Journal of Loss Prevention in the Process Industries xxx (2016) 1–15

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Achieving operational process safety via model predictive control

Fahad Albalawi [b], Helen Durand [a], Anas Alanqar [a], Panagiotis D. Christofides [a, b, *]

[a] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA
[b] Department of Electrical Engineering, University of California, Los Angeles, CA 90095-1592, USA

ARTICLE INFO

Article history:
Received 5 September 2016
Received in revised form
2 October 2016
Accepted 30 November 2016
Available online xxx

Keywords:
Model predictive control
Chemical processes
Process control
Process functional safety
Process operation

ABSTRACT

Model predictive control (MPC) has been widely adopted in the chemical and petrochemical industry due to its ability to account for actuator constraints and multi-variable interactions for complex processes. However, closed-loop stability is not guaranteed within the framework of MPC without additional constraints or assumptions. An MPC formulation that can guarantee closed-loop stability in the presence of uncertainty is Lyapunov-based model predictive control (LMPC) which incorporates stability constraints based on a stabilizing Lyapunov-based controller. Though LMPC drives the closed-loop state trajectory to a steady-state, it lacks the ability to adjust the rate at which the closed-loop state approaches the steady-state in an explicit manner. However, there may be circumstances in which it would be desirable, for safety reasons, to be able to adjust this rate to avoid triggering of safety alarms or process shut-down. In addition, there may be scenarios in which the current region of operation is no longer safe to operate within, and another region of operation (i.e., a region around another steady-state) is appropriate. Motivated by these considerations, this work develops two novel LMPC schemes that can drive the closed-loop state to a safety region (a level set within the stability region where process functional safety is ensured) at a prescribed rate or can drive the closed-loop state to a safe level set within the stability region of another steady-state. Recursive feasibility and closed-loop stability are established for a sufficiently small LMPC sampling period. A comparison between the proposed method, which effectively integrates feedback control and safety considerations, and the classical LMPC method is demonstrated with a chemical process example. The chemical process example demonstrates that the safety-LMPC drives the closed-loop state into a safe level set of the stability region two sampling times faster than under the classical LMPC in the presence of process uncertainty.

1. Introduction

Process functional safety is critical to industrial chemical plants. The catastrophic incidents and disasters that have occurred over the past decades highlight the importance of safety and can be studied to prevent similar accidents in the future (Crowl and Louvar (2011)). These accidents may cause chemical substances to be released which can affect limited resources such as water and agricultural resources (Valipour (2012); Yannopoulos et al. (2015); Valipour and Singh (2016); Valipour (2016)). The frequency of accidents has motivated systematic methods for evaluating and improving process functional safety to be developed. For example, in (Leveson (2004)), an accident model is developed that can improve process functional safety. In (Kadri et al. (2014)), methods are developed to apply corrective actions based on data analysis, measurement and sorting processes to achieve meaningful process functional safety performance improvements. Process control is also utilized to control the risks that are associated with chemical processes (Bahr (2015)). Despite these methods for assessing and improving process functional safety, technological advances and further process/plant intensification continue to increase the complexity of maintaining safe process operation (Venkatasubramanian (2011); Leveson and Stephanopoulos (2014); Mannan et al. (2015)). Therefore, implementing control techniques that can predict and control the interactions between the components of these complex processes is necessary (Venkatasubramanian (2011)). In chemical plants, techniques such as hazards and operability (HAZOP) (Khan and Abbasi (2000); Dunjó et al. (2010)) analysis, fault trees and what-if scenarios are performed to evaluate the safety of a process. These techniques

---

* Corresponding author. Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

http://dx.doi.org/10.1016/j.jlp.2016.11.021
0950-4230/© 2016 Elsevier Ltd. All rights reserved.

Please cite this article in press as: Albalawi, F., et al., Achieving operational process safety via model predictive control, Journal of Loss Prevention in the Process Industries (2016), http://dx.doi.org/10.1016/j.jlp.2016.11.021

usually result in a report that describes the damage that would result from an accident. Chemical process safety has traditionally been addressed through process design decisions (e.g., designing the process to be inherently safe in terms of its chemistry and physics Kletz and Amyotte (2010); Gentile et al. (2003); Heikkilä et al. (1996)) and control and safety system design decisions (e.g., adding measurement sensors for critical process variables that trigger an alarm when an undesirable measurement is obtained).

Inherently safer designs are achieved through four primary principles: minimize (reduce the quantity of hazardous substances used and stored by a process), substitute (utilize less hazardous process chemistries), moderate (dilute chemicals or change operating conditions), and simplify (choose designs with less complexity and less potential to create hazardous conditions when faults or errors occur) Kletz (1985). Though designs can be made inherently safer, it is not possible to eliminate all hazards Kletz (2009), so a safety system, comprised of several independent layers, should be added to chemical processes. The layers of protection commonly used in industry are the basic process control system (BPCS), safety critical alarm system, safety trips/interlocks system, safety relief devices, containment and emergency response. Ideally, the layers of the safety system should not be activated regularly because a basic process control system (BPCS) regulates process variables to their set-points. When the control system is unable to keep the process variables within acceptable ranges due to, for example, equipment faults or unusually large process disturbances, alarms are triggered that alert operators to the issue so that actions can be taken to prevent further unsafe deviations. When operators are unable to bring the process back into a normal operating regime and the process variables exceed allowable values, the safety trips/interlocks system is triggered, which takes automatic and extreme actions such as forcing a valve to its fully open position to bring the process to a safer state of operation. Safety relief devices such as relief valves are used on vessels that can become highly pressurized very quickly, such that the control system, alarms, and safety trips/interlocks system would not be effective for preventing an explosion without the relief device. Containment is used to prevent hazardous material from entering the environment or injuring workers when the other layers of the safety hierarchy fail to prevent release of the material. The emergency response plan is used in severe cases that were not mitigated by any of the other layers of the safety hierarchy to minimize the impact to humans and the environment. The layers of the safety hierarchy are independent of each other and of the control system (i.e., they have separate sensors, computing elements, and actuators) to allow redundancy and improve safety Marlin (2012).

In (Leveson and Stephanopoulos (2014)), it has been argued that safety considerations can be used as constraints in control systems to combine process functional safety and process control in one framework. Nevertheless, the majority of the control techniques currently in use such as, for example, the traditional single-input/single-output (SISO) feedback control systems (e.g., PID controllers), would be incapable of enforcing safety constraints in the process control layer (Whiteley (2006)). Traditional SISO control strategies can be replaced with advanced control techniques that can potentially integrate safety and process control in one framework (Leveson and Stephanopoulos (2014)). One example of an advanced control system is tracking model predictive control (MPC), which is widely adopted in industry. MPC is a control technique that applies control actions (manipulated inputs) which are computed by formulating and solving a dynamic optimization problem on-line that takes advantage of a dynamic process model while accounting for process constraints (e.g., Mayne et al. (2000); Qin and Badgwell (2003); Mhaskar et al. (2006)). Several research works have integrated safety with MPC; for instance, an adaptive learning-based model predictive controller was designed to decouple safety and performance in an optimization framework (Aswani et al. (2013)) and a two-mode MPC with a standard mode and a reactive safety mode was designed to account for unexpected state-constraint changes (Carson et al. (2013)). In (Ahooyi et al. (2016)), a model-predictive safety system was developed that can detect operation hazards in a proactive fashion using model predictions to aid in safety alarm triggering. In addition, a recent research work has proposed data-based probabilistic models for special-cause event occurrences and operator response-times to evaluate the likelihood of alarm and safety interlock system failures (Moskowitz et al. (2016)).

Recently, a form of MPC termed Lyapunov-based model predictive control (LMPC) has gained attention (Mhaskar et al. (2006)) due to its guaranteed and explicit closed-loop stability properties in terms of characterization of the closed-loop stability region that the standard tracking MPC formulation with terminal stability constraints lacks. Though LMPC is guaranteed to drive the closed-loop state to a small neighborhood of the steady-state, the rate at which the LMPC drives the closed-loop state toward the equilibrium using a quadratic objective function and Lyapunov-based stability constraints alone may not be fast enough to ensure process functional safety. This can pose a safety issue if there are process transients that make it necessary for the closed-loop state to approach a safe level set of operation (safety region) around the steady-state more quickly and can lead to triggering safety alarms or process shutdown. Furthermore, quantifying *a priori* the rate at which the closed-loop state will move toward the safety region for a given tuning of the weighting matrices in the quadratic objective function is not possible in general, showing that adjusting the weighting matrices to achieve a required rate of approach to the safety region would not be sufficient.

Hence, it is necessary to develop an LMPC design that can adjust the rate at which the state approaches the safe operating region in unsafe scenarios. Moreover, the safe operating region may shift from a level set around one steady-state to a level set around another, and the LMPC should be able to drive the state to the newly computed safe operating region. However, the classical LMPC would be incapable of accomplishing this task because it is not designed to drive the closed-loop state to a safe operating region that corresponds to a new steady-state. To date, no work on formulating an MPC scheme that utilizes safety-based constraints, which controls the rate at which the closed-loop state approaches the steady-state in a direct manner, with guaranteed closed-loop stability properties, has been completed. Motivated by the above considerations, two LMPC schemes are first designed that can achieve safe operation of nonlinear processes by controlling the rate at which the closed-loop state moves toward a safe operating region which is associated with the original operating steady-state, and second, modifications to these LMPC schemes are developed that allow the closed-loop state to be driven to a level set within the stability region of another steady-state. Recursive feasibility and closed-loop stability of both safety-LMPC schemes are addressed for a sufficiently small LMPC sampling period. Using a chemical process example, the applicability of the proposed LMPC with safety-based constraints, which effectively integrates feedback control and safety considerations, is demonstrated and the performance is compared with that of a classical LMPC scheme.

2. Preliminaries

2.1. Notation

The transpose of a vector x is represented by the symbol x^T. The Euclidean norm of a vector is denoted by the operator $|\cdot|$. A level set

Please cite this article in press as: Albalawi, F., et al., Achieving operational process safety via model predictive control, Journal of Loss Prevention in the Process Industries (2016), http://dx.doi.org/10.1016/j.jlp.2016.11.021