Safety and Reliability Assessment by using Dynamic Reliability Analysis Method

Sook-Hyung Lee, Jong-Woon Park, Jae-Cheon Lim
Institute for Advanced Engineering ,

David W Lloyd
University of Bradford

Abstract - DYLAM and its related applications are reviewed in detail and found to have many favourable characteristics. Concerning human factor analysis, the study demonstrates that DYLAM methodology represents an appropriate tool to study man-machine behaviour provided that DYLAM is used to model machine behaviour and an appropriate operator interface human factor model is included. A hybrid model which is a synthesis of the DYLAM model, a system thermodynamic simulation model and a neural network predicative model, is implemented and used to analyse dynamically the CANDU pressurizer system.

1. Introduction

In recent years the growing sentiment that system dynamic and their interaction with the random evolution of component or operator states was inadequately treated by classical methodology resulted in the development of new models. Theses new models are reviewed in this paper.

The usual approaches for probabilistic accident evaluation do not satisfactorily take into account the dynamic aspects of the random interaction between the "physics" of the transients and the "logic" of the system. The presence of control loop, the human interventions, protection system and failure delay system which the occurrence of cut set causes a top event condition only after a significant condition and a significant time delay are difficult to treat. In order to remove these limitations and to fill the gap between the need of more realistic analysis and available tools, dynamic methods have been developed. Among these dynamic methods, Discrete Event Trees (DYLAM) is particularly suitable for treating complex dynamic systems.

2 DYLAM ((DYnamic Logical Analytical Methodology)

2.1 Basic Features of the DYLAM approach

The DYLAM method can be seen as a systematic attempt to combine the stochastic and physical behaviour. It is different from other traditional techniques because the impacts of hardware system failures on the progress of physical parameters are immediately evaluated by solving the governing equations for new system conditions. Since the DYLAM consider the process simulation and changes of the system structure due to control and due to random events in a combined way, it can be seen that the DYLAM has the capability to perform a systematic and dynamic analysis.

The way in which a fault tree model is constructed and then analysed is that at first the undesired condition for the system is identified and then the fault tree is constructed by top-down deductive reasoning by linking the TOP event to its more proximate causative sub events and these down to the primary events. On the other hand, DYLAM is based on bottom up procedures for identifying the sequences of events that can lead to undesired conditions. Component modelling consists of identification of the different failure or degradation states in which a component may be. Once the components have been modelled, implicitly, the system has been described for all its possible states.

2.2 The basic steps of DYLAM

The basic steps to implement DYLAM can be summarised as follows.
(1) Component modelling
(i) constant probabilities;

(ii) stochastic transition;
(iii) functional dependent transitions;
(iv) stochastic and functional dependent transitions;
(v) conditional probability;
(vi) stochastic transition with variable transition rates;

(2) system equation modelling
To implement the system, non-linear algebraic equations have been solved. Considering large computational times, the physical models to be adopted should be as simple as possible compatible with the requirements of the analysis.

(3) Top event definition
The next step is to define undesired system states. These are defined in physical quantitative terms rather than hardware states and Top event analysis determines when a particular accident sequence simulation should be terminated.

(4) Event sequence generation rules
To exploit all possible accident sequences, following procedure is applied: Firstly starting at t=0 and some user-defined initial state; secondly the system physical model is used to determine the system variable value change in the next step Δt; thirdly at the end of the first time interval (0, Δt), all possible system state transitions are identified and transition likelihoods are calculated.

When the probability of the initial sequence becomes less than or equal to a fraction of the initial probability,

$$P(A_0, t) \leq P(A_0,t_0) * Wlim$$

where Wlim is the fractional probabilistic threshold , the branch point is triggered. Here P(A,t) consists of the probability of remaining in the initial state and birth probability for the descendent sequence. If the probability satisfies the upper condition, branch point is generated. These new states are then used to provide boundary conditions for the physical variable updating. Until an absorbing state is reached, all possible event sequences continuously are generated in the same manner.

3 Simulation

In order to better understand the features of DYLAM code when applied to the reliability analysis of a dynamic system, dynamic behaviour of a CANDU type pressurizer has been chosen as a case study. The preparation work required to implement CANDU pressurizer model using DYLAM and also describes DYLAM results obtained.

A hybrid model has been developed for assessing pressurizer transient. The hybrid model is composed of 3 parts :
i) DYLAM code;
ii) System thermodynamic simulation code;
iii) Neural network code.

Since DYLAM is a simulation-based dynamic approach, to analyse system reliability, system thermodynamic simulation code is needed. However, to reduce calculation time and to enhance the efficiency, data required for the transient behaviour of the system other than pressurizer were generated using neural technique model developed.

3.1 Neural Network Back-propagation Fitting

In developing a model which represents system behaviour, it is the topology of the network, together with the neuron, or node, processing function, which determines the accuracy and degree of the representation. Here, the neural network was used for estimating physical variables to implement

DYLAM. Generally, the power plant physics simulation codes involves of a large number of variables. That means for implementing DYLAM, it should involve considerable physical data as required restart values. When considering the computing effort, this is not an efficient way to simulate whole system on every component states in order to obtain the behaviour of a subsystem. In other word, a drawback of DYLAM is that it is a total system technique and can be relatively inefficient because of very many variables involved to get a restart values and considerable computational time required if one is wishing to focus on a particular subsystem such as the pressurizer.

When future predictions rely on previous network outputs which are fed back to network inputs, the usefulness of the neural network model has been frequently noted. Since this application describes system dynamics, the integration of dynamics into the network should be required. The most concise network representation of a dynamic system is obtained by using network inputs comprised of past input and output data. In this application (Fig. 2), the following configurations for process modelling, so called predictor structure, has been adopted.

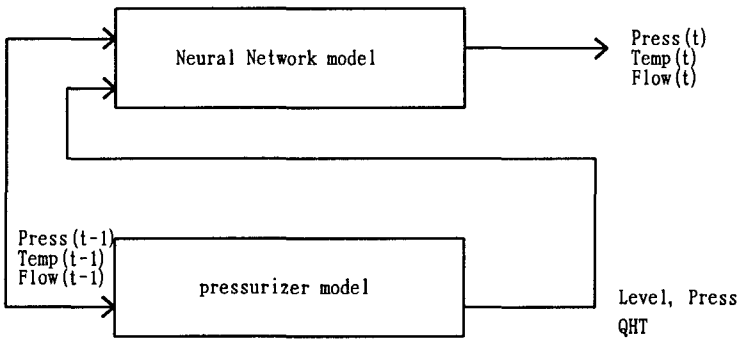


Fig. 2 Dynamic system predictor structure

In neural network model, following input data are needed

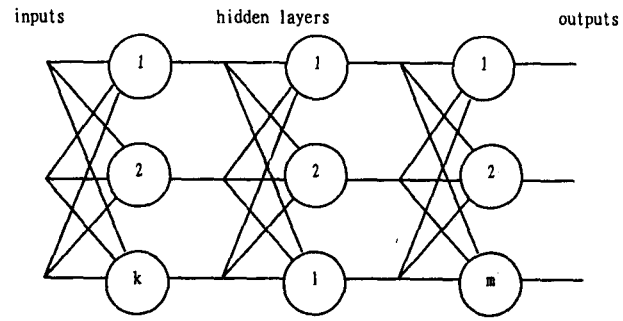
- Outlet header pressure at previous time : Press(t-1)
- Outlet header temperature at previous time : Temp(t-1)
- Surge flow rate at pervious time : Flow(t-1)
- Power fraction
- Pressure in pressurizer : Press
- Pressurizer level : Level
- heat generated in pressurizer : QHT

and following data are updated :

- Outlet header pressure : Press(t)
- Outlet header temperature : Temp(t)
- Surge flow rate : Flow(t)

These trained data generate a non linear equation. The computer code used to generate training data was the CANDU simulation code which is under development in IAE.

The following figure shows the back-propagation neural network used to model the performance of a pressurizer during the power transition.



Here k=8 (including one bias neuron)
l=8 (including one bias neuron)
m=3

Fig. 3 Typical feedforward neural architecture

3.2 DYLAM modelling

The stepback power transient procedure was chosen to simulate the behaviour of the pressurizer. Pressurizer is composed of heaters and bleed valve. In step power transient procedure, the steam bleed valve does not act. So, in this application, only heaters need to be considered. Furthermore to reduce calculation time component grouping rule was adopted. Component 1 represents a variable heater and component 2 represents four on-off heaters.

Two different top conditions depending on outlet header pressure were chosen. When the outlet header pressure is below a prescribed value, the fail Top condition is triggered. The mission time is 100 seconds and during the mission time, reactor power is reduced from full power by 60 %.

The following assumptions were made to use DYLAM :

- The components failure behaviour are statistically independent of each other
- All the components have the same nominal conditions at time zero.
- A failed component can not be repaired during the mission time.

As mentioned in the previous section, data required for the transient behaviour of the system other than pressurizer were generated using the neural technique model developed for the present neural network.

3.3 Numerical Results

To demonstrate the thermal hydraulic model of pressurizer combined with neural network modelling, stepback power transient event was simulated as a case study.

CASE 1

When the components have a probabilistic behaviour that depends on time according to constant transition rates between states, the following assumptions are made:

- All the components behave stochastically
- The failure rates of the components are $\lambda_1 = 3.0 \times 10^{-5}$, $\lambda_2 = 7.0 \times 10^{-4}$ respectively for component 1, component 2.

CASE 2

When the components have a probabilistic behaviour that depends on the time and is also functionally dependent on a physical variable of the system, the following assumptions are made:

- All the components states are subject both to stochastic transitions and to transitions due to the effects of process physical variables (TZ1)
- All the components are normal at initial pressurizer water temperature
- Functional dependent transition probabilities are :

$P_{00}(TZ1 \uparrow 305°C) = 0.8$, $P_{01}(TZ1 \uparrow 305°C) = 0.2$, $P_{10}(TZ1 \uparrow 305°C) = 0.0$, $P_{11}(TZ1 \uparrow 305°C) = 1.0$
$P_{00}(TZ1 \downarrow 305°C) = 0.8$, $P_{01}(TZ1 \downarrow 305°C) = 0.2$, $P_{10}(TZ1 \downarrow 305°C) = 0.0$, $P_{11}(TZ1 \downarrow 305°C) = 1.0$

CASE 3

When the components have a probabilistic behaviour that depends on time according to variable transition rates between states which are function of a process variable, the following assumptions are made:

- All the components have the transition rates which are function of TZ1 (including time).
- All the components are in normal condition at the initial pressurizer water temperature.
- Variable transition rates of between the states (i) TZ1 < 305°C, ii) TZ1 ≥ 305°C) are :

When TZ1 < 305°C, $\lambda_1 = 3.0 \times 10^{-4}$

$\lambda_2 = 7.0 \times 10^{-3}$

When TZ1 ≥305°C, $\lambda_1 = 3.0 \times 10^{-5}$

$\lambda_2 = 7.0 \times 10^{-4}$

4. Conclusion

From the present study, the following conclusion can be drawn :

1) Event/fault tree methodology has serious deficiencies with respect to modelling of dynamic scenarios.

2) The major advantage of DYLAM related approach is that it can realistically model physical behaviour, since it includes the physical equations governing system behaviour.

3) DYLAM has its particular value in that it can provide a comprehensive and structured approach for studying dynamic problems.

4) Use of DYLAM is unrealistic when used to analyse complex system without introducing truncation rules that can effect accuracy of representation.

5) It is demonstrated that an effective methodology for system reliability analysis is a hybrid model which is a synthesis of the following three models: i) DYLAM model; ii) system thermodynamic simulation model; iii) neural network predicative model.

6) DYLAM can be used to model human operator interface behaviour provided an appropriate human factor model.

References

[1] Amendola & G. Reina, " Event Sequences and Consequence Spectrum: A Methodology for Probabilistic Transient Analysis" , Nuc. Sci. and Eng. Vol.77, pp297,(1981)

[2] A.Amendola, "Accident Sequence Dynamic Simulation versus Event Trees", Reliability Engineering and System Safety, Vol. 22, pp3~25, (1988)

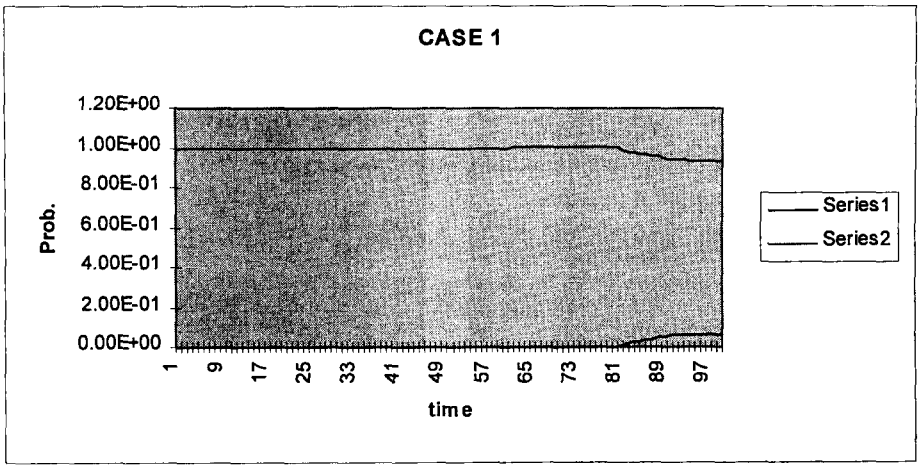
[3] Cacciabue, A.Carpinano and C.Vivalda, "Expanding the Scope of DYLAM Methodology to Study the Dynamic Reliability of Complex Systems: the case of chemical and volume control in nuclear power plants Reliability Engineering and system safety, Vol. 36, pp127~136 (1992)

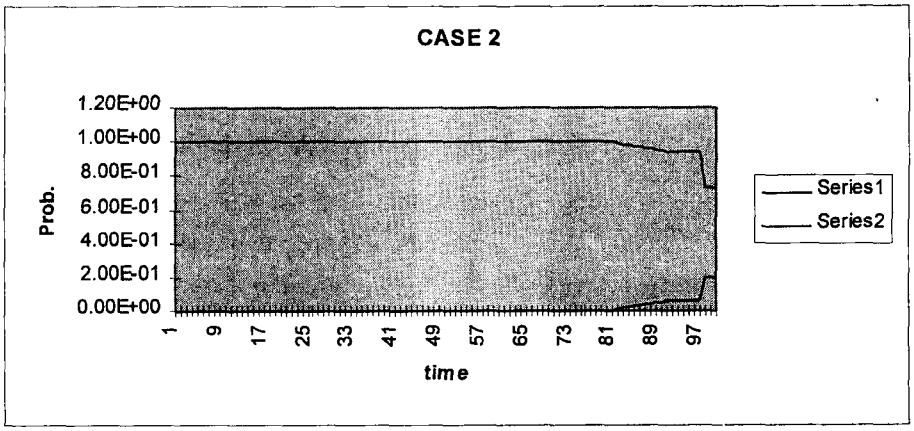
[4] Cacciabue & G. Cojazzi, "A Human Factor Methodology for Safety Assessment based on the DYLAM Approach", ISEI/IE 2502/93

[5] Cojazzi. G., Cacciabue,P.C. & Parisi, P., " DYLAM-3, A Dynamic methodology for Reliability Analysis and Consequences Evaluation Industrial Plant. Theory and How to use ", IEI/SET 2/92/92, (1993)

[6] N.Siu, " Risk Assessment for Dynamic System: An Overview", Reliability Engineering and System Safety, Vol.43, pp43, (1994)

[7] G.Cojazzi, P.C.Cacciabue, " The DYLAM Approach for the Reliability Analysis of Systems with Dynamic Interactions ", EUR 15266 EN





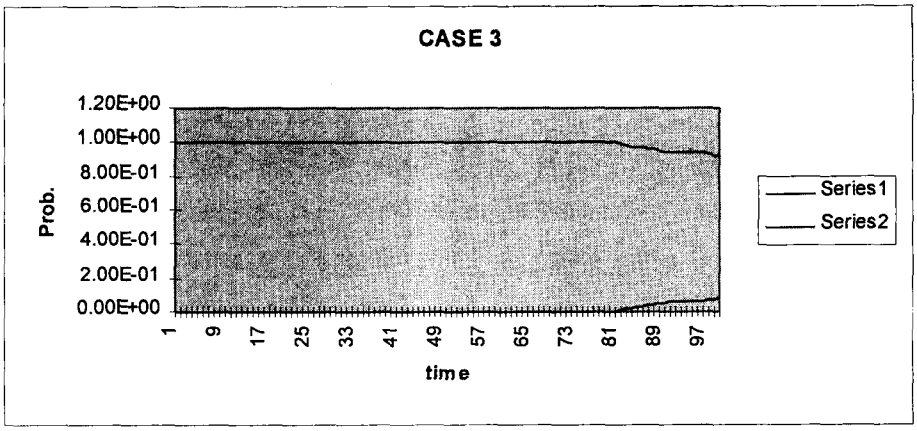


Fig. 4 TOP event probability of each case study

Here, Series 1: probability of fail TOP event

Series 2: probability of success TOP event