CHEMICAL ENGINEERING TRANSACTIONS, Volume 13, 2008
Edited by Simberto Senni Buratti
 ISBN 978-88-95608-07-5

Integrated Dynamic Decision Analysis: a method for PSA in dynamic process system

M. Demichela & N. Piccinini
Centro Studi su Sicurezza Affidabilità e Rischi, Dipartimento di Scienza dei Materiali e Ingegneria Chimica, Politecnico di Torino
Corso Duca degli Abruzzi, 24 10129 Torino, Italia

One of the important issues still under investigations in order to increase the confidence in the results obtained in the PSA of technological systems is the physical modelling of the process. Integrated Dynamic Decision Analysis provides a full representation of the plant states, as well as all the possible occurrences patterns, expressed in a set of mutually self-excluding sequences. Availability of the full set of alternatives allows the complete spectrum of possible probability-consequence conditions to be used as a basis for decisions in risk reduction. Furthermore it is possible to interface with the logic-probabilistic model a process simulator, in order to assess the status of each relevant process variable with reference to the failure sequence identified, allowing the mutual interactions of the hardware components and the physical evolution of the plant to be taken into account. This approach is here described through a simple case study taken from literature.

1. Introduction

In the present work, through the application to a simple exercise taken from literature, the capabilities of dealing with the risk assessment of dynamic system of IDDA (Integrated Dynamic Decision Analysis) methodology were investigated.
IDDA is based on an enhanced form of dynamic event tree. Starting from a description, reflecting the level of knowledge that the analyst has about the system, IDDA is able to develop all the sequences of events compatible with the description received, from the point of view both of the logical construction, as of the probabilistic coherence.
The system description has the form a binary chart, where the real logical and chronological sequence of the events is described; the direction of each branch is characterised by a probability of occurrence that can be modified by the boundary conditions, and in particular by the same development of the events themselves (probabilities conditioned by the events dynamic).
As a matter of fact, in a dynamic cause-consequence logic, in addition to the direct logical interactions characterising it, each event can influence the subsequent events, depending on deterministic cause-consequence relations or stochastic dependences.
At the end of the analysis, the full set of the possible alternatives in which the system could evolve is obtained. These alternatives represent a "partition" since they are mutually exclusive; they are all and the sole possible alternatives, this allowing the method to guarantee the completeness and the coherence of the analysis.
The above logical-probabilistic model can be interfaced with a phenomenological model of the system, in order to obtain, for each alternative sequence:

- Probability of occurrence;
- Trend of the significant physical variable;
- Consequences entity.

The analysis of the alternatives in terms of logical congruence and correspondence with the knowledge of the plant is made easier by their representation as concatenations of events, placed along a well-defined time-trajectory.
Once the model has been defined, all the information worked out by the software are made available to the analyst as results (Piccinini et al., 1996; Galvagni & Demichela, 2003).

2. The Case Study

The case study is taken from Marseguerra & Zio (1996). In particular, the system object of the study (Fig. 1) is a tank containing a liquid. Its level is controlled discontinuously by three independent units, made of three level transmitters, all measuring the level in the main tank, each activating respectively two feed systems (U1 and U2) and one extraction system (U3). The liquid supply takes place through two pumps, fed by different tanks, with a flow rate able to maintain a constant level variation of 0,6 m/h each pump. The extraction system is made of a on-off valve with a flow rate able to bring to a level reduction of 0,6 m/h. At time t=0, the system is in its nominal configuration, with the units U1 and U3 operating and the U2 component in stand-by. In this case, the net flow rate is zero and the level is constant, until the first stochastic modification of the component status occurs. The system components can assume 4 status, whose transitions follow to an exponential law:

1. operating (on)
2. stand-by (off)
3. stuck on
4. stuck off

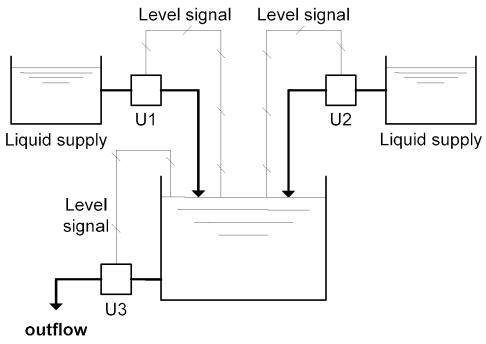

Figure 1. The tank object of the analysis.

The mean time between failures is respectively:

- U1: 219 h
- U2: 175 h
- U3: 320 h

The probability over time of main tank overfilling or dry out has been assessed over a mission time of 1000 h, in different conditions as described below.

3. Non Repairable Components

The first stage of the analysis is the construction of the logical-probabilistic model of the system, using the IDDA syntax.

Each line consists in a "question" that can have multiple possible answers, each one characterised by an expectation degree. Every question is a "level" in the IDDA syntax and a branch point in an event tree. Each branch is characterised by a probability of occurrence, its uncertainty degree and a series of addresses, that define the logical path depending on the answer to the analyst question. The alternatives are mutually exclusive. In the present case, the transition rates do not change if the component is operating and fails stuck-on, or if it is in stand-by and fails stuck-off, thus the process control system intervention, activating or de-activating the components, as a matter of fact have not any influence on the occurrence probability of a failure. At this stage no probabilities were introduced in the model, but only conventional values "0.5". This indicating that the real probabilities will be provided by an external file, that from failure rates and mission times calculates the probabilities for each branch. IDDA combines the answers to the analyst questions in all the possible ways, in order to obtain the "partition" made of all the possible alternative sequences of events, to which a probability of occurrence in associated. The sequences are of immediate reading and understanding. They show, step by step, the chosen paths, the associated probabilities and the modification on the logical status and on the probability of each event included in the sequence. The reading of the alternatives immediately reveals possible incongruence and omissions in the logical representation of the problem. In the present case, only a sequence can bring to the dry-out of the tank, as detailed in Table 1. The possible alternative sequences rise to 5 if the events bringing to overflow are considered: their single and cumulative probabilities are shown in Table 2.

Table 1. Dry out constituent.

CONSTITUENT Number :			1
10	U1	Fails	9.8960E-01
15	U1	S. Off	4.9480E-01
20	U2	Fails	4.9317E-01
25	U2	S. Off	2.4658E-01
40	U3	Fails	2.3575E-01
45	U3	S. On	1.1788E-01
94	Exit	Dry out	1.1788E-01
CONSTITUENT PROBABILITY:			1.1788E-01

Table 2. Overflow constituents

COSTIT. N.	PROBABILITY
1	2.466E-01
2	1.179E-01
3	1.179E-01
4	2.477E-03
5	7.802E-04

CUMULATE PROB.	4.856E-01

Figure 2 shows the results of the input model processing. At each time the probabilities of the four incompatible operating modes (overflow, dry out, no flow and normal operations) add up to 1.

The second case investigated through IDDA is the one in which the transition probability to the state 3 (stuck on) is increased of a factor 10 and the one to the state 4 (stuck off) increased of a factor 100: the logical-probabilistic model will undergo substantial modifications

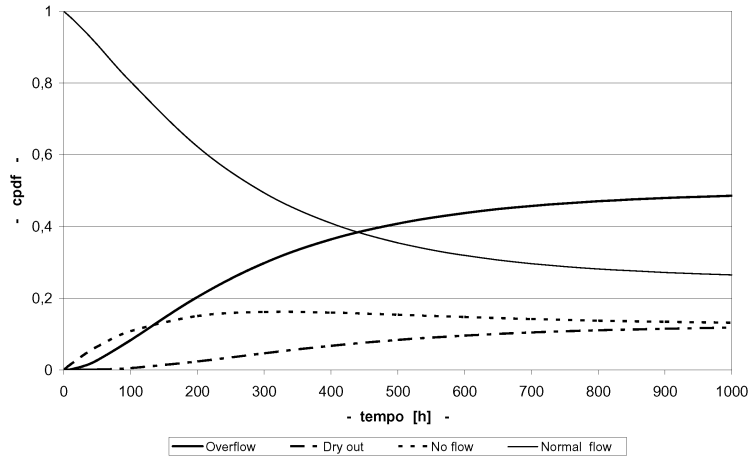

Figure 2. Non repairable components, transition rates invariable with the transition type.

In fact, while in the previous case, the event probability was independent on the occurrence order of the components failures, in the following one, the event probability will be strongly dependent on it. As an example, let's consider the first failure of the U1 component (the whole input model will keep into account also the case of a first failure of the U2 or U3 component) in the "stuck on" failure mode.
The subsequent level examines the presence of other failures: if no other failure is present, the model will directly send to a normal operating condition; otherwise it will be investigated what of the other components, U2 or U3, will fail first.
Let's consider a failure of U3 component: it could fail stuck on or stuck off. In the case of U3 stuck off, the consequence will be the overflow, independently from the behaviour of U2. With U3 stuck on, instead, the behaviour of U2 will be decisive: if U2 is stuck on, the result will be an overflow, if stuck off, the result will be a normal operating condition.
Similarly, let us consider the case of a failure of the U2 component after the U1 component has failed. If U2 is stuck on, the event will result in an overflow, independently from the behaviour of U3; if U2 is stuck off, the whole system performance will depend on the U3 component behaviour: even with U3 stuck on, there will be normal operating conditions, instead U3 stuck off will bring to an overflow. The input model thus includes all the possible evolution path of the system failures.
Furthermore, also the complexity of the factors to be included in the probability assessment will increase.

The solution of the differential equation system:

$$\begin{cases} \dfrac{dP_f}{dt} = -\lambda \cdot P_f \\ \dfrac{dP_g}{dt} = +\lambda \cdot P_f \end{cases}$$

Will bring to the following probabilities:

- *Absence of failures* $p_1 = \{1 - \exp[-\Sigma \cdot T]\}$ with $\sum=\lambda1+\lambda2+\lambda3$ sum of the transition rates of the single system components.
- *First failure of U1* $p_2 = \dfrac{\lambda_1}{\Sigma}$
- *Absence of U2 and U3 failures*

$$p_3 = \left\{ \left(\frac{1}{1-k_2} \right) \cdot \frac{[1 - \exp[-(\lambda''_2 + \lambda_3) \cdot T]]}{p_1} - \left(\frac{k_2}{1-k_2} \right) \right\}$$

where $k_2 = \dfrac{\lambda''_2 + \lambda_3}{\Sigma}$ and λ''_2 transition rate of U2 modified after a failure of U1 occurred.

- *Second failure of U2* $p_4 = \dfrac{\lambda''_2}{\lambda''_2 + \lambda_3}$
- *U3 operating or failed* $p_5 = \dfrac{P_{U1,U2,U3}}{p_1 \cdot p_2 \cdot p_3 \cdot p_4}$.

Hereafter the result obtained are reported: 6 sequences has been identified for the dry out, with a cumulate probability of 8.05E-02; 18 sequences bring to the overflow, with a total cumulate probability of 3.546E-01. Figure 3 shows the results as a diagram.

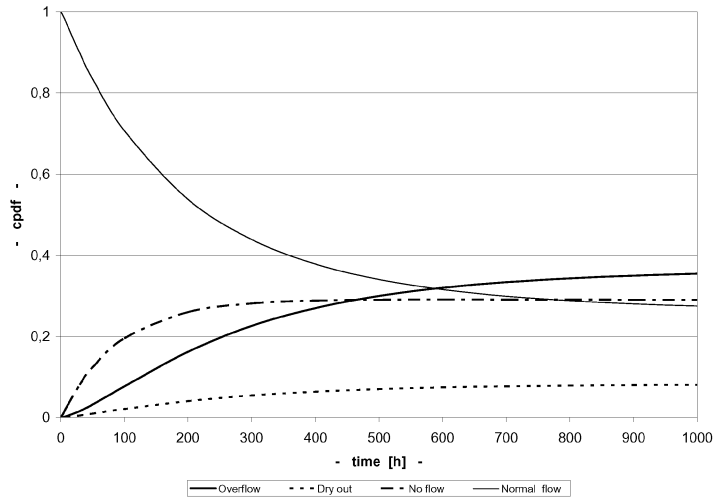

Figure 3: Non repairable components, transition rates variable with the transition type.

In Figure 4 a comparison between the results of the cases previously discussed is reported, with reference to the main events dry-out (a) and overflow (b). Thick lines represent the case of constant transition rate, while thin ones the case of increased transition rate for stuck on and stuck off conditions.

a

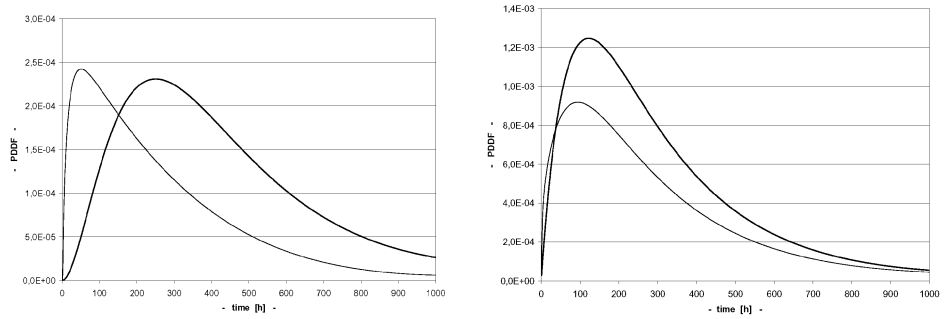

Figure 4. Comparison between the results of the cases discussed in the first sections.

b

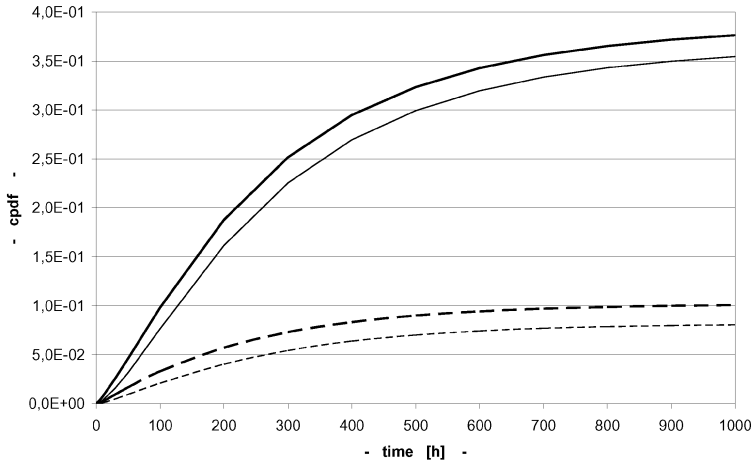

Figure 5 Comparison between the case of the failure on demand of the PCS and the previous cases analysed

Both the logical-probabilistic model and the calculation tool developed allow taking into consideration the possibility of a failure on demand of the process control system (PCS), with the hypothesis that this failure didn't influence the probability of the subsequent failures. In this case the unavailability on demand of the control system has been taken equivalent to 0.1.

In Figure 5 the results in the case of failure on demand (thick lines) are compared with the previously discussed cases of overflow (continuous lines) and dry out (dotted lines) for constant transition rates. Both the top events occurs in shorter times and with higher cumulative probabilities in the case of failure on demand of the PCS.