Computers and Chemical Engineering xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Process operational safety via model predictive control: Recent results and future research directions

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

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

ARTICLE INFO

Article history:
Received 20 June 2017
Accepted 9 October 2017
Available online xxx

Keywords:
Process safety
Process control
Model predictive control
Process operation
Nonlinear processes
Safety systems

ABSTRACT

The concept of maintaining or enhancing chemical process safety encompasses a broad set of considerations which stem from management/company culture, operator procedures, and engineering designs, and are meant to prevent incidents at chemical plants. The features of a plant design that take action to prevent incidents on a moment-by-moment basis are the control system and the safety system (i.e., the alarm system, safety instrumented system, and safety relief system). Though the control and safety systems have a common goal in this regard, coordination between them has been minimal. One impediment to such an integrated control-safety system design is that the traditional industrial approach to safety focuses on root causes of incidents and on keeping individual measured variables within recommended ranges, rather than seeking to understand incidents from a more fundamental perspective as the result of the dynamic process state evolving to a value at which consequences to humans and the environment occur. This work reviews the state of the art in control system designs that incorporate explicit safety considerations in the sense that they have constraints designed to prevent the process state from taking values at which incidents can occur and in the sense that they are coordinated with the safety system. The intent of this tutorial is to unify recent developments in this area and to encourage further research by showcasing that the topic, though critical for safe operation of chemical processes particularly as we move to more tightly integrated and economics-focused operating strategies, is in its infancy and that many open questions remain.

1. Introduction

Due to the dangers to people and the environment that are inherent in operating chemical processes, process safety has been an important consideration for both the design and operation of chemical processes throughout time (Crowl and Louvar, 2011). The concept of ensuring process safety is very broad and is often considered to refer to appropriate engineering designs that prevent incidents in the presence of abnormal operating conditions, combined with management decisions, training, and procedures put in place at a site to protect people and the environment against hazards so that the risk of incidents can be mitigated (Center for Chemical Process Safety, 2010, 2001). The definition of "incidents" broadly includes all situations termed "near misses" or "accidents" of various severity levels in industry that are considered to have had the potential to lead to hazards to people, the environment, or property, or that did lead to harm (Jones et al., 1999; Phimister et al., 2003). The prevention of incidents at a plant is considered to involve both human engagement (at the level of procedure development and daily execution of these procedures, and also at the level of determining what unexpected scenarios may occur for which barriers to incidents should be set up through techniques such as Hazard and Operability (HAZOP) studies and fault tree analysis Center for Chemical Process Safety, 2008) and the success of automation at the plant (e.g., software functioning according to the expectations of those who install it Leveson (1995), the safety instrumented system functioning properly, and the control system regulating process variables to their steady-state values). The multifaceted nature of process safety as described above has caused it to be addressed from many different angles. Some of the topics that have been addressed in the literature include automating aspects of the engineering judgment process (Venkatasubramanian et al., 2000), preventing fires and explosions and understanding the effects of chemical release (Englund, 2007; Reniers and Cozzani, 2013), designing processes to be inherently safe

* Corresponding author at: 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).

https://doi.org/10.1016/j.compchemeng.2017.10.006
0098-1354/

(Khan and Amyotte, 2003), studying past incidents (Kidam and Hurme, 2013; Kletz, 2009), quantifying the risk associated with incidents (Center for Chemical Process Safety, 2000), and dynamic failure assessment (Meel and Seider, 2006). An additional consideration is that incidents do not necessarily occur during continuous process operation, but may also occur under atypical operating conditions, such as when the plant is off-line during maintenance or is being started up (Ness, 2015; Bloch, 2016). In this work, we will focus on the aspect of process safety related to designing equipment that takes action in response to a certain stimulus (the control system and safety system, which in this work is defined to include the alarm (Rothenberg, 2009), safety instrumented (Mannan, 2012; Center for Chemical Process Safety, 2017b), and safety relief systems Center for Chemical Process Safety, 1998; Fisher et al., 1992) to prevent incidents at a plant. Therefore, the references to "process safety" and "process operational safety" throughout this work should be understood in this context.

The control system and the safety system complement one another as part of an approach to maintaining operational safety in the chemical process industries which can be considered, at a high level, to be hierarchical according to Fig. 1. The control system is typically used to regulate process states like temperature and pressure to their steady-state values in the presence of disturbances. The alarms will be triggered when process variable measurements either exceed certain thresholds (when the threshold represents an upper bound) or fall below them (when the threshold represents a lower bound) (Pariyani et al., 2010) due to, for example, disturbances or equipment faults, and the alarm system will supply some information to an operator regarding the reason for the alarm system activation so that the operator has a chance to take corrective actions based on the alarm. Other thresholds on measured process variables are set such that the safety instrumented system will take automated actions with an on/off characteristic (e.g., it may fully close a valve for the fuel stream to a reactor to shut off the process completely) when the process variables exceed/fall below these thresholds. The safety relief system is often comprised of valves or rupture disks that are mechanically actuated (e.g., they open or burst due to the properties of the materials from which they are made when a certain pressure builds up behind the valves/disks). Safety relief devices are typically used with vessels within which the pressure can rise and lead to explosion of the vessel if the pressure is not reduced by the valves/rupture disks. When necessary, containment of chemical releases or emergency response plans are utilized (Marlin, 2012). Standard practice emphasizes the independence of the control system and the elements of the safety system in the sense that failure of critical components of the control, alarm, safety instrumented, or relief system should not cause failure of the other systems. It is worth investigating, however, how the control and safety systems may be designed to account for limitations of one another (e.g., the control system could anticipate the activation of the safety system through state predictions during process operation and the safety system could be triggered by state-based considerations typically only accounted for in the control design) without sacrificing redundancy in the design. Coordination between the control and safety systems has traditionally been limited; it may involve, for example, determining how close the controller needs to keep the process state to an operating steady-state (and what that means for the controller's design) to avoid activating elements of the safety system as much as possible (Center for Chemical Process Safety, 2017a), or it may involve state constraints on predicted states in control designs that explicitly handle constraints (Qin and Badgwell, 2003).

Greater coordination of the control and safety systems may be beneficial given the complementary roles of those systems in preventing incidents and also the typical hierarchical nature of their use (i.e., if the control system does not prevent a measured process state from crossing a threshold, an alarm sounds; this indicates that the way that the control system functions directly impacts whether the safety system needs to take action). A starting point for pursuing this greater coordination is designing the control system to explicitly account for safety considerations so that under normal process operation, the process state is maintained in a region in state-space where incidents are not expected to occur and where the safety system is not activated. The concept of incorporating safety within control (specifically, within model predictive control (MPC) (Qin and Badgwell, 2003; Ellis et al., 2016), which will be the focus of this paper due to the industrial relevance of MPC and its ability to account for constraints and multivariable interactions that can be important for analyzing whether the process state is within regions in state-space where incidents may occur) has been associated primarily with closed-loop stability and robustness arguments, incorporation of safety metrics in control design, and designing controllers to respond to changes in the process dynamics or available equipment over time. In this tutorial, we highlight the need for characterizing safe operating regions in state-space using safety metrics that mathematically formalize the concept of a systems approach to process operational safety (this systems perspective will be shown to result in safety-based constraints for MPC that are different from the types of state constraints traditionally considered to be related to operational safety), especially as there are greater pushes toward more integrated manufacturing paradigms that may operate processes in a time-varying fashion as opposed to the traditional steady-state fashion. We will also enumerate desirable properties for controllers that seek to maintain process safety, identifying fundamental benefits and limitations of different control designs for achieving these desirable properties. We will conclude with an outlook on how a system-theoretic safety metric may impact safety system design and an outlook on further advances that will enable greater coordination between the control and safety systems to prevent incidents at chemical plants.

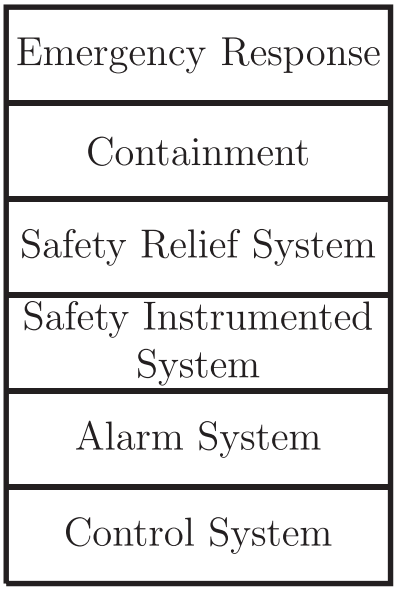

Fig. 1. Hierarchical approach to maintaining operational safety (Marlin, 2012).

2. Preliminaries

2.1. Notation

The notation $|\cdot|$ signifies the Euclidean norm of a vector. The symbol $S(\Delta)$ signifies the class of piecewise-constant functions with period Δ. A function $\alpha : [0, a) \to [0, \infty)$ is said to be in class $\mathcal{K}$ if

Please cite this article in press as: Albalawi, F., et al., Process operational safety via model predictive control: Recent results and future research directions. Computers and Chemical Engineering (2017), https://doi.org/10.1016/j.compchemeng.2017.10.006