Process Safety and Environmental Protection xxx (2013) xxx–xxx

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Transmission Functions and its application to the analysis of time uncertainties in Protection Engineering

Sergey E. Galushin[a,*], José María Izquierdo[b], Miguel Sánchez Perea[b,1]

[a] Nuclear Engineering Department, Technical University of Madrid, José Gutiérrez Abascal 2, 28006 Madrid, Spain
[b] Modeling and Simulation Department, Nuclear Safety Council (MOSI CSN), Justo Dorado 11, 28040 Madrid, Spain

ABSTRACT

In this paper we explore the concept of transmission Functions and its application to the resolution of the problem posed by the uncertainty in the time to take manual protective actions due for instance to different operator abilities. This time uncertainty is a very special kind of uncertainty with obvious relevance in Protection Engineering problems. Tackling it involves a large amount of simulations of transients associated to sequences of system transitions, resulting from those actions, where the only difference from one simulation to another is the time interval between transitions, the evolution laws being always the same. In order to solve such type of problems, a new formalism is proposed based on the concept of transmission Function. We prove that for a large class of Multiple Input–Multiple Output (MIMO) piecewise linear systems, the output may be obtained as additive contributions of each interval of the sequence, each one characterized via a Transmission Function. We then provide efficient methods to compute Transmission Functions of sequences of canonical Single Input-Single Output (SISO) piecewise systems, and to find the locus of protective action times that lead to damage (damage domain).

Keywords: Piecewise linear systems; Damage domain; Time uncertainty; Simulation; Transmission Function; Protection Engineering

1. Introduction and purpose

Protection Engineering may be defined as the set of technologies aimed at the optimization of the design of protections. Problems requiring them appear in many branches of engineering, most relevant in Nuclear, Chemical, Aeronautic, and Electric Power Generation facilities, but today's extending beyond those. Because these facilities may generate unacceptable damage to the public, they are regulated industries with regulations based on a specific body of principles.

There are recent trends (Gennat and Tibken, 2006) toward a technology-neutral approach that reflect common underlying regulatory principles corresponding to common features of the protection problem. This trend is clearly visible in Nuclear Safety (IAEA, 2007), in order to regulate in a common but concrete approach a multiplicity of new designs.

This paper is one of a series of contributions that try to precisely formulate and suggest solutions to important aspects of the common protection problem, in a unified way. As a result, we aim to obtain a set of general, computerized methods and tools to verify adequate protections in a way that ensures that the main figures of merit of risk assessment, namely the exceedance frequencies of safety limits (Hess, 2009; SMAP, 2007), are kept at acceptable regulatory levels.

The peculiarities of the application are encapsulated through specialized computer codes, specific of the discipline. They mainly describe the phenomena leading to time evolutions of the continuous variables characterizing the system states and keep track of them along the different stages of accident progressions, where new phenomena are expected to accompany and/or to induce the progression itself (Griesmeyer and Smith, 1989; U.S. Neclear Regulatory Commission, 1990; Raimond et al., 2004).

Abbreviations: SISO, single input single output; MIMO, multiple input multiple output; SOT, sequence of transitions.

* Corresponding author. Tel.: +34 600728151.
E-mail addresses: sergey.e.galushin@gmail.com (S.E. Galushin), jmir@csn.es (J.M. Izquierdo), msp@csp.es (M.S. Perea).

Received 18 February 2013; Received in revised form 5 July 2013; Accepted 26 July 2013

[1] Tel.: +34 913460237.

0957-5820/$ – see front matter © 2013 The Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.psep.2013.07.004

This paper, in particular, deals with new techniques to analyze the uncertainty in the time to take protective actions (time uncertainty), including identification of combinations of actuation-times leading to damage (operator damage domains). Typical examples are those associated with different operators that take actions at different times when reacting to activation of alarms. These techniques help also to clarify the actual meaning of the qualitative concept of "being too late". Time uncertainty is a very special class of uncertainty, of obvious relevance in protection problems.

The organization is as follows. In Section 2 the formulation of the problem is given. In Section 3 the basis of the method is presented. Section 4 contains the main theorem of the Transmission Function approach and some computational aspects of the problem. Examples to illustrate the method are included in Section 5, and finally conclusions are given in Section 6.

2. Problem formulation

2.1. *Describing the evolution of sequences of transitions in dynamic systems*

Most mathematical models that simulate real processes taking place in industrial facilities include dynamic models, i.e. they consider evolutions with time. System states may often be described by a set of continuous variables, like pressures, temperatures, angles, concentrations, velocities, etc. (process vector), as well as by a set of discrete state variables (discrete states), like the status of certain plant subsystems in terms of "operating", "out of service", "standby" or "failed") (Aldemir et al., 1992).

For instance, consider a tank storage facility containing a mixture of reacting substances in a solvent at a given temperature, the reaction being exothermic. The substance and solvent concentrations, as well as the mixture temperature, may be used to define the components of a process vector that evolves with time, either as a result of the operation of fixed-flow injection/extraction systems of any one of the components/solvent or that of the mixture fixed-power heater/cooler systems. The different modes of operation of those (injecting, extracting, or no flow), as well as the three on-of states of the heater/cooler modes constitute the discrete vector. Then, associated to each discrete state, the chemical reaction evolution varies, generating a dynamic state with a distinct law of evolution.

More specifically, we consider a system that may be, during successive time intervals (sojourn times), in successive discrete dynamic states, its time evolution laws being different in each one.[2] Its overall evolution is then constituted by a sequence of transitions (SOT) in-between the discrete states, resulting in a piecewise dynamic model. When these transitions are the result of stochastic events, any SOT outcome also becomes a stochastic outcome and its frequency may be used as a measure of the likelihood of its occurrence (Izquierdo and Cañamon, 2008).

In the example above, assuming an initial steady state of the process/discrete vectors, any change in any of its components will generate a time evolution of the concentrations and temperature. To any sequence of changes in the discrete vector, there will correspond a sequence of transitions of its associated time evolutions.

2.2. *Sequences of transitions in Protection Engineering. Stimulus activations*

In particular, in the context of Protection Engineering, transitions are often associated to system failures, eventually followed by the subsequent actuation of protections (safeguard systems), so accident math descriptions become naturally sequences of transitions (SOT), resulting from sequences of failure and protection events.

They are such that, for each successful safeguard operation, the associated transition changes the evolution (curbing this way the bad trend of the system). However, a safeguard action failure does not result in a dynamic change and the evolution is kept the same (meaning that the system behavior continues its degraded evolution).

In the example above, in order to have a steady reaction we need a cooling action, so the steady initial discrete state includes the on-mode of the cooling system.

An accidental initial on-of transition of the cooling mode as a result of cooling system failure may lead to a temperature increase that ultimately may evolve into a runaway reaction out of control. The systems able to extract key reactants or add solvent may avoid this, acting as safeguards systems.

The success of any of these safeguards interventions implies an additional transition, so we have an accident SOT of several transitions, the first associated to the initial cooling system failure, followed by the different changes in the safeguards extraction (addition) modes of the key reactants (solvent).

As a result, some of these accident SOTs may result in damage, if certain limits (safety limits) are exceeded. The stochastic frequency of the damage outcome is then a measure of risk. The set of limits imposed by the designer or regulator on these damage frequencies associated to each and all of the safety limits constitute a general risk metrics of the problem.

In the example above we may consider reaching a pressure safety limit as a threshold that prevents container breach, as well as a maximum flow-out of some of the toxic reactants in case of non-null breach flow. The risk metrics is then the set of design/or regulatory limits imposed to the frequency to exceed the two of them.

Thus, in order to qualify facility risk, an essential point in protection design verification is the study of potential accident SOTs that could lead to damage. If safeguards systems are well designed and highly reliable, damage SOT outcomes are expected to be a very small fraction of all the possible SOT outcomes, yet essential to safety assessment.

On the other hand, protective actions, being generally aggressive, are activated if and only if certain conditions are fulfilled. These conditions, usually implemented as plant alarms and/or automatic protection system set-points, can be generically called "stimuli" of the protective actions (Labeau and Izquierdo, 2005) and their fulfillment can be referred to as "stimulus activations".

[2] Such type of systems is referred in some contexts as hybrid systems.

Please cite this article in press as: Galushin, S.E., et al., Transmission Functions and its application to the analysis of time uncertainties in Protection Engineering. Process Safety and Environmental Protection (2013), http://dx.doi.org/10.1016/j.psep.2013.07.004