety, Proactive methods, Functional Safety

Introduction

The safety of processes has been improving as a result of better instrumentation, hardware, and computer-based methods, as well as effective safety standards and regulations. In spite of these, over only the past decade more than 75 serious accidents have occurred according to the U.S. Chemical Safety and Hazard Investigation Board (http://www.csb.gov/). These accidents point to the need for further improvement in existing methods and the introduction of new methods that can enhance process safety (Leveson and Stephanopoulos, 2014; Mannan et al., 2015).

In a chemical, petrochemical, refining, or power-generation plant, two separate instrumentation systems exist: a control system and a safety instrumented system. The control system ensures that the process operates efficiently and produces high-quality products under normal operation. The safety instrumented system is employed to take automatic action to prevent personnel, environmental, or equipment damage consequences. Therefore, these systems are subject to higher levels of governmental and industrial regulation and oversight than the control systems. As Figure 1a shows, in a conventional hierarchical structure, an alarm system receives signals from the control system and safety instrumented system, and generates alarms to alert the process personnel to an existing abnormal condition. Further corrective actions may

[*] To whom all correspondence should be addressed

be taken by operators through operator inputs (OI) to the control system, the process directly, or both.

Despite significant advances in alarm system design and management (Wei et al., 2011; Schleburg et al., 2013; Kondaveeti et al., 2013), there are still challenges that need to be addressed. For example, alarms are often triggered when individual variables exceed their thresholds; typical conventional mechanisms by which existing safety and control systems trigger alarms are unable to account properly for interactions among variables, leading to an excessive number of false alarms. Furthermore, existing safety and control systems activate alarms that are *reactive*; i.e., they alert process personnel only to present operation hazards (identified from past and current measurements), which have already affected processes.

First-principles process models have been used widely in design, optimization, process monitoring, model-based control, and offline safety analysis and validation of chemical and petrochemical processes. These models predict steady-state and dynamic behaviors of the processes, based on recent and historical process data. Such models, validated with process data, indeed represent compact forms of process historical data. While they may not predict future process behavior accurately, they can be used to forecast potential future consequences. Such forecasts can lead to proactive actions whose consequences (outcomes) can be predicted. This combined predictive and proactive (prescriptive), real-time use of process models in process safety had not been explored until very recently (Mohseni Ahooyi et al., 2016).

The model-predictive safety (MPS) system design method (Mohseni Ahooyi, et al. 2016) represents a new paradigm in process safety; that is, the use of model predictions to detect operation hazards before they lead to safety risks. Figure 2 depicts an alternative hierarchical structure with an MPS system. Unlike conventional safety systems that are individually *reactive* to current conditions and specifically designed logic, the proposed MPS is a *smart* system that systematically accounts for process nonlinearities and interactions among process variables, and generates predictive alarm signals alerting process personnel to potential and imminent future operation hazards. Therefore, this new paradigm in functional safety systems is analogous to the previous evolution in process control systems from only single-loop control (e.g., PID) towards multivariable model-based control (e.g., MPC).

MPS System Design Method

The MPS system has two major components: a set of operability constraints and a state predictor, which is derived from a first-principles model of the process.

Process Model

A process model in the following general form is considered:

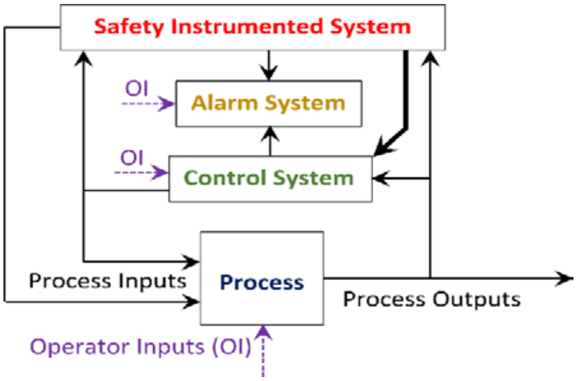

Figure 1. Typical conventional hierarchical structure for a control system, safety instrumented system, and alarm system in a process. The thicker black line represents override. (Mohseni Ahooyi et al., 2016)

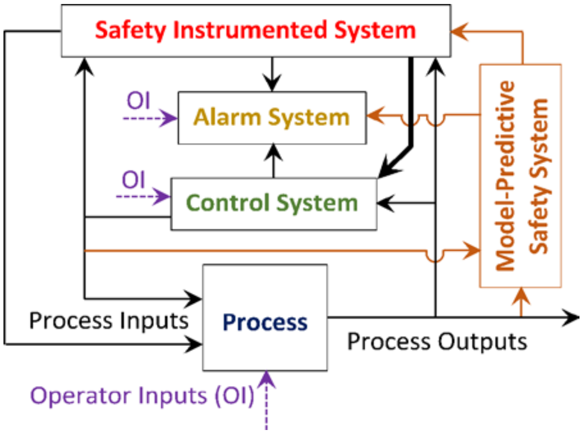

Figure 2. Hierarchical structure including the model-predictive safety system. The thicker black line represents override. (Mohseni Ahooyi et al., 2016)

$$\left.\begin{aligned} \frac{dx(t)}{dt} &= f\big(x(t), d(t), d_m(t), p(t), u(t)\big), \\ & \qquad x(0) = x_0 \in \Omega_{x_0} \subset \mathbb{R}^{n_x} \\ y(t) &= h\big(x(t)\big) \end{aligned}\right\} (1)$$

with the *operability* constraints:

$$G\big(x(t), d(t), d_m(t), p(t), u(t)\big) \in \Omega_c \subset \mathbb{R}^{n_c} \qquad (2)$$

where $x \in \Omega_x \subset \mathbb{R}^{n_x}$ is the vector of state variables of the process, $d \in \Omega_d \subset \mathbb{R}^{n_d}$ is the vector of unmeasured input variables, $d_m \in \Omega_{d_m} \subset \mathbb{R}^{n_{d_m}}$ is the vector of measured input (other than manipulated) variables, $p \in \Omega_p \subset \mathbb{R}^{n_p}$ is the vector of the process parameters, $u \in \Omega_u \subset \mathbb{R}^{n_u}$ is the vector of manipulated variables, and $y \in \Omega_y \subset \mathbb{R}^{n_y}$ is the vector of measured output variables. Parametric uncertainties are accounted for by defining a range for every quantity that is uncertain. Each range is set based on based on historical data, operation procedures, and/or process-personnel experience. The uncertain quantities can be initial conditions, operators' inputs, and process parameters.

Eq.(2) can include all process operability constraints such as individual upper and lower bounds on (i) input and output measured variables, such as temperatures, flow rates, and pressures; and (ii) *unmeasured* state variables, such as concentrations. G can include a wide variety of functions of the variables and parameters. The rate of change of each variable can also be added to the constraints. These constraints systematically allow for including all existing process alarm thresholds of primary and secondary process variables. This formulation also allows for the inclusion of the saturation of each manipulated variable (actuator). Thus, the general constraint formulation of Eq.(2) permits the design of safety systems that activate alarms accounting for process nonlinearities and interactions among process variables, leading to fewer false and missed alarms.

Moving-Horizon Operability Analyses

The MPS system can detect current and future hazardous operation conditions based on its main components that are employed to assess the likelihood of the risk scenarios. This assessment is conducted based on the definitions given next.

Definition 1 (Mohseni Ahooyi et al., 2016): An operation hazard is said to exist when *no control system* is able to prevent the violation of an operability constraint over a time horizon into the future.

An operation hazard is a hazard that no control system is able to prevent its occurrence. Upon its detection, process safety systems and personnel that by design have access to a higher degree of controllability must intervene to manage the hazard and minimize the likely losses that it can cause.

Definition 2 (Mohseni Ahooyi et al., 2016): The operation of a process at a time instant t is said to be *nominally* hazard-free over a time horizon of $[t, t+\tau]$, if at the time instant t there exists a feasible control profile (action), $u(\ell|t) \in \Omega_u$, $\ell \in [t, t+\tau]$, that satisfies the following conditions:

$$G(\hat{x}(\ell|t), d(\ell|t), d_m(\ell|t), p(\ell|t), u(\ell|t), y(\ell|t)) \in \Omega_c, \quad d_m(t|t) = \tilde{d}_m(t),\ d(\ell|t) = d_n,\ d_m(\ell|t) = d_{m_n},\ p(\ell|t) = p_n,\ x_0 = x_{0_n},\ \forall \ell \in [t, t+\tau] \qquad (3)$$

where d_n, d_{m_n}, x_{0_n} and p_n are the *nominal* (typical operating) values of d, d_m, x_0 and p, respectively. The size of the moving prediction horizon, τ, is chosen by the MPS system designer on the basis of the time constant of the process under consideration and the time needed to arrest the operation hazard proactively.

A dissatisfaction of a condition of Eq.(3) is indicative of the existence of an operation hazard at the present time or the development of an operation hazard in the future. In other words, checking the satisfaction of each condition of Eq.(3) allows for the prediction of *future* risks; the MPS system determines whether the process design has adequate ability to move away from current and future operation hazards at any given time. A dissatisfaction of a condition of Eq.(3) implies that no controller, whether traditional or model-based, can prevent an operation hazard from occurring over the time horizon $[t, t+\tau]$.

Definition 3 (Mohseni Ahooyi et al., 2016): The operation of a process at a time instant t is said to be *absolutely* hazard-free over a time horizon of $[t, t+\tau]$, if at the time instant, t, there exists a feasible control profile (action), $u(\ell|t) \in \Omega_u$, $\ell \in [t, t+\tau]$, that satisfies the following conditions:

$$G\big(\hat{x}(\ell|t), d(\ell|t), d_m(\ell|t), p(\ell|t), u(\ell|t)\big) \in \Omega_c, \quad d_m(t|t) = \tilde{d}_m(t), \forall\, d(\ell|t) \in \Omega_d, \forall d_m(\ell|t) \in \Omega_{d_m}, \quad \forall p(\ell|t) \in \Omega_p,\ \forall x_0 \in \Omega_{x_0},\ \forall \ell \in [t, t+\tau] \qquad (4)$$

where $\tilde{d}_m$ denotes a measurement of d_m.

If the operation of a process is absolutely hazard-free at a time instant t, then the control system can operate the process such that all operability constraints of Eq.(2) are satisfied over a time horizon of $[t, t+\tau]$ into the future for every possible value that measured and unmeasured input variables and parameters can take in the future. Because the conditions of Eq.(4) are required to be satisfied for every $d \in \Omega_d$, every $d_m \in \Omega_{d_m}$, every $p \in \Omega_p$, and every $x_0 \in \Omega_{x_0}$, this formulation systematically accounts for parametric uncertainties (including operators' uncertainties) and unmeasured input changes. As will be shown in the Real-Time Implementation section, the physical nature of processes and their operability constraints facilitate greatly the task of determining whether the conditions of Eqs. (3) and (4) are satisfied.

State Predictor

The moving-horizon operability analyses require predicting the present and future estimates of process state variables. This process state prediction can be achieved by simply using a process model directly (without any corrective feedback of output measurements) or by using a state estimator that takes advantage of the corrective feedback from the current and past measurements. The feedback has several advantages such as improving the robustness of the estimates to process-model mismatch.

To calculate the present and future estimates of the process state variables, one can first design a nonlinear state estimator based on a process model, and then project the estimates into the future (Mohseni Ahooyi et al., 2016). A major challenge here is the robust calculation of the future estimates of all process state variables. This is a much more difficult estimation problem than that in state-space-model predictive control where only controlled outputs should be predicted at each time instant.

MPS System Alarm Mechanism

An MPS system alarm mechanism at each time instant t, triggers alarms to alerts process personnel and safety instrumented system to whether the process design is able to satisfy every condition of Eqs. (3) and (4) over a time horizon, $[t, t+\tau]$. Upon the dissatisfaction of a condition of Eq.(3) or (4) at a time instant t, the MPS system generates an alarm signal corresponding to the condition:

- **Definitely Hazardous Operation** (DHO), when the operation is not *nominally* hazard-free (when a condition of Eq.(3) is not satisfied).
- **Potentially Hazardous Operation** (PHO), when the operation is not *absolutely* hazard-free (when a condition of Eq.(4) is not satisfied); or

It is straightforward to show that when the DHO alarm corresponding to a condition is ON, the PHO alarm corresponding to the same condition is ON too. However, the converse may not be true, because a necessary condition for a DHO alarm to be OFF is that its PHO alarm counterpart be OFF.

Remark 1: Process personnel errors, controller faults, and process faults can be included in the formulation through the parameters. For example, a binary parameter can be added to represent the state of health of a pump, and the moving-horizon operability analyses are then conducted to determine whether operability constraints are satisfied under the pump failure. The MPS system allows for determining whether a control system has the ability to force a process to satisfy operability constraints/conditions of the process at the present time and in the future, when the process is subject to real and hypothetical errors and faults.

Remark 2: The model-predictive safety system determines whether the process can satisfy its operability constraints using the most aggressive, feasible, manipulated input profiles, but it does *not* calculate optimal feasible manipulated input profiles that minimize or maximize a performance index. Thus, the computational cost of the MPS system is by far less than that of MPC using the same process model and constraints. Furthermore, once an alarm is triggered by the MPS system, because of the limited controllability given to the control system by the process design, the control system, whether model-based or conventional, is unable to prevent the corresponding process variables from leaving their normal operation ranges. In this case, a higher-level process-protection layer (i.e., a safety system) with access to more controllability is needed to intervene due to the limitation of the control system.

Real-Time Implementation

In practice, $\Omega_{x_0}, \Omega_d, \Omega_{d_m}, \Omega_p,$ and Ω_u are typically hyperrectangles. Also, the boundary of Ω_c represents the line between safe (operable) and unsafe (inoperable) regions, the corner boundary points of Ω_u represent the most aggressive actions a controller can take, and the corner boundary points of $\Omega_{x_0}, \Omega_d,$ $\Omega_{d_m},$ and Ω_p correspond to combinations of lower or upper bounds on $x_0, d, d_m,$ and p, respectively. Furthermore, knowledge of each process often guides us to identify which combinations of the lower and upper bounds for the components of $x_0, d, d_m,$ and p represent the most extreme combination. These features suggest that if the most-extreme combinations of the corner boundary points of $\Omega_u,$ $\Omega_{x_0}, \Omega_d,$ $\Omega_{d_m},$ and Ω_p satisfy the conditions of Eq.(4), then the operation of the process at a time instant t is absolutely hazard-free over a time horizon of $[t, t+\tau]$. This computational approach requires relatively little computer time, as the satisfaction of each operability constraint is evaluated only once for the worst-case combination of the disturbances and parameter values and the corner boundary point of Ω_u that corresponds to the most aggressive control action.

Application to a Polymerization Reactor

To show the application and performance of the MPS system design method, the method was applied to a semi-batch, industrial-scale, solution-polymerization reactor that produces acrylic resins (Mohseni Ahooyi et al., 2016). The reactor operation recipe is as follows. First, the reactor is loaded with $2{,}229\,kg$ of an organic solvent. Second, the reactor is heated to a desired temperature of 90°C by using the jacket steam. Third, once the reactor is at the desired temperature, (a) $0.78\,kmol$ of a thermal initiator (about 3% of the total molar mass of the monomer) dissolved in $278.6\,kg$ of the organic solvent is added to the reactor at a constant flow rate over a period of $4.0\,h$, and (b) $42.6\,kmol$ of the monomer is added to the reactor at a constant flow rate over a period of $3.5\,h$. After the monomer and initiator solution feed tanks are emptied, they are rinsed with specific amounts of the solvent, and then the solvent amounts are added to the reactor; $195\,kg$ of the solvent used to rinse the monomer feed tank is added to the reactor at a constant flow rate over $0.5\,h$ starting at $t = 4.0\,h,$ and $83.6\,kg$ of the solvent used to rinse the initiator feed tank is added to the reactor at a constant flow rate over $0.5\,hour$ starting at $t = 4.5\,h.$ To maintain the reactor temperature at the desired level, the reactor control system changes the jacket fluid temperature by manipulating the cooling water and steam flow rates.

An operation hazard in the form of the accumulation of an excessive amount of the unreacted monomer is simulated. Note that the conversion of the monomer to polymer is highly exothermic, and the rate of heat production by the reactions, which is directly proportional to unreacted monomer concentration, should never exceed the maximum heat removal capacity of the reactor. The reactor mathematical model and other details are given in (Mohseni Ahooyi et al., 2016).

The reactor control system adjusts the cooling water flow rate, F_{cw}, and the steam mass flow rate, $\dot{m}_s$, using proportional valves; the inlet monomer and initiator flow rates, $\dot{n}_M$ and $\dot{m}_{IS}$, using ON-OFF control valves; and the solvent mass flow rates from rinsing the initiator and monomer feed tanks, $\dot{m}_{S_I}$ and $\dot{m}_{S_M}$, using ON-OFF control valves within the following ranges:

$$0 \le F_{cw} \le F_{cw_{max}} = 8.00 \times 10^{-3}\,m^3.s^{-1}$$
$$0 \le \dot{m}_s \le \dot{m}_{s\,max} = 0.2212\,kg.s^{-1}$$
$$0 \le \dot{n}_M \le \dot{n}_{M\,max} = \;0.00338\,kmol.s^{-1}$$
$$0 \le \dot{m}_{IS} \le \dot{m}_{IS\,max} = 0.0282\,kg.s^{-1}$$
$$0 \le \;\dot{m}_{S_I} \le \dot{m}_{S_{I}max} = \;0.0464\,kg.s^{-1}$$
$$0 \le \dot{m}_{S_M} \le \dot{m}_{S_{M}max} = 0.1083\,kg.s^{-1}$$

In other words, the ability of the control system to control the reactor is limited by the preceding manipulated variable constraints. To evaluate the performance of the MPS system *only*, we request and achieve "perfect" temperature control using a "perfect" model-based controller (Mohseni Ahooyi et al., 2016), which adjusts the cooling water and steam flow rates. To enforce the perfect control, two assumptions are made: (i) all state variables are measured; and (ii) there is no mismatch between the reactor model that the model-based controller is based on and the actual reactor. The model-based controller enforces $T(t) = T_{sp}, \forall t \ge 0,$ as long as the upper constraint on the steam flow rate or the cooling water flow rate is not activate.

Model-Based Alarms

Alarm signal(s) are attached to each of the following constraints; that is, the violation of each constraint at any moment over a moving horizon of τ triggers alarm signal(s):

(a) A saturation alarm for violating each of the two conditions:

$$F_{cw}(t) < F_{cw_{max}} = 8.00 \times 10^{-3} m^3.s^{-1} \tag{5}$$

$$\dot{m}_s(t) < \dot{m}_{s_{max}} = 0.2212\ kg.s^{-1} \tag{6}$$

(b) DHO and PHO alarms for violating the following constraints:

$$\hat{T}(\ell|t) \le T_{max} = 375\ K,\ \frac{\hat{m}(\ell|t)}{\rho} \le V_{max} = 7.560\ m^3 \tag{7}$$

$$\hat{n}_m(\ell|t) \le n_{m_{max}} = 6\ kmol \tag{8}$$

$$\hat{n}_I(\ell|t) \le n_{I_{max}} = 0.2\ kmol \tag{9}$$

$$\hat{n}_i(\ell|t) \le n_{i_{max}} = 0.003\ kmol \tag{10}$$

$$\hat{k}_P(\ell|t)\hat{n}_M(\ell|t)\hat{R}(\ell|t)\Delta H + \theta(\ell|t)c\left(T_i(\ell|t) - \hat{T}(\ell|t)\right) < \hat{m}(\ell|t)\frac{2U}{\rho r}\left(\hat{T}(\ell|t) - T_{cw}\right) \tag{11}$$

The last constraint ensures that at every time instant the rate of heat production by the reactions never exceeds the maximum rate of heat removal (from the reactor) capacity of the reactor jacket (Mohseni Ahooyi et al, 2016).

Hazard-Free Operation

According to the reactor recipe, after loading the reactor with 2,229 kg of solvent, the control system heats the reactor, operates the reactor at the desired constant temperature of 90°C, adds the thermal initiator solution to the reactor at a constant flow rate over 4.0 h, and adds the monomer at a constant flow rate over 3.5 h. In this case, we simulate the reactor dynamics when the monomer feed contains no inhibitor. Figure 3 shows the moles of unreacted monomer, initiator, and inhibitor in the reactor, the reactor and jacket temperatures during the first six hours of operation after the reactor reaches the desired operating temperature. As can be seen during normal operation, no alarms are activated as none of the constraints of Eqs.(5)-(11), shown by the red lines in Figure 3, are violated.

Hazardous Operation

In this case, according to the reactor recipe, the control system heats the reactor, operates the reactor at the desired constant temperature of 90°C, and adds the initiator solution and the monomer to the reactor as in hazard-free operation. However, the monomer feed has 0.5 mol% inhibitor. The inhibitor reacts with free radicals, preventing polymer chain formation and growth. The polymerization rate increases, as the concentration of unreacted inhibitor decreases. We compare the performance of a conventional safety system with that of the MPS system in detecting and managing this operation hazard.

Conventional safety system. We consider a conventional safety system that activates an alarm when one of the following constraints:

$$T(t|t) \le T_{max} = 375\ K,\ \frac{m(t|t)}{\rho} \le V_{max} = 7.560\ m^3 \tag{12}$$

is violated. Upon reaching either of these thresholds, the safety system sets the coolant flow rate to its maximum, and the steam, initiator-solution, and monomer flow rates to zero. As Figure 4 shows, at $t = 0.564\ h$ the reactor temperature constraint (375 K) is violated, resulting in the safety system activating the reactor temperature alarm and setting the inlet cooling water flow rate to its maximum, and the inlet steam, initiator-solution, and monomer flow rates to zero. As can be seen, with these most aggressive actions, the violation of the upper bound on the reactor temperature (undesirable temperature rise) cannot be prevented.

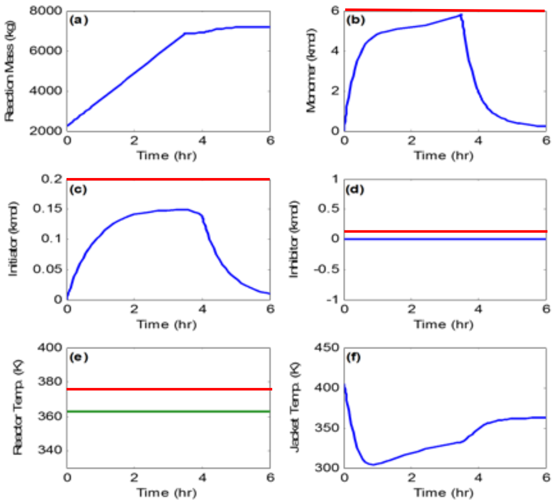

Figure 3: Reactor state variables in the absence of the inhibitor (under Hazard-Free Operation conditions): (a) reaction mass, (b) moles of unreacted monomer, (c) moles of unreacted initiator, (d) moles of unreacted inhibitor, (e) reaction temperature, and (f) jacket temperature. (Mohseni Ahooyi et al., 2016)

MPS system. Now, in this case an MPS system is implemented for the reactor. It activates a DHO alarm when each of the constraints of Eqs.(5)-(11) is violated over a moving horizon of $[t, t+\tau]$, where $\tau = 900\ s$. Figure 5 shows the moles of the unreacted monomer, initiator, and inhibitor in the reactor, and the reactor and jacket temperatures – after the reactor reaches the desired operating temperature. The constraint of Eq.(10) is violated at $t = 0.058\ h$ first when the reactor inhibitor concentration estimate is projected over the moving horizon of $[t, t+\tau]$, leading to the MPS system activating the DHO alarm corresponding to the constraint of Eq.(10), and setting the inlet cooling water flow rate to its maximum, and the inlet steam, initiator-solution, and monomer flow rates to zero. As can be seen, with the proactive action taken by the MPS system, the violation of the upper bound on the reactor temperature (undesirable temperature rise) is prevented. This clearly demonstrates the advantage of the MPS system; that is, the activation of the DHO predictive alarm corresponding to the constraint of Eq.(10) long before the reactor temperature exceeds its limit.

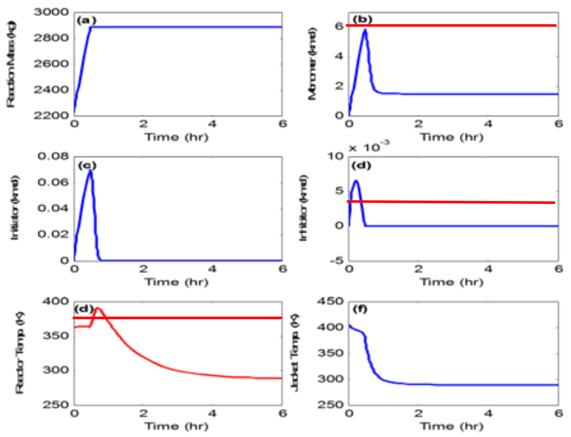

Figure 4: Reactor state variables in the presence of the inhibitor when a conventional safety system is used. Reactor temperature high-alarm threshold of 375 K was violated at t=0.564 hr. (Mohseni Ahooyi et al., 2016)

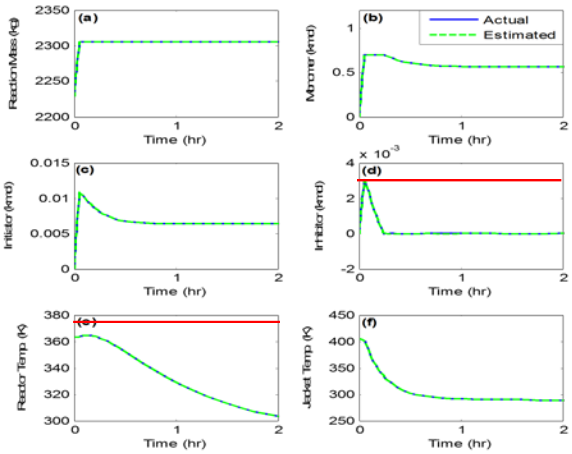

Figure 5: Reactor state variables and their estimates in the presence of the inhibitor when the MPS system with DHO alarms is used. (Mohseni Ahooyi et al., 2016)

Conclusions

The MPS system is capable of predictively detecting current and future hazards in the operation of processes. It generates predictive alarm signals tied to measurements, variable estimates, operability constraints, and control-effort saturations. In addition to assigning predictive alarms to measured variables, such a safety system:

- Determines whether a process can satisfy its operability constraints/conditions at the present time and in the future, when the process is subject to real and/or hypothetical errors and faults;
- Accounts for process nonlinearities and interactions among process variables systematically;
- Assigns alarms to important process variables that are unmeasured but detectable; and
- Predictively detects imminent and potential, current and future, operation hazards in processes.

Typical current safety systems lack these important features.

While the MPS system has the moving-horizon, constraint handling, and model-predictive features of MPC, unlike MPC it does not have a performance index to be minimized; the MPS system is a proposed element of functional safety, and is not a control system. Therefore, the computational cost of the MPS system is much less than that of MPC using the same process model and constraints. Furthermore, once the MPS system activates an alarm, because of the limited controllability allocated to the control system by the process design, no control system can return the corresponding process variables to their normal operation ranges. Consequently, a higher-level protective layer (i.e., a safety system) that has access to more controllability, is needed to intervene. As safety systems are upper protective layers of processes to prevent accidents, they should be *separate from* control systems (that are the lowest [first] protective layers of processes) and should have the ability to *override* control systems. When proactive actions are taken based on the predictive alerts generated by an MPS system, the resulting MPS system will be *prescriptive*.

Acknowledgments

This material is partially based upon work supported by the National Science Foundation under the grants CBET-1066461, CBET-1160169 and CBET-1066475. The authors would like to thank Ulku Oktem, Benjamin J. Jurcik, and Brian M. Besancon for their invaluable comments on this work.

References

Kondaveeti, S.R., Izadi, I., Shah, S., Shook, D., Kadali, R., Chen, T. (2013). Quantification of Alarm Chatter Based on Run Length Distributions. *Chem. Eng. Res. Design*, 91(12), 2550.

Leveson, N.G, Stephanopoulos, G. (2014). A System-Theoretic, Control-Inspired View and Approach to Process Safety. *AIChE J.* 60(1), 2.

Mannan, S.M., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu Y., Laboureur, D.M. (2015). Trends and Challenges in Process Safety. *AIChE J.*, 61(11), 3558.

Mohseni Ahooyi, T., Arbogast, J. E., Seider, W. D., Oktem, U. G., Soroush, M. (2016). Model-Predictive Safety System for Proactive Identification of Operation Hazards. *AIChE J.*, 62, 2024.

Schleburg, M., Christiansen, L., Thornhill, N. F., Fay, A. (2013). A Combined Analysis of Plant Connectivity and Alarm Logs to Reduce the Number of Alerts in an Automation System. *J. Proc. Cont.* 23(6), 839.

U.S. Chemical Safety and Hazard Investigation Board, http://www.csb.gov/.

Wei, L., Guo, W., Wen, F., Ledwich, G., Liao, Z., Xin, J. (2011). An Online Intelligent Alarm-Processing System for Digital Substations. *IEEE Trans. Power Deliv*. 26(3), 1615.