CHEMICAL ENGINEERING TRANSACTIONS
VOL. 33, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Enrico Zio, Piero Baraldi

ISBN 978-88-95608-24-2; **ISSN** 1974-9791
DOI: 10.3303/CET1333089

Dynamic Reliability by Using Simulink and Stateflow

Huilong Zhang*[,a,c], Benoîte de Saporta[b,c], Francois Dufour[a,c], Gilles Deleuze[d]

[a]Univ. Bordeaux, IMB UMR 5251, 33400 Talence, France
[b]Univ. Bordeaux, Gretha UMR 5113, 33600 Pessac, France
[c]INRIA Bordeaux Sud-Ouest, 33400 Talence, France
[d]EDF R&D, 1 Avenue du Général de Gaulle, 92141 Clamart, France
Huilong.Zhang@math.u-bordeaux1.fr

The safety of high criticity industrial systems relies heavily on relatively complex programmed systems. Due to the complexity of the interactions between physical processes and their control, classical methodologies such as even- trees/fault-trees or Petri nets may not represent adequately the dynamic interactions existing between the physical processes (modeled by continuous variables) and the functional and dysfunctional behavior of its components (modeled by discrete variables). These hybrid systems can be mathematically modeled by piecewise deterministic Markov processes. To illustrate our approach, we present an academic problem. It has already been extensively studied in the literature under the name “heated hold-up tank” (Marseguerra, 1994; Marseguerra et al., 1995; Zhang et al., 2009).

1. Introduction

A current challenge in reliability analysis today is to take into account the dynamic behavior of systems. The modeling is a key step in order to study the properties of the involved physical process. It appears now necessary to take into account explicitly and in a realistic way the dependencies, in other words the dynamic interactions existing between the physical parameters (for example: pressure, temperature, flow rate, level) of the process supported by the system and the functional and dysfunctional behavior of its components. For a large class of industrial processes, the layout of operational or accidental sequences generally comes from the occurrence of two types of events:

- The first type is directly linked to a deterministic evolution of the physical parameters of the process,
- The second type of events is purely stochastic. It usually corresponds to random demands or failures of system components.

It is well known that the classical methods used in systems reliability field, such as combinatory approaches (fault trees, event trees, reliability diagrams) or Markov and semi-Markov models are not able to correctly model physical processes involving deterministic behavior.

In 1980, M.H.A. Davis (1993) introduced in probability theory the Piecewise Deterministic Markov Processes (PDMP) as a general class of models suitable for formulating optimization problems in queuing and inventory systems, maintenance-replacement models, investment scheduling and many other areas of operation research. The notion of piecewise deterministic process is very intuitive and simple to describe. The state space of this system is given, for example, by a subset E of the set R^d. Starting from x in E, the process follows a deterministic trajectory (given, for example, by the solution of an ordinary differential equation) until the first jump time T_1 which occurs either spontaneously in a random manner or when the trajectory hits the boundary of E. In both cases, a new point is selected by a random operator and the process restarts from this new point. Consequently, if the parameters of the physical process under consideration are described by the state x of a piecewise deterministic process, between two jumps the system follows a deterministic trajectory.
The approach combined with Simulink and Stateflow offers interesting perspectives for dynamic reliability analysis for hybrid system. The continuous part of the system can be modeled by Simulink block while its discrete part can be modeled by Stateflow charts. In the first part of the paper, a benchmark system is

Please cite this article as: Zhang H., De Saporta B., Dufour F., Deleuze G., 2013, Dynamic reliability by using simulink and stateflow, Chemical Engineering Transactions, 33, 529-534 DOI: 10.3303/CET1333089

described and modeled by a PDMP. In the second part, the simulation procedure based on Simulink/Stateflow is proposed to evaluate the cumulative probability of three undesirable events inherent to the hybrid system. In the last part, to validate numerically our approach, we compare with the results obtained in (Zhang et al., 2009).

2. The heated hold-up tank problem

The system was first introduced by Aldemir (1987) where only one continuous variable (liquid level) is taken into account, and then in (Marseguerra, 1994) and (Marseguerra et al., 1995) where the second variable (temperature) is introduced. They have tested various Monte Carlo approaches to reliability and safety analysis. Tombuyses et al., (1996) have used the same system to present continuous cell- to-cell mapping Markovian approach (CCCMT). The holdup tank example has been widely studied in the literature (not exhaustive) (Siu, 1994, Cojazzi, 1996, Dutuit et al., 1997, Schoenig et al., 2006, Li et al., 2011, de Saporta et al., 2012).

The system consists of a tank containing a fluid whose level is controlled by three components: two inlet pumps (Unit 1 et 2) and one outlet valve (unit 3) . Each component has four states: OFF, ON, Stuck OFF, and Stuck ON. The transition among different states is schematized by the right hand side of figure 1. It is an inhomogeneous Poisson jumps process. A thermal power source heats up the fluid, the failure rates λ^c of the components depends on the temperature: $\lambda^c = a(\theta)\hat{\lambda}^c, c = 1,2,3$, where

$$a(\theta) = (b_1 e^{b_c(\theta-20)} + b_2 e^{-b_d(\theta-20)})/(b_1 + b_2) \tag{1}$$

with

$$b_1 = 3.0295, b_2 = 0.7578, b_c = 0.05756, b_d = 0.2301$$

$$\hat{\lambda}^1 = 2.2831 10^{-3} h^{-1}, \hat{\lambda}^2 = 2.8571 10^{-3} h^{-1}, \hat{\lambda}^3 = 1.5625 10^{-3} h^{-1}.$$

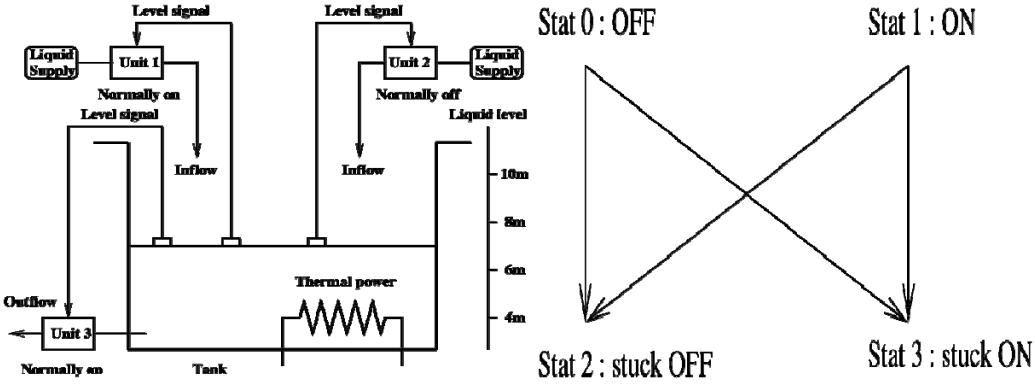


Figure 1: Heat holdup tank and states transitions of the components

A control law is used to modify the state of the components to keep the liquid between two limits : 6 meters and 8 meters.

- Law 1: If the liquid level drops under 6 meters, the components 1,2,3 are put respectively in the state ON,ON and OFF (if they are not stuck ON of OFF)
- Law 2: if the liquid level rises above 8 meters, the components 1,2,3 are put respectively in the state OFF,OFF and ON (if they are not stuck ON of OFF)

The two continuous variables are the liquid level h and the temperature θ, which are both functions of the state of the components. At t = 0, the system is assumed to be in the equilibrium state, i.e. the components are in state (ON, OFF, ON), the temperature θ is 30.9261 ^{0}C and the liquid level h is 7 meters. The variables (h(t), θ(t)) satisfy the following differential equations

$$\begin{cases} dh/dt = r_1(v) \\ d\theta/dt = (r_1(v) - r_3(v)\theta)/h \end{cases} \tag{2}$$

where $v = (v_1, v_2, v_3)$

$$v_c = \begin{cases} 0 & if\ c\ is\ OFF\ or\ stuck\ OFF \\ 1 & if\ c\ is\ On\ or\ stuck\ ON \end{cases} \tag{3}$$

and

$$r_1(v) = (v_1 + v_2 + v_3)G,\ r_2(v) = (v_1 + v_2)G\theta_{in} + 23.88915,\ r_3(v) = (v_1 + v_2)G \tag{4}$$

with $\theta_{in} = 15, G = 1.5$.

Physically, the discrete variable v denotes the different regimes of the system and $r_c,\ c = \{1,2,3\}$, are constant in each regime. The system (2) is derived from the mass and energy conservation laws. We are interested in three possible Top Events: dry out (h ≤ 4 meters), overflow (h ≥ 10 meters) and hot temperature ($\theta \geq 100^0 C$), $p_1(t)$, $p_2(t)$ and $p_3(t)$ are the cumulative probabilities of these Top Events at time t. Let $x_0 = (h_0, \theta_0), v = (1, 0, 1)$ be the initial condition of the process variables at time t=0. According to the configuration of the system, the coefficients of the differential equation system can be zero, and there exist four different behaviors for (h(t), θ(t)) and for every case, an analytical solution exists. The heated tank problem can be modeled rigorously by piecewise deterministic Markov processes (PDMP) (Davis, 1993). One can find the detail in (Zhang et al., 2009), where a Monte Carlo simulator is implemented using the analytical solution. Unfortunately, in general, especially in industrial applications, analytical solutions do not exist, numerical approximation has to be used to solve the differential equation.

3. Simulink/Stateflow implementation

A Simulink/Stateflow design is represented graphically as a diagram consisting of inter connected Simulink blocks. It represents the time-dependent mathematical relationships between the inputs, states and outputs of the design.

Time Discretization: Let Δt be the time step size, the objective of our approach is to calculate the couple (h(t),θ(t)) and simulate the probability of failure of each component at every time step. Let T be the failure time of a component, let λ(t) be the failure rate, then the density function and distribution function of T are defined respectively by $f(t) = \lambda(t)e^{-\int_0^t \lambda(s)ds}$ and $F(t) = 1 - e^{-\int_0^t \lambda(s)ds}$, the probability that the component fails during time interval [t, t + Δt) given that T ≥ t is defined by

$$P(t \leq T < t + \Delta t \mid T \geq t) = \frac{F(t+\Delta t) - F(t)}{F(t)} = \frac{e^{-\int_0^t \lambda(s)ds} - e^{-\int_0^{t+\Delta t} \lambda(s)ds}}{e^{-\int_0^t \lambda(s)ds}} = 1 - e^{-\int_t^{t+\Delta t} \lambda(s)ds} \tag{5}$$

Here we considered that the failure rate is defined by $\lambda^c = a(\theta)\hat{\lambda}^c, c = 1,2,3$ and θ(t) is piecewise constant in [t, t + Δt) so that this probability can be estimated by $1 - e^{-\hat{\lambda}^c a(\theta(t))\Delta t}$.

Let's present now the detail of our approach. The global Simulink/Stateflow scheme of the simulator is presented in the left part of the Figure 2. It is composed of three principal sub blocks, named respectively Diff. Equation, Gamma Function, and Controller.

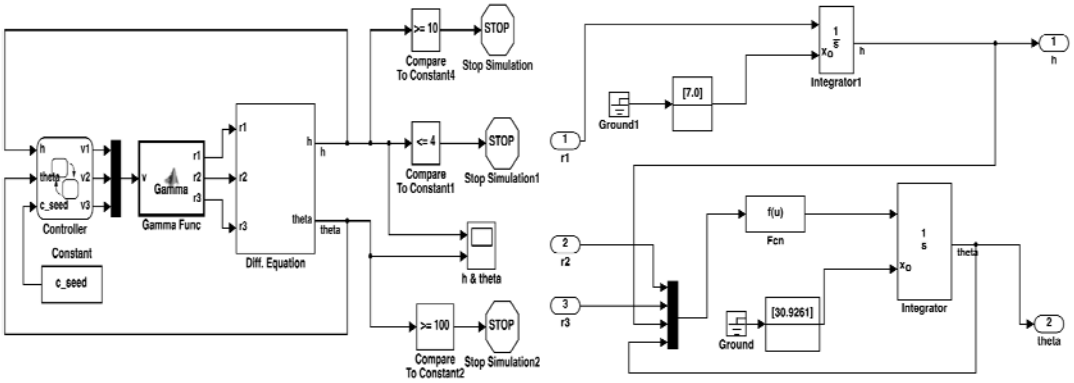


Figure 2: Simulink/Stateflow model and implementation of differential equation

Differential equations solver: one of the reasons for which we chose this software is that it is a powerful tool for modeling in a concise way the behavior of nonlinear differential equations. The right hand side of figure 2 shows the details of the solver. Two dependent equations are modeled. The first one ($dh/dt = r_1(v)$) represents liquid level, with 7.0 as initial condition. The second one ($d\theta/dt = (r_2(v) - r_3(v)\theta)/h$) represents the

temperature, with 30.9261 as initial condition. As illustrated, the Matlab function f(u) has four input variables : u(1)=r2, u(2)=r3, u(3)=h and u(4)=θ, the function is defined by f(u) = (u(1)− u(3)*u(4))/u(2). At every time step, according to the flow rate values (r_1, r_2, r_3), the solver calculate the variables (h,θ). Simulink proposes different solvers, we chose an order four Runge-Kutta solver.

Gamma Function: the objective of this Matlab function is to calculate (r_1, r_2, r_3), the flow rate of the three valves.

```
function [r1 r2 r3] = Gamma(v)
r1 = (v(1)+v(2)-v(3))*1.5;
r2 = (v(1)+v(2))*1.5*15+23.88915; r3 = (v(1)+v(2))*1.5;
```

It has v=(v_1, v_2, v_3) as input variables, which represent discrete state of three valves.

Controller: the discrete part of this hybrid system is modeled by the Stateflow charts Controller. Figure 3 illustrates the implementation. The input variables are (h, θ) and c_seed. We distinguish four parallel states: valveI,2,3 and ValveValue. Each valve has four states: On, Off, Stuck− On and Stuck− off, the transition among the states is conditioned by the two types of event: the crossing of a threshold of liquid level h or the failure. At the beginning of the simulation, the state of the chart is (Valve1.On, Valve2.Off, Valve3.On), which means the state of three valves is (ON, OFF, ON). It will not be changed until an event occurs. For example, suppose at time t the valve1 is in state On, two kinds of events can induce the transition of state.
Deterministic event: when the liquid level reaches 8 m.
Stochastic event: when the valve1 fails (to Stuck− On or Stuck− Off).
To simulate the second event, a random Bernoulli variable B(p) is drawn (implemented by a Matlab function failure(lamb)) with parameter $p = 1 - e^{-\hat{\lambda}^c a(\theta(t))\Delta t}$. For instant, if the result x of the drawn is 1, then the valve1 fails, a transition to Stuck− On will be done. As the liquid level h(t) and temperature θ(t) are calculated at every time step by the Simulink block Diff.Equation, the state transition (failure, level control) of the three valves is then simulated dynamically. The output variable is v=(v_1, v_2, v_3), it is calculated by the fourth parallel state ValveValue at each time step by using Eq(3).
The constant c_seed is added in order to initialize the random generator. The simulation is stopped whenever one of the three conditions is reached: h≥10, h≤4 and θ≥100, otherwise the simulation will stop at the final time 1000 h.

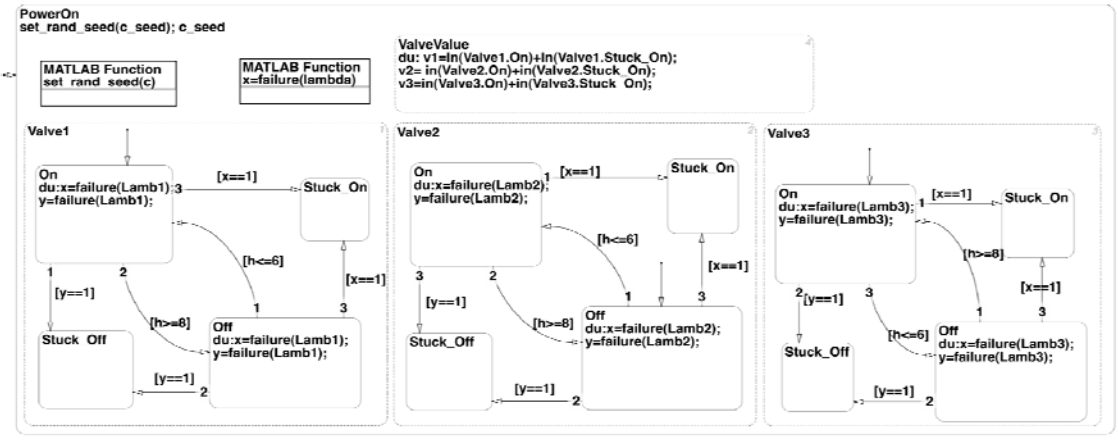
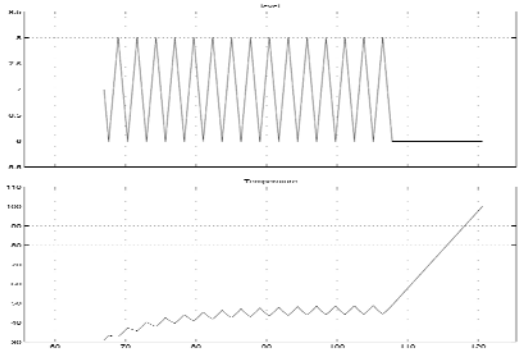


Figure 3: Stateflow chart: Level controller

4. Numerical results

The trajectories of (h(t), θ(t)) can be monitored by a Scope block. The left hand side of figure 4 illustrates an example, the simulation is stopped at t = 120.61 by a Top Event θ ≥ 100.



T	Dry out		Hot temp.		Overflow	
(h)	ref.	Sim	ref.	Sim	ref.	Sim
200	0.059	0.059	0.143	0.143	0.337	0.341
400	0.087	0.086	0.161	0.161	0.442	0.446
600	0.094	0.093	0.163	0.163	0.473	0.477
800	0.096	0.095	0.163	0.163	0.484	0.487
1000	0.096	0.095	0.163	0.163	0.488	0.491

Figure 4: A trajectory example and cumulative probability of Top events

A small sample of results is presented in the table in Figure 4. They correspond to the occurrence probabilities of the above top-events estimated from both the reference solution from (Zhang et al., 2009) and the Simulink/Stateflow approach. The cumulative probabilities of the Top Events can be estimated by using a large number of histories. Figure 5 gives the results from a 10^3 and a 10^5 histories sampling compared with the reference solution. The time step size is fixed as 0.01h. We can observe the convergence of the method with respect to the number of histories. We use the results from 10^7 histories

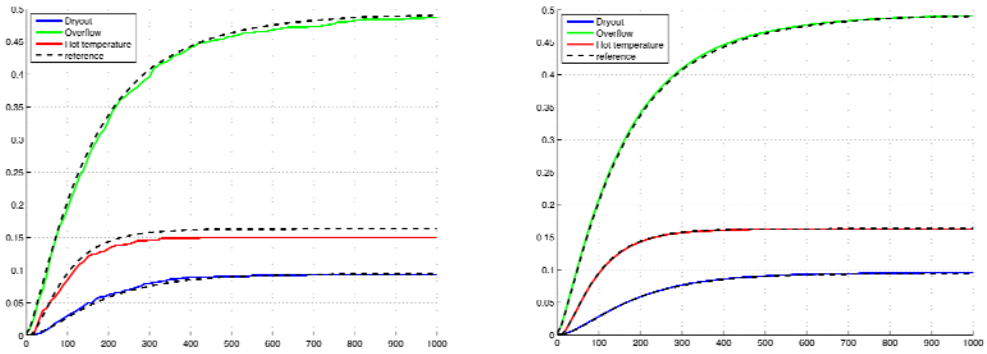


Figure 5: Results for N=10e3 and N=10e5 compared with reference solution

obtained in (Zhang et al., 2009) as our reference solution.

5. Conclusions

In this paper, we are interested in an academic example. It has only 3 components and 64 discrete states. However, despite its simplicity, this example is considered as a good benchmark in reliability-community for several reasons: it is not trivial because it has two continuous variables, the differential equations have analytical solutions, which provides a reference result and facilitates comparisons of different approaches.
But from the point of view implementation, some methods proposed in the literature are not feasible in industrial scale due to the combinatorial explosion problem. A judicious choice in software becomes crucial. The modeling by PDMP applies very well to problem of dynamic reliability. The approach combined with Simulink/Stateflow allows building an interactive simulator. It has many merits: the upgrade maintenance of the simulator is easy and intuitive; there is no limit in the number of components; several continuous variables can be simultaneously taken into account.
The approach proposed in this paper has been applied to an industrial example (Zhang et al., 2012), where a control system of water level in the steam generator (SG) in the secondary circuit of a nuclear power plant is considered. In particular

- 7 components are taken into account, the total number of possible combinations for all components is 9.09E+11.
- 4 continuous variables are modeled, they follow a system of non-linear differential equations.
- A PID controller is integrated in the system.

We have simulated the complete behavior of the system, including sensors and a continuous-time PID controller. A 18 months scenario takes around 10-20 s per history. Numerical experiments show that this approach is well suited for treating this class of hybrid systems of industrial size.
The main disadvantage of this approach is execution time. For the hold-up tank test case that we handled, 10^5 histories are simulated in about 23 h (on a laptop), while a C++ simulator (Zhang et al., 2009) to this takes only 16 min. We have partially solved the problem by using the parallel computing toolbox of Mathworks. A computer equipped with 12 cores, reduced the computation time to 2.4 h.

References

Aldemir T., 1987, Computer-Assisted Markov Failure Modeling of Process Control Systems. IEEE Transactions on Reliability, 36(4), 133–144.

Cojazzi G., 1996, The DYLAM approach for dynamic reliability analysis of systems. Reliability Engineering and System Safety, 52, 279-296.

Davis M., 1993, Markov models and optimization. London: Chapman and Hall.

De Saporta, B., Zhang H., 2012, Predictive maintenance for the heated hold-up tank. In Proceedings of PSAM11-ESREL12. Helsinki.

Dutuit Y., Chatelet E., Signoret J., Thomas P., 1997, Dependability modeling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering and System Safety, 55, 117-124.

Li J., Moslehb A., Kanga R., 2011, Likelihood ratio gradient estimation for dynamic reliability applications. Reliability Engineering and System Safety, 96, 1667-1679.

Marseguerra M., 1994, Approximated physical modeling in dynamic PSA using artificial neural networks. Reliability Engineering and System Safety, 45, 47–56.

Marseguerra M., Zio E., 1995, The cell-to-cell boundary method in Monte Carlo based dynamic PSA. Reliability Engineering and System Safety, 45, 199–204.

Schoenig R., Aubry J., Cambois T., Hutinet T., 2006, An aggregation method of Markov graphs for the reliability analysis of hybrid systems. Reliability Engineering and System Safety, 91, 137-148.

Siu N., 1994, Risk assessment for dynamic systems: an overview. Reliability Engineering and System Safety, 43, 43-73.

Tombuyses B., Aldemir T., 1996, Continous cell-to-cell mapping and dynamic PSA. In Proceedings of ICONE 4 conference, 431–438.

Zhang H., Dufour F., Dutuit Y., Gonzalez, K., 2009. Piecewise deterministic Markov processes and dynamic reliability. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 222(4), 545–551.

Zhang H., De Saporta B., Dufour F., Deleuze G., 2012, Dynamic reliability: towards efficient simulation of the availability of a feedwater control system. In Proceedings of NPIC & HMIT 2012, 714-723.