In the reliability modeling of complex control systems, 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). This paper proposes a framework for modeling and simulation of a water level control system in the Steam Generator (SG) of the secondary circuit of a nuclear power plant. We have developed a complete benchmark case. The behavioral model of SG is obtained from a linearized model published in 2000 by EDF [1,2]. Four physical variables (steam flow rate, water flow rate, steam-water level, water level) are modeled; they follow a system of linear differential equations with piecewise constant coefficients, coupled with a PID controller that regulates the water level in the SG. Detailed description of the components, failure modes and control laws of the principal components is presented. For modeling the system, we use the Piecewise Deterministic Markov Processes (PDMP) framework and for implementation we chose Simulink associated with Stateflow. PDMP offer a very general modeling framework to deal with dynamic reliability problems; Simulink is an appropriate tool to simulate non linear differential equations and their controller, while Stateflow implementation is appropriate for finite state machine descriptions of different components.

Key Words: Dynamic PRA/PSA, Piecewise Deterministic Markov Processes

1 INTRODUCTION

Hybrids systems are described by continuous variables, deterministic events and stochastic events (e.g. control logic and mechanical parts failures, unplanned variations of operational profile...). 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.

Unfortunately, the static methods used for systems reliability modeling, such as combinatorial approaches (fault trees, event trees, reliability diagrams) are not relevant to model hybrid systems. This is a current challenge in reliability
analysis, and requires the development of so-called “Integrated Deterministic-Probabilistic Safety Analysis (IDPSA). The need of IDPSA methods comes from the observation that static methods applied in PSA are limited to find time dependent interactions and unknown vulnerable sequences regarding physical phenomena, control logic, operator actions, equipment failures [8].

The benchmark system that we study is a Feedwater Control System (FCS) for the Steam Generator (SG) in the secondary circuit of a nuclear plant. The mission of the system is to maintain the water level in the steam generator around a reference position. The mission fails if the water level rises above or falls beyond threshold limits. This test case has the advantage of being representative of a real system and to cover most of the situations encountered in the dynamic reliability literature. A similar benchmark system was described by the U.S. Nuclear Regulatory Commission [4] where two approaches for dynamic reliability were compared: DFM (Dynamic Flowgraph Methodology) and Markov/CCMT (Cell-to-Cell Mapping Technique). But the date released by the NRC report did not permit us to reconstruct the model.

The work presented here is a continuation of a series of works already realized within the INRIA team CQFD. They are intended to illustrate the efficiency of a method combining the modeling power of Piecewise Deterministic Markov processes (PDMP) and the Monte Carlo computational implementation, to treat certain dynamic reliability problems. We have in the past modeled and simulated systems of "academic" size [6] and "industrial" size [5], where implementations were done in C++ or Matlab. But to model the Feedwater Control System, we chose the software Simulink/Stateflow of Mathworks. This paper is organized as follows. Section 2 briefly presents the Piecewise Deterministic Markov processes (PDMP). Section 3 gives the functional description of our benchmark. Section 4 then presents the implementation by Simulink/Stateflow. Section 5 shows some numerical results. Finally, section 6 presents our conclusions.

2 PIECEWISE DETERMINISTIC MARKOV PROCESSES

PDMP provide a very general modeling framework to deal with dynamic reliability problems. Let M be the finite set of the possible regimes of the system. For all m in M, let E_m be an open set of $\mathbb{R}^d$. A Piecewise deterministic Markov process is defined from the three local characteristics ($\Phi$, $\lambda$, Q) where

- the flow $\Phi : M \times \mathbb{R}^d \times \mathbb{R} \to \mathbb{R}^d$ is continuous and for all s, t $\geq 0$, $\Phi(s, t+s) = \Phi(\Phi(s, t), t)$. It describes the trajectory of the deterministic process between jumps. For all $(m, x)$ in $M \times E_m$, we set $t^*(m, x) = \inf \{ t > 0 : \Phi(m, x, t) \in \partial E_m \}$ the time to reach the boundary of the domain.
- the jump intensity $\lambda$ characterizes the frequency of jumps. For all $(m, x)$ in $M \times E_m$ and $t \leq t^*(m, x)$, we set $\mathcal{L}(m, x, t) = \int_0^t \lambda(\phi(m, x, s)) ds$
- the Markov kernel Q represents the transition measure of the processes that allows to select the new position after each jump.

The trajectory $X=(m_n, x_n)$ of the process can be defined iteratively. We start from an initial point $X_0 = (k_0, y_0)$ with $k_0 \in M$ and $y_0 \in E_k$. The first jump time $T_1$ is determined by the distribution $P_{(k_0, y_0)}(T_1 > t) = \begin{cases} e^{-\lambda(k_0, y_0)}, & t < t^*(k_0, y_0) \\ 0, & t \geq t^*(k_0, y_0) \end{cases}$

On the interval $[0, T_1)$, the process follows the deterministic trajectory $m_n = k_0$ and $x_n = \Phi(k_0, y_0, t)$. At the random time $T_1$, the process has a jump. The regime changes and the process is then reset at $X_{T_1}$, a random variable that follows the law given by $Q_{k_0}(\Phi(k_0, y_0, T_1), \cdot)$. We then similarly draw a new jump time $T_2 - T_1$ and on the interval $[T_1, T_2)$ the process follows the trajectory $m_1 = k_1$ and $x_1 = \Phi(k_1, y_1, t - T_1)$. This builds iteratively the PDP.

A particularity of the steam generator system is that it is regulated. The flow $\Phi$ is thus the solution of a differential equation controlled by a PID controller. It admits no analytical solution and will be numerically approximated at each time step. The reason why we choose the PDP model is twofold. First, it provides a modeling framework that is both general and accurate. Second, this model offers the perspective in the future to perform optimal control: optimal stopping, predictive maintenance [7], etc.
3 FUNCTIONAL DESCRIPTION

We have modeled a part of the secondary circuit of a pressurized water reactor. It is composed of seven components: one passive system representing the whole steam transport system (VVP), three extraction pumps (CEX), two feeding turbo pumps (TPA), and one water flow regulation valve (ARE). The rest of the secondary circuit does not interest us for the test case as it has no direct influence on the reliability and safety of the circuit. The reliability diagram we modeled is given in Figure 1.

![Figure 1. Reliability diagram for the mechanical and electromechanical systems of FCS.](image)

3.1 Description of the system

The VVP barrel maintains the steam flow to the turbo pumps and dryers. A breakdown in the barrel VVP is a critical point of failure and represents a minimum level of system reliability. The three pumps CEX maintain the vacuum in the condenser (upstream of VVP) and ensure a flow of feeding water. They are redundant in 2/3. The third pump is stopped, in standby. It is started when one of the other pumps fails. A failed pump, once repaired, remains in standby. The two turbo pumps TPA work together, they provide the common pressure to the SG, discharged into a common cylinder integrated in the VVP. In the case of failure of a TPA, the second one switches over speed and provides some of the charge. We consider in this model that the power of the installation decreases automatically to 60% when only a single TPA works. Finally, the actuator (ARE) is used to command the feed water flow rate in the SG. It consists of a main valve and a bypass valve. A logic sequence determines the openings and closing of the individual valves as a function of the power of the installation.

In our benchmark system, four physical processes are considered: the feed water flow rate \( Q_{\text{fe}} \), the steam flow rate \( Q_s \), the narrow range water level \( N_{\text{ge}} \) and the wide range water level \( N_{\text{gl}} \). A PID controller is used to maintain the water level within limits of reference-points. The behavioral model of the SG is obtained from a non-linear model published in 2000 by EDF [1, 2]. The general control strategy consists in maintaining the narrow range and wide range water levels within limits of their set points. This can be accomplished by concentrating the control effort on the single controlled variable: the narrow range water level \( Q_{\text{ge}} \). Figure 2 shows the basic PID feedback control structure.

![Figure 2. Basic feedback structure of the PID controller](image)
3.2 Steam generator level control model

The model used in this study for the purpose of controller design, is a somewhat simplified version of the Irving model [1]. It was developed by the Research and Development division of EDF. The detailed model for the Steam Generator can be found in [2]. Such theoretical models use fundamental conservation equations for mass, energy, momentum, volume and basic thermodynamic principles. It is a simple fourth-order model. We will give a brief description. The relationship among \( N_{ge}, Q_e, Q_v \), and \( N_{gf} \) can be modeled by the following transfer functions:

\[
N_{ge}(s) = \frac{1}{T_n s} \left( \frac{Q_e(s)}{1 + \tau s} - \frac{1 - F_g T_n s}{1 + T_g s} Q_v(s) \right), \quad N_{gf}(s) = \frac{1}{T_{int} s} \left( Q_e(s) - Q_v(s) \right). \quad (1)
\]

The parameters \( T_n, F_g, T_h, \tau \) are functions of the operating power \( P_n \) and are summarized in Table I. Note that \( T_g = 1.429 \) and \( T_{int} = 20 \) are constants. The term \( 1 - F_g T_g S \) is incorporated to account for the modeling of the two-phase swell and shrink effects. Due to proprietary reasons, the model discussed in this paper is a scaled and modified version of the model used by EDF.

### Table I. Parameters variation over the power range

<table>
<thead>
<tr>
<th>( P_n ) (%)</th>
<th>3.2</th>
<th>4.1</th>
<th>9.5</th>
<th>24.2</th>
<th>30</th>
<th>50</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T_n )</td>
<td>5.14</td>
<td>8.00</td>
<td>9.00</td>
<td>6.29</td>
<td>5.71</td>
<td>5.71</td>
<td>5.71</td>
</tr>
<tr>
<td>( F_g )</td>
<td>13.0</td>
<td>18.00</td>
<td>10.00</td>
<td>4.00</td>
<td>4.00</td>
<td>4.00</td>
<td>4.00</td>
</tr>
<tr>
<td>( T_h )</td>
<td>24.29</td>
<td>8.00</td>
<td>4.29</td>
<td>1.43</td>
<td>1.14</td>
<td>0.71</td>
<td>0.71</td>
</tr>
<tr>
<td>( \tau )</td>
<td>1.43</td>
<td>1.43</td>
<td>1.43</td>
<td>4.29</td>
<td>4.29</td>
<td>4.29</td>
<td>4.29</td>
</tr>
</tbody>
</table>

Denoting the water levels by \( y_1 = N_{ge} \) and \( y_2 = N_{gf} \) and the steam and feed-water flow-rates by \( d = Q_v \) and \( u = Q_e \), we have following equivalent state-space form:

\[
\dot{x}(t) = \begin{bmatrix} 0 & 0 & 0 & \frac{1}{T_n} \\ 0 & -\frac{1}{T_h} & 0 & -\frac{1}{T_v} \\ 0 & 0 & -\frac{1}{T_v} & 0 \\ 0 & 0 & 0 & -\frac{1}{\tau} \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} u(t) + \begin{bmatrix} \frac{1}{T_n} \\ 0 \\ 0 \\ \frac{1}{T_{int}} \end{bmatrix} d(t),
\]

\[
y(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} = \begin{bmatrix} \frac{1}{T_n} & 1 & 1 & 0 \\ T_{int} & 0 & 0 & \frac{\tau}{T_{int}} \end{bmatrix} x(t).
\]

3.3 Reliability data and state graphs

Reliability data and state graphs have been defined for each component. We provide in Table II and Figure 3 the details for the simplest case, the VVP. The necessary data for the other sub systems are much more numerous and will not be presented in this paper due to obvious reasons of clarity. The worst case is that of the ARE with four graphs and more than a dozen states and thirty parameters.

### Table II. Reliability data example (VVP) (Failure rate=2.17e-5/h)

<table>
<thead>
<tr>
<th>Mesh</th>
<th>Contribution to the failure rate</th>
<th>Pfd</th>
<th>MTTR</th>
<th>Effect</th>
<th>Mode of failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outflow</td>
<td>89%</td>
<td>na</td>
<td>12</td>
<td>Automatic reactor trip</td>
<td>Mode I</td>
</tr>
<tr>
<td>Break</td>
<td>11%</td>
<td>na</td>
<td>168</td>
<td>Automatic reactor trip</td>
<td>Mode II</td>
</tr>
</tbody>
</table>
3.4 Test scenario

We consider the following scenario, illustrated in Figure 4. After a piecewise linear rise lasting 24 hours, the system reaches its stationary state, 100% $P_n$ and remains there for 18 months, followed by a descent of 24 hours. The objective is to simulate the behavior of the system subject to random failures. The simulation is stopped when an automatic reactor trip (RT) occurs. In this scenario, we suppose that the control law of the two ARE valves satisfies the following logic: when the operation power is in $[0\%, 2\%]$, a supplement system (ASG) is applied to control the feed water rate, between $[2\% 15\%]$, the bypass valve is used, and if $P_n$ is above 15%, the bypass valve is turned off and the main valve comes into operation.

Figure 4. Test case scenario

4 SIMULINK/STATEFLOW IMPLEMENTATION

The global scheme of the simulator is presented in Figure 5. The Ramp block is parameterized to generate a constantly increasing or decreasing signal ($P_n$). The range of the ramp is restricted to $[0, 100]$ by the saturation block. Four output signals $N_{ge}$, $P_n$, $N_{gi}$, and RT (automatic reactor trip) are computed, the last one stopping the simulation when an RT occurs.

Figure 5. Global scheme of simulator
The Steam generator is fully modeled by the subsystem SG, presented in Figure 6. It consists of

- a Stateflow chart named *installation*, which includes the seven components VVP, CEX, TPA and ARE described above. This block is activated at each time step, and also whenever the power \( P_n \) crosses one of the thresholds 2%, 15%.

- the Steam Generator modeled by the \( gv \) block with two inputs \( (Q_v,Q_e) \) and two outputs \( (N_{ge},N_{gl}) \). This system obeys a system of differential equations whose coefficients depend on \( Q_v \). Here the operation power \( P_n \) and steam rate \( Q \) share the same signal, because they are supposed to be proportional.

- a PID controller, which input is the difference between the set point \( P_n \) and \( N_{ge} \), and which output is \( Q_e \), the flow rate of feed water injected into the SG. The variable \( Q \) represents the disturbances from ARE.

A main advantage of Simulink/Stateflow modeling is that it takes the form of an interactive graph, which makes easy the understanding of the model. If the system works in nominal mode, when no component is down, the water level is controlled by the PID controller. If a component fails, it can either cause an AAR or a minor fault. In the former case the simulation is stopped, in the letter case the simulation goes on, the component is under repair, a decreasing followed by an increasing ramp is scheduled if necessary.

The Stateflow chart installation models the discrete behavior of the SG. It includes all the seven discrete components ARE, VVP, 3 CEX and 2 TPA, see Figure 7. We will present in detail here only two components: VVP and CEX.
4.1 VVP Modeling

This component has three possible states (OK, Outflow, Break), see Figure 8. The time spent in each state is exponentially distributed. When this component is active, its default state is OK. Two random variables are then drawn, $x = \text{E}(2.17e^{-5}/\text{h})$ represents an exponential distribution with parameter $\lambda = 2.17e^{-5}/\text{h}$, and $p = B(0.89)$ is a Bernoulli draw. When the time spent in this state exceeds $x$, the transition after $(x, \text{sec})$ occurs. The state of the component switches to Outflow if $p=1$ or to Break if $p=0$. In this latter case, an RT signal is send to stop the simulation. The codes 301 and 302 can record the failed component and the cause of the failure, for future Monte Carlo analysis.

![Figure 8. VVP Model](image)

4.2 CEX Modeling

The principle of operation of the CEX is similar, but much more complex. Figure 9 illustrates the implementation of a CEX, this is indeed the details of CEX1 found in Figure 7. The other two CEX are almost identical (copy-paste), only the initial conditions are different. In the initial state, two CEX are in operation, the third is in standby.

![Figure 9. CEX implementation](image)
5 NUMERICAL RESULTS

The total duration of the scenario is 18 months. There are two types of regimes: transient and steady. When the system is in the transient regime, the water level $N_{ge}$ and power $P_n$ vary rapidly. To follow this command, one must choose a discretization time step small enough (0.6 seconds), otherwise the PID controller loses its stability. In the steady state, all physical variables remain constant, only the component failures affect the system state. As the system is very reliable, the nominal duration is often very long and a small time step is not pertinent because it dramatically slows down the simulator. We propose a specific technique to solve this problem by using inhomogeneous time steps. Two distinct Simulink models were created, the first one with the PID, and the second one without PID. This allows setting two different time steps. During the transient period, we use a time step of 0.6 seconds, and during the stationary period, a time step of 60 minutes is sufficient to simulate component failure.

To illustrate the results, we simulated a history without failure, and we set steady period to be 3 days (instead of 18 months, for illustrative reason). Figure 10 shows that the $N_{ge}$ (red) coincides well with the reference point (blue).

![Figure 10. Reference point and $N_{ge}$ level](image)

On a total of 4000 simulated histories, 2190 Reactor Trips (RT) occurred, representing a probability of 54.75%. That is to say that in this scenario the system has about one chance over two to suffer a RT, for a period of 18 months. Table III summarizes the number of RT caused by each component. It also gives the percentage of occurrence among the 2190 RT.

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Number of RT</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVP</td>
<td>792</td>
<td>36%</td>
</tr>
<tr>
<td>ARE</td>
<td>1301</td>
<td>59%</td>
</tr>
<tr>
<td>CEX</td>
<td>50</td>
<td>2.28%</td>
</tr>
<tr>
<td>TPA</td>
<td>47</td>
<td>2.1%</td>
</tr>
<tr>
<td>Total</td>
<td>2190</td>
<td>100%</td>
</tr>
</tbody>
</table>

We found no RT caused by the bypass valve ARE. This can be explained by the fact that the stay in the transitional regime is too short (48 hours) compared to the total duration (18 months) of the scenario. This failure is a rare event. We also note that many RT are caused by the barrel VVP (36%). Its failure rate (2.17e-5/h) is comparable to those of the CEX (4.35 e-5) and TPA (5.9 e-4), but these components are redundant unlike the VVP, which minimizes the RT.
Figure 11 illustrates the cumulative probability of Reactor Trips over time.

6 CONCLUSION

The modeling by PDMP applies very well to this problem of dynamic reliability. The approach combined with Simulink/Stateflow allows building an interactive simulator. It therefore offers interesting perspectives in several points of view.

- Graphical programming. The source code looks like a reliability diagram. In debugger mode, users can view the states and transitions step by step.
- Upgrade maintenance of the simulator. Components VVP, CEX, TPA, ARE can be modeled and tested separately (assuming that the other components are 100% reliable) and then combined by simple copy and paste. We can easily add in the future other components. Similarly, one can handle the problem of redundant components in pre-building a component library.
- Limiting the number of components. One of the main difficulties in hybrid system modelling, is the number of possible modes. By using this approach, there is no problem of combinatorial explosion. Indeed, the state machine of Stateflow is component oriented, that is to say that, at each time step and for each component, the simulator calculates the component state separately. It is not necessary to know a priori the number of possible states.

The main disadvantage of this approach is execution time. For the test case that we handled, a story is simulated in about 30 seconds (on a laptop), so 33 hours are necessary to run 4000 Monte Carlo runs. Experience shows that a C++ simulator dedicated to a problem of this size can probably run ten times or hundred times faster, but at the cost of a heavy investment in programming and the generated code is hardly evolutionary [5,6]. 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 3 hours.

Others perspectives can also be explored. Representing the positive feedback between system trips and reliability or of mechanical systems or sensors drift will be a step towards dynamic reliability representation. Also, from the basis of this model, simulations may be used to simulate fault inside the control logic, incl. measurement logic. Moreover, the INRIA CQFD team proposes numerical algorithms for optimal control: optimal stopping, impulse control, etc [7], that permit to study various inspection and maintenance strategies for the FCS, taking into account hybrid and

Figure 11. Cumulative probability of RT
dynamic aspects. In all these methods, the Monte Carlo simulator is the key step necessary to perform the optimization.

7 ACKNOWLEDGMENTS

This work was financed by the GIS 3SGS (Groupement d’Interêt Scientifique, Surveillance, Sûrte et Sécurité des Grands Systèmes) under contract APPRODYN (APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques).

8 REFERENCES