Computers and Chemical Engineering 108 (2018) 74–88

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Understanding rare safety and reliability events using transition path sampling

Ian H. Moskowitz [a,b], Warren D. Seider [a,*], Amish J. Patel [a], Jeffrey E. Arbogast [b],
Ulku G. Oktem [c]

[a] Department of Chemical and Biomolecular Engineering, University of Pennsylvania, Philadelphia, PA 19104-6393, United States
[b] American Air Liquide Newark, DE 19702, United States
[c] Risk Management and Decision Processes Center, Wharton School, University of Pennsylvania, Philadelphia, PA 19104, United States

ARTICLE INFO

Article history:
Received 29 August 2016
Received in revised form 10 June 2017
Accepted 12 June 2017
Available online 14 August 2017

Keywords:
Risk analysis
Abnormal events
Transition path sampling

ABSTRACT

In the chemical and process industries, processes and their control systems are typically well-designed to mitigate abnormal events having potential adverse consequences to human health, environment, and/or property. Strong motivation exists to understand how these events develop and propagate. These events occur so rarely that statistical analyses of their occurrences alone are incapable of describing and characterizing them – especially when they have not yet occurred. Moreover, the use of process models to understand such rare events is hampered by the orders of magnitude separating the frequencies with which reliability and safety events (years to decades) occur and the duration over which they occur (minutes to hours). To address these challenges, we adapt a Monte-Carlo based, rare-event sampling technique, Transition Path Sampling (TPS), which was developed by the molecular simulation community. Important modifications to the TPS technique are needed to apply it to process dynamics, and are discussed herein.

1. Introduction

Safety and reliability are paramount to the chemical and process industries. Because chemical plants are often operated at high temperatures and pressures, and with hazardous materials, the potential for adverse human health and environmental impacts exists. With proper process design, effective implementation of control and safety instrumented systems (SIS) reduces the likelihood of such risks. More likely are product losses which result from poor plant reliability. As chemical manufacturing processes approach dangerous operating conditions, automatic safety interlocks activate, shutting them down before dangerous consequences are realized. When functioning correctly, the dangerous consequences are avoided, but manufacturing processes lose valuable production over the time period encompassing the automatic shutdown, process maintenance, and startup. Furthermore, plant startup can involve potential dangers considering that the procedures followed are not routine and the process may have changed due to maintenance activities. Thus, there is clear motivation to prevent chemical manufacturing processes from operating in abnormal regions, including situations where safety interlocks activate automatic plant shutdowns.

Safety interlocks are often based on HAZOP (hazard and operability analysis) (Kletz, 1999; Venkatasubramanian and Vaidhyanathan, 1994; Kennedy and Kirwan, 1998) and LOPA (layer of protection analysis) (Dowell, 1998; Summers, 2003). With HAZOP, potential hazards to personnel and capital equipment that may occur during process operation are identified through a meticulous (yet qualitative) procedure. It provides “a more complete identification of the hazards, including information on how hazards can develop as a result of operating procedures and operational upsets in the process” (Crowl and Louvar, 2001). With LOPA, the probabilities of identified hazards occurring are maintained under a low, pre-specified value by utilizing a system of high-performing, independently-acting safety systems. Said differently, the hazards identified by HAZOP analysis are mitigated to lower-consequence events (such as plant shutdowns) with high probability by using safety systems identified through LOPA. Through these analyses, safety interlock thresholds are determined. From a reliability perspective, operators seek to avoid costly shutdowns by adjusting valves when control systems are too slow or insufficient in responding to severe disturbances (known as special-cause events). Avoiding shutdowns is also beneficial from a safety perspective, as transient shutdowns and startups are avoided. Clearly, the events

---

[*] Corresponding author.
E-mail address: seider@seas.upenn.edu (W.D. Seider).

http://dx.doi.org/10.1016/j.compchemeng.2017.06.016
0098-1354/

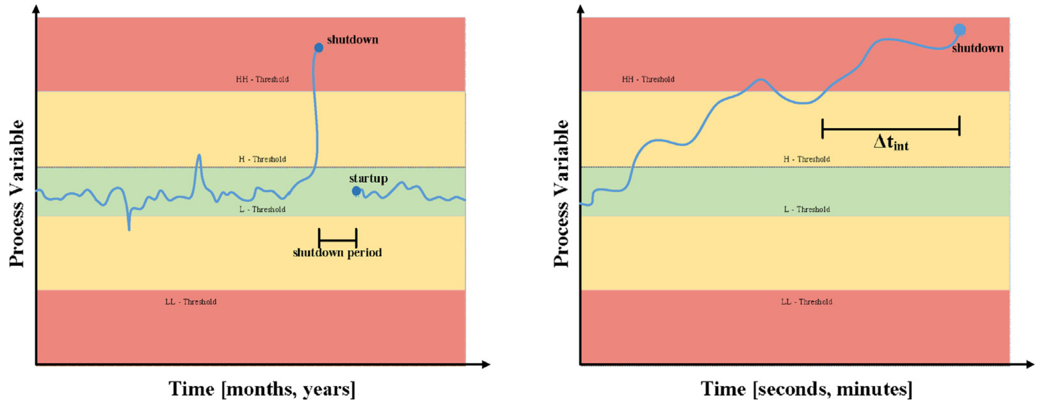

Fig. 1. Alarm belt-zones and interlock shutdown for a process variable.

resulting in interlock shutdowns are undesired, and in most cases these events occur infrequently. This paper will refer to these events as 'rare events'.

Operators are aided by an alarm structure in which process variables pre-specified to be important to the reliability and safety of the process are equipped with alarms. When a variable moves outside of its typical (safe) operating region, the green-belt zone, either a low (L) or a high (H) alarm activates accordingly. Often, process variables have levels of alarms, possibly a yellow belt-zone (bounded by L and H alarms), and a red belt-zone (bounded by LL and HH alarms). Such an alarm scheme is depicted in Fig. 1. Here, in Fig. 1a, a process variable is displayed over months and years, normally residing within its green-belt zone – and, when perturbed into its yellow-belt zone, safety systems/operator actions usually return it to its safe green-belt zone. Rare events can result in the automatic shutdown (safety interlock) of the process, followed by a shutdown and restart, which occur over minutes and hours, as shown in Fig. 1b. The safety-interlock shutdown is activated when the process variable resides in the red belt-zone for a pre-specified length of time, Δt_{int}, typically on the order of seconds (if any). As a variable moves into each successive belt-zone, the operator becomes aware that interlock activation is impending and takes more severe actions to return the variable to its green-belt zone.

The alarm thresholds are set in the process commissioning phase (Hollifield and Habibi, 2010), with competing objectives to: (1) assure that when an alarm is activated operators have sufficient time to act, avoiding subsequent (more severe) alarms or interlock activations, and (2) that the alarm isn't a nuisance, often activated unnecessarily reducing the urgency of operator response. Commissioning is usually performed using expert knowledge of process behavior (based upon the actions of similar processes and upon insights gained in the process design phase), and tests to observe typical transient responses of the variables.

Clearly, alarms are commissioned to alert operators to *postulated*, more common, events that could propagate to interlock activation. But, alarm structures may be insufficient to alert operators to rare or *un-postulated* events. Such unforeseen safety events have the potential to move to the red belt-zone and activate the interlock shutdown faster than the alarms are designed to handle. These events may arise early involving variables that are not alarmed, or when some combination of variables leads to such an event. Without proper alarming of such hidden variables, operators may not be able to prevent automatic shutdowns; on the other hand, with the benefit of proper alarms, these events may be easily handled by operators.

A quantitative technique to better identify and understand events that lead to process shutdowns would be very useful to engineers responsible for commissioning alarms and operators that respond to those alarms. This paper introduces transition path sampling (TPS) as such a technique for application in the chemical manufacturing industries. TPS is a Monte-Carlo sampling strategy that simulates process models as they propagate toward interlock-activating events. Trajectories of these events are randomly generated, uncovering many un-postulated events, and enabling postulated events to be better understood. With many similar trajectories generated, the probability of a typical trajectory can be estimated, identifying the most likely unsafe events, suggesting more effective alarm thresholds. TPS has been widely investigated by the molecular dynamics community to study rare molecular events (Bolhuis et al., 2002; Dellago et al., 2002), but the application of TPS to process dynamics for studying rare interlock-activating events is novel and presents its own challenges.

2. Transition path sampling

TPS was invented to study rare molecular dynamic trajectories; for example, the dissociation of a weak acid in an aqueous solution. A weak acid, such as hydrofluoric acid (HF), dissociates in water in approximately once every millisecond, but its dissociation event occurs in just nanoseconds (Bolhuis et al., 2002). Hence, its average initiation time is on the order of 10^6 times longer than the event itself! Clearly, the majority of the computation time in the simulation of the initiation/dissociation sequence is devoted to tracking the uninteresting *initiation* phase. In TPS, to circumvent this, a trajectory of length t_{final} that is just long enough to capture one initiation/dissociation event is simulated. Then, at a random time, t', along the event trajectory (spanning $[0, t_{\text{final}}]$), state variables (such as atom locations and momenta) are randomly perturbed. This new state is simulated forward spanning $[t', t_{\text{final}}]$ and backwards spanning $[t', 0]$. If the acid is associated at $t = 0$, and dissociated at $t = t_{\text{final}}$, then a second rare-event trajectory has been generated, and if it has a likelihood that is reasonably similar to the original trajectory, the new trajectory may be accepted. The new trajectory is then perturbed, and over many iterations, numerous rare-event trajectories can be generated, with minimal computational effort in simulating the initiation phase (Dellago et al., 2002).

When applied to process dynamics, TPS can identify and explain rare-events resulting in interlock activation. The models and time scales in process dynamics are vastly different from those in molecular dynamics, but the challenge of simulating rare (yet particularly interesting) events is similar. A typical rare interlock-activating event may occur once in several years if not decades, while the event itself lasts only minutes to hours. Once again, TPS can be used to circumvent simulation of the initiation phase – the time in between rare safety-events of interest. As shown schematically in Fig. 2a, a complete trajectory is identified by simulation (or by a