# Modelling the Safety Envelopes of Joint Operator-Process Systems

Y. M. Sebzali and X. Z. Wang*
Department of Chemical Engineering, The University of Leeds, Leeds LS2 9JT, UK

## Abstract

A methodology is presented for modelling the operational safety envelopes of joint operator-process systems and for involving human factors into the development of systems for identification and diagnosis of abnormal operations. The method is developed and tested in a joint operator-process simulation environment in which the process is modelled as a dynamic emulator while the operator part is developed as a real-time expert system to simulate the behaviour of operators in interpretation of signals, planning and execution of decisions. A dynamic signed digraph is used to describe the causal conditions that lead to a specific operational state.

## 1. Introduction

Operational safety is of paramount importance and is regarded as the first objective of process control. It is estimated that the cost attributable to preventable losses in the petrochemical industry only is more than billions of pounds per year. As a result, there has been a significant progress in recent years in developing computer based systems for process fault detection and diagnosis. The current work is motivated mainly by the following observations on previous studies on computer aided systems for fault identification and diagnosis. Firstly, most previous studies assumed that after a fault has occurred, the process would evolve without operators' intervention. For example, high fidelity dynamic simulators have been widely used in developing and testing various techniques and tools for fault detection and diagnosis. They only emulated the process behaviour without considering possible operators' intervention during the dynamic transition. Secondly, almost all the studies on automatic fault detection and diagnosis have focused on only part of the integrated system, i.e., the process part. Little effort has been made on automatic monitoring and assessing the operators' performance.

The lack of effort in integrating operators' factors into automated fault detection and diagnostic system is disproportionate to statistics. According to a worldwide survey carried out by a Honeywell led consortium (Nimmo, 1995), 40% of faults happened in chemical history is due to human errors. A parallel study on case histories by the Health and Safety Commission (Larder and Fleming, 1996) of UK indicated that 80% of accidents have human factors involved. Efforts in addressing human errors in process safety have so far limited to hazard and operability studies in the process design stage, training of operational personnel and prediction of human reliability.

The overall objectives of the work were to develop a methodology to involve the human factors into the development of systems for automatic identification and diagnosis of abnormal operations, and to develop an approach to characterising the safety envelopes of joint operator-process systems.

## 2. The Joint Operator-Process Simulation System

To carry out the study, a platform is developed which is a join process-operator simulation environment. The process is a dynamic process simulator developed using Matlab, which emulates in high fidelity the dynamic behaviour of the process under the influence of various disturbances as well as operator's actions. The operator part is modelled using Visual Prolog as a real-time expert system which emulates operator's behaviour in interpretation of signals, planning and execution of the decisions. The interaction between the process simulator and the real time expert system is managed through an interaction module. The dedicated interaction model manages the synchronisation through dynamic data exchange (DDE), transformation of data formats, and also serves as an interface for

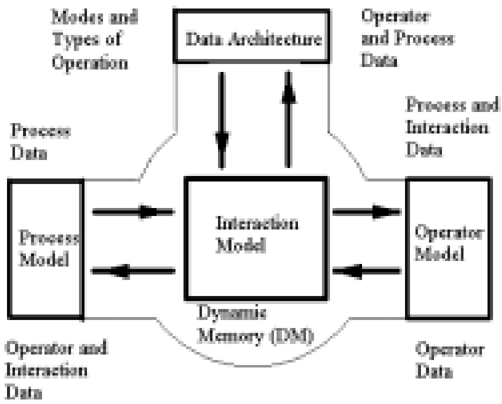


Figure 1 Architecture of the process-operator interaction system

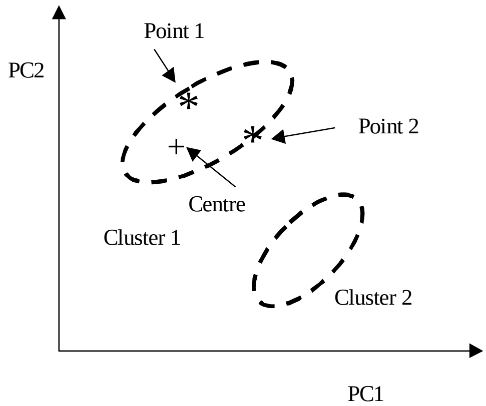


Figure 2 Points 1 and 2 have equal value of fuzzy membership

initiating variations, performing data analysis as well as displaying the operational envelopes. Figure 1 shows the structure of the system.

## 3. A Method for Modelling Operational Safety Envelopes

The method involves the following steps: categorical characterisation of dynamic trends, modelling of the operational envelopes and signed digraph based causal explanation.

### 3.1 Categorical characterisation of dynamic trends

Li and Wang (2000) developed a method for categorical characterisation of dynamic trends using both principal component analysis (PCA) and fuzzy *c*-means. The method uses PCA to project the dynamical trajectories of a variable in a windowed time scale to two or three dimensions and then clusters the trends to qualitative values in the PCA clusters. One observation on the method is that it is not sufficiently accurate, because if the fuzzy membership values of the points in the same cluster are equal to each other, they are treated the same. For example, points 1 and 2 in Figure 2 are in the same cluster and have the same fuzzy membership values, but clearly they should be given different values, but in the method of Li and Wang (2001) they treated them as having the same value. In this work, an improved method is developed in which each cluster is further divided into sections. The PC1-PC2 plot in Figure 3 is divided into four clusters, and each cluster is divided into sections. A specific location in the plot, representing a dynamic trend, can be described by a pair of qualitative values, i.e., C_out (1, 3) refers to that a dynamic trend of C_out belongs to the cluster 1 and section 3.

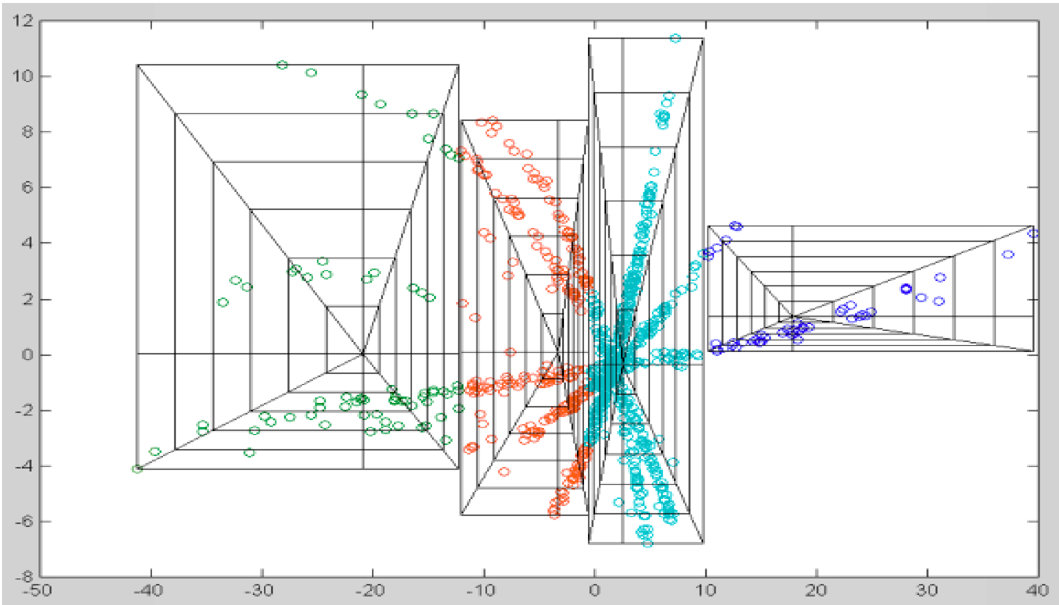

Figure 3 Categorical characterisation of the dynamic trends of a variable.

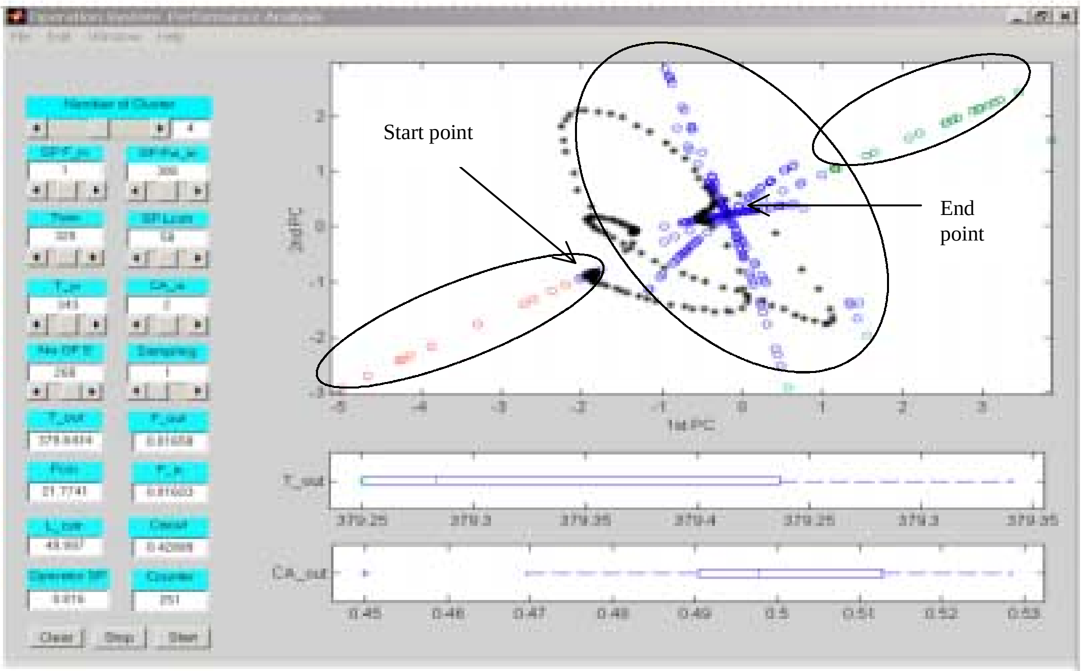


Figure 4  The operational envelopes and real-time display of the operational trajectories.

The number of clusters and sections can be determined using either a local or global method. In the local method, the number of clusters and sections are determined purely based on the variable itself. In the global method, it depends on the accuracy in predicting the output, i.e., the operational state space of the process. In developing the method, the data can be divided into training and test sets. Increasing the number of clusters and sections will often increase the accuracy for training data, but further increasing the numbers of clusters and sections can deteriorate the performance over the test data.

### 3.2 Envelopes of operational safety

We use the method of multi-level PCA developed by Yuan and Wang (2001) to plot the envelopes of the process (although other clustering approaches could also be used). The method has two steps. In the first step, the dynamic trends of each variable are processed using PCA, as described in section 3.1. Then in the second step, the first few (e.g. one, two or three) PCs of all variables are further processed to develop the two (or three) dimensional space of operation. Fuzzy *c*-means clustering can also be used in the second step to automatically find the cluster centres of operational regions and assign points to different clusters. Figure 4 shows the operational envelopes of a CSTR reactor which are obtained using the multi-level PCA approach to process a collection of simulation data. The operational point of the process can be projected onto the operational space in real-time. In Figure 3, an example trajectory of operation by an operator is shown (the dark asterisks).

### 3.3 A signed digraph describing the causal relationship between the variables' trajectories and operational envelopes

The structure of the digraph describing the causal relationship between the variables' trajectories and operational envelopes has no difference from previous digraphs used by other researchers. However, the trajectories of individual variables in a windowed time scale are transformed to qualitative descriptions using the method introduced in Section 3.1. The digraph uses rules to describe the conditions leading to a specific location of the operational point in the operational envelopes. An example rule is shown below:

```
IF      T_out (cluster =1, section = 3)      //T_out is the reaction temperature
AND     Ca_out (cluster = 2, section = 5)    // Ca_out is the concentration of
… …                                          // component A in the outlet stream
THEN  Process Operation (cluster = 3, section = 2)
```

## 4. Case Studies

In this section we present the result of a case run to demonstrate the use of the system for modelling the safety envelopes of a joint operator-process system. The case study is concerned with two operators (operators A and B) with varied experience operating a CSTR reactor. Suppose the CSTR is initially operated at steady state. As a result of the influences of three disturbances, i.e. the feed temperature, the feed composition and the cooling water temperature, at sampling points 9, 85 and 164, there are deviations from the set point of the reaction temperature of the magnitudes of 2 K, 3.6 K and 0.2 K respectively. After observing this deviations, the operator will consider taking actions and continuously monitoring the operation until he is satisfied. We demonstrate how the operational envelope method can be used to monitor the operational trajectories and assess the operation.

The following discussion will be based on Figures 5 and 6. Figure 5 shows the stress measures, intervention measures and the reaction temperature variation. In Figure 5, the stress measure reflects the stress of the operator which changes from -0.1 (no stress) to 0.1 (maximum stress). The intervention measure is an indication of how frequently the operator intervenes. It changes from -10 (no intervention) to 10 (most frequent intervention). In Figure 6, the dark asterisks indicate the starting and end points and the trajectories of the operational point.

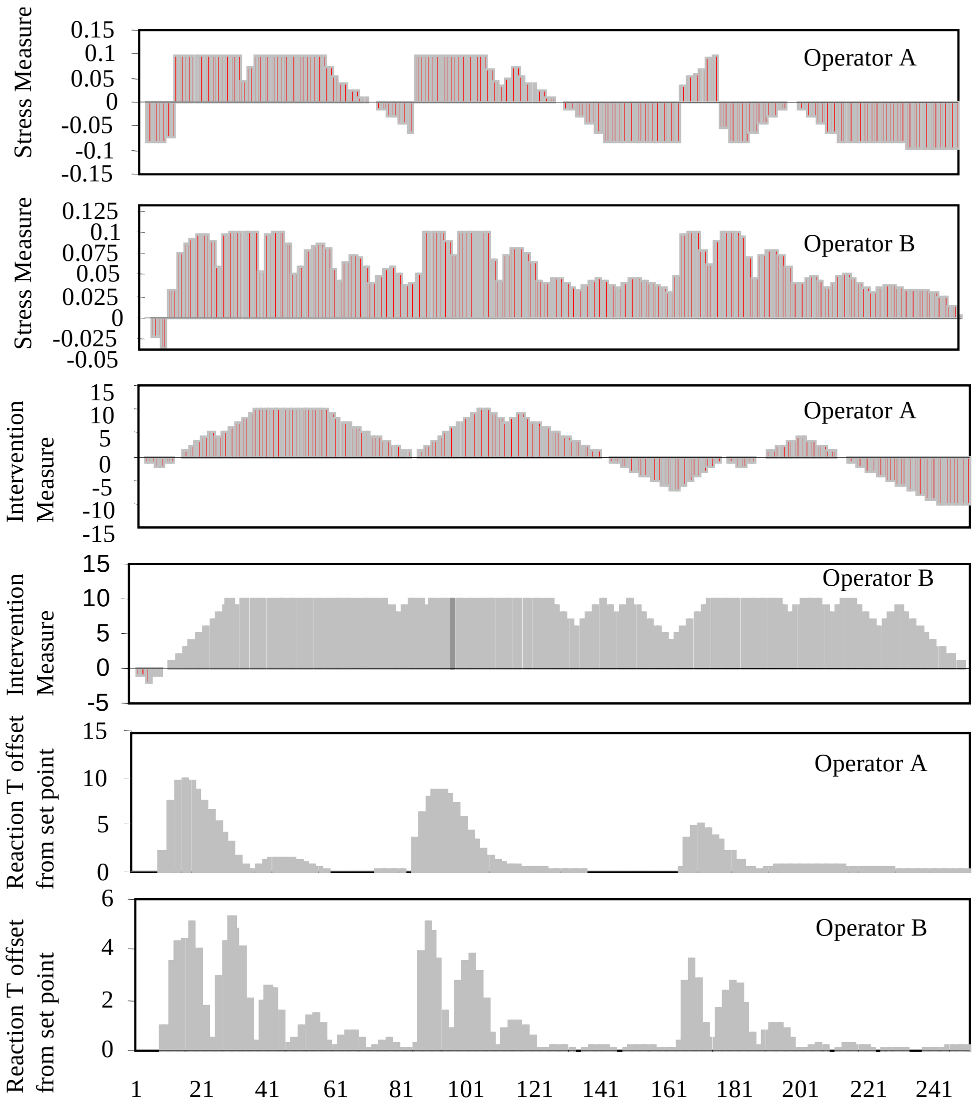


Figure 5 The stress and intervention measures for operators A and B and the temperature deviations.

### 4.1 Operator A

Upon detecting the deviation of 3 K in reaction temperature from the set point at sampling point 9, operator A developed a stress measure of 0.1 (maximum stress) and decided at sampling point 17 to intervene the operation every three seconds. He stopped intervention at the sampling point 57, but his stress was still at high level. When the temperature offset dropped dramatically, the intervention became every four seconds, until sampling point 75 when he stopped intervention completely, but still kept examining the process operation every 7 seconds. However, at sampling point 85, there was another sudden increase of 3.6 K in reaction temperature and the operator's stress immediately reached the maximum again. The operator managed to adjust the process to normal at sampling point 160. The third disturbance occurred at the sampling point 164 when the reaction temperature increased by 0.6 K. The operator did not react instantly due to the relatively small change and the stress measure did not reach maximum this time.

### 4.2 Operator B

Subject to the same three disturbances at the same times, operator B had different stress models and responded in a different way. He instantly noticed the first disturbance, but his stress measure didn't reach maximum immediately. His decision rules are that he would intervene the process every three seconds if the temperature deviation from the set point is greater than 1 K, and every four seconds if the deviation is smaller than 1 K.

Figure 6 shows the operational trajectories of the two operators. Operator A was able to maintain the operation within the normal region during the adjustment process while operator B made the operation outside the normal zone and ended at a point close to the boundary of the normal operational zone.

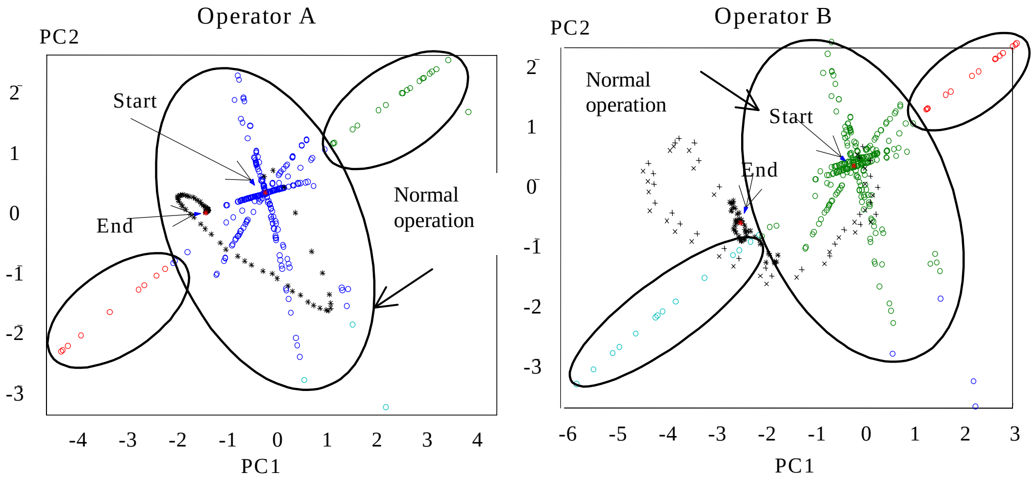


Figure 6 The operational trajectories of operators A and B.

## References


Lardner, R. and M. Fleming, 1999, The Chemical Engineer 7 Oct., 18.
Li, R.F. and X.Z. Wang, 2001, AIChE J. 47, 906.
Nimmo, I., 1995, Chem. Eng. Progr. 91(9), 36.
Yuan, B. and X.Z. Wang, 2001, Chem. Eng. Comm. 185, 201.