MODELING, IDENTIFICATION AND CONTROL, 1985, VOL. 6, NO. 3, 127–140
doi:10.4173/mic.1985.3.2

Simulation as a tool in operational safety, reliability and control

ARNE TYSSØ‡

Keywords: *Monte Carlo simulation, operator training, safety shutdown systems, modeling, computer-aided modeling, error detection, fault diagnosis, dynamic simulation.*

Dynamic simulation has long been considered indispensable for the understanding of process dynamics and for control system design. There has been a tremendous increase in the number of computer based simulation tools, and considerable improvements have been made in the development of complex plants with advanced automatic control.

When it comes to the question of operational safety and reliability, the traditional approaches have been fault-tree analysis and Monte Carlo simulation techniques. So far very little has been done to incorporate the safety and reliability problem with the automatic control system design and evaluation.

This paper discusses how various simulation techniques combined with interactive programming methods can be applied in the field of control system design and in the evaluation of operational safety and reliability. Typical applications will be: evaluation of control system performance, error detection and fault diagnosis, maintenance scheduling, process operator training, and analysing of reliability and safety.

Special emphasis will be given to the development of a computer based modeling/simulation tool that to a large extent will simplify the work involved in modeling and simulation of industrial processes. With this tool available it would be straightforward to evaluate different control strategies and protective system design and thus obtain better control system performance and reduction of spurious and hazardous shutdowns.

1. Introduction

Technological improvements in processes and in automatic control have made increasingly complex plants possible, and control schemes that were considered impractical a few years ago are now routine.

A typical trend is that risk reduction of plant shutdowns has now become the responsibility of the control system design. Control specifications such as minimum deviation in the control error and minimization of response time are now extended with specifications related to operational properties such as: fail safe operation, robustness with respect to equipment (sensors, actuators) malfunctions, and ease of start-up and tuning. This implies that control system design cannot be regarded as a separate task to be taken care of by the control engineer, but has to be considered as a part of an integrated design procedure where the process design, the design of start-up and shutdown system and control system design are strongly interrelated.

Received 15 June, 1985.

† This paper was presented at the International Seminar on Modern Methods in Dynamic Simulation of Industrial Processes, Trondheim, Norway, May 1985.

‡ CAMO A/S, PO Box 2893, 7001 Trondheim, Norway.

When discussing operational safety and reliability it is therefore natural to regard the plant as a process with instruments and equipment controlled by the protective system, the operator, and the control system. Figure 1 illustrates the interactions. When designing control systems it is necessary to apply dynamic analysis, and therefore dynamic simulation systems have been widely accepted as useful design tools. The safety and reliability questions are regarded in most cases, however, as steady state problems, and analysing techniques such as fault-tree analysis and logical graph technique methods combined with Monte-Carlo simulation are often applied. A protective system acts as a feedback element and is activated by a plant malfunction or an abnormal disturbance forcing the process to shut down to ensure safety. It is obvious that the safety and reliability problem is closely connected to the dynamic properties of the plant because a protective system may operate quite differently under transient conditions than under steady state. By disregarding the dynamics, important information will be lost, and in the worst case this may lead to wrong conclusions about the safety and reliability aspects of the plant. This is of course of great importance because even short start-up delays or short production shutdowns represent considerable losses of revenue and may also lead to hazardous plant situations.

The number of interactive program packages for simulation and control system design is steadily increasing, but so far these tools have only to a slight extent been used in industry. The main reason for this is that it takes a lot of time and expertise to develop the mathematical models that describe the plant in an adequate way. Thus it has been very difficult to motivate engineering companies, control system vendors, or the industry's own control engineers to apply new control strategies and alternative instrumentation system design.

What the industry seems to need is a modeling/simulation tool that makes it easy to generate process models and that can be used to simulate control system performance as well as analysing of reliability and safety.

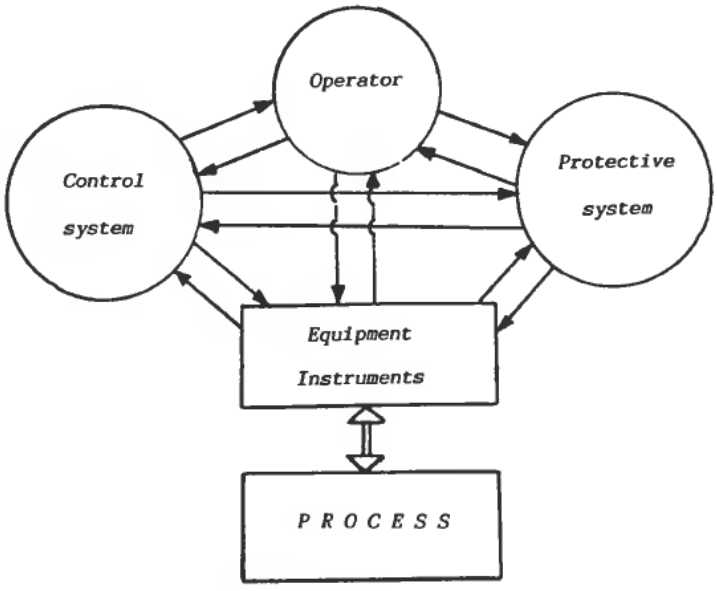


Figure 1

2. Control system design

One of the main motivations to apply dynamic simulation is the possibility to evaluate new control strategies before installation in the real plant. This is in particular true when it comes to highly complex processes that operate under continuously changing load conditions and where it is important to minimize feedstock and energy costs. Many process control systems have to be evaluated under conditions that are neither desirable nor possible to produce in the real plant, either from the point of view of safety or of economy. In such situations a simulation system is essential.

During the last decade several new control schemes based on modern control theory have been suggested, but control strategies more advanced than PID-algorithms have failed to gain wide acceptance in the process industry. There is no doubt that advanced control offers potential benefits, but costs are higher than traditional algorithms because the design process and the tuning procedure are more difficult. To overcome the first limitation, computer-aided design software is necessary to simplify the work. Standard software packages that support configurations other than traditional single loop structures are needed, for instance:

Multi-variable control based on either 'the theory of optimal control' or 'the theory of modal/pole placement control'

Adaptive control.

Perhaps more significant, though, is the need for satisfactory process models and simulation tools.

Simulation is important when designing control systems, for instance, to check the relationship between the choice of weighting coefficients in the optimal performance functional and the time-domain behaviour. But simulation is essential when it comes to evaluation of control performance before installation in the real plant. For instance, to evaluate the robustness of the control system with respect to modeling errors and any reasonable disturbance situation. The role of the human operator is also important because ease of start up and tuning are specifications that are not considered typical control requirements. The operator expects to be able to place arbitrarily selected combinations of loops under manual and automatic control, and the transfer of control mode must take place in a 'bumpless' manner. In a process with strong interactions being controlled by a multivariable algorithm, it could be very difficult to handle transfer operations. An automatic control mode transfer strategy is the only solution, and simulation is essential when designing and evaluating such strategies.

Other properties that are important to test are the interaction between the control system and the protective system in order to guarantee fail safe operation, in particular during transient operating conditions. Many simulation packages are available that provide interactive simulation of continuous and discrete interconnected systems, and thus will be suitable for evaluation of control system behaviour, for example:

ASCL: Mitchell and Gauthier Associates, US
SIMNON: Lund University, Sweden
SIM: SINTEF, Dep. of Automatic Control/CAMO A/S, Trondheim
SPEEDUP: Imperial College, London, England
GEPURS: Combustion Engineering SIMCOM Inc, US

SPEEDUP has been integrated with IBM's ACS (Advanced Control System) via a special interface that provides an efficient simulation tool for operator training and control strategy design (Herman 1985). The control design strategy can take place using standard ACS facilities. Once the control strategy is developed the entire system (tags, programs etc) can be transferred to the real time process system.

The importance of having a simulation tool available in connection with multivariable control system design, is clearly illustrated in a paper by Tyssø and Bembo (1979). The process is a drum boiler producing steam for a ship turbine. The boiler is a typical multivariable process with strong interactions between the five input variables (air flow, oil flow, feedwater flow, attemporator steam flow and outlet steam flow which is a disturbance) and the three output variables (drum boiler pressure, outlet steam pressure and drum level). Figure 2 shows a simplified boiler system. The model is described by a nonlinear state space model of 9th order and the most characteristic response of the model is the 'shrink and swell' phenomenon of the drum water level (non-minimum phase response).

Experience from the ship in operation clearly indicated that the conventional control system delivered by the boiler manufacturer did not operate satisfactorily. The main troubles were caused by the interactions and the non-minimum phase response (a zero in the right complex plane), but also coloured noise in the drum level measurement due to the ship rolling and pitching caused problems. The multivariable control system design was based on optimal control theory and on a Kalman filter of 8th order as a state estimator. Through extensive simulation applying the nonlinear model as the process, it was made clear that the multivariable controller was superior to the conventional controller. The main advantages came from improved dynamic performance and insensitivity to measurement noise. The improved dynamic behaviour made it easier to handle critical manoeuvring situations and to reduce the number of boiler shutdowns.

The tuning and start-up procedures which generally are more complicated when applying multivariable control could, in this case, be solved beforehand by utilizing the simulation facility. The simulation study clearly indicated the necessity of including the dynamics and constraints of the control devices and of the measure-

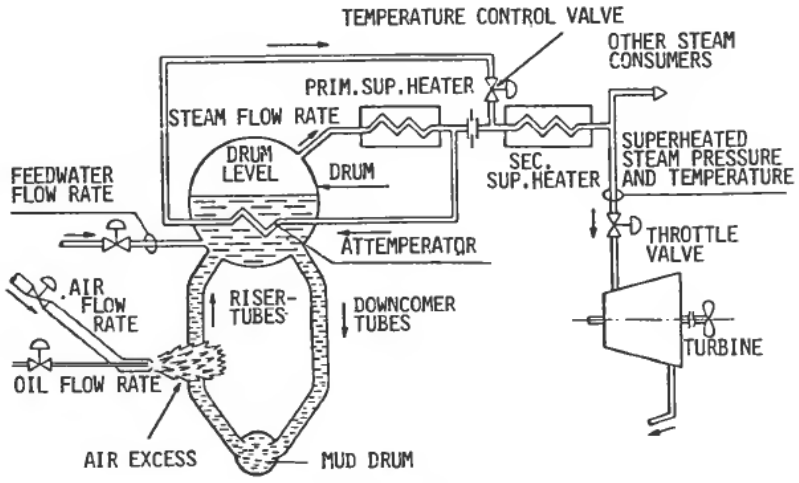


Figure 2. A simplified boiler system.

ment system when evaluating the control system behaviour. The process interface (D/A-, A/D-converters) had also to be included.

The expectations gained after the very promising simulation studies were fully met during installation on the ship. In Tyssø and Brembo (1979) several examples are given that show the performance of the multivariable controller, and of particular interest are the comparisons made between the conventional back-up system and the multivariable control system. Even though the conventional control system performance could have been improved by proper tuning by a specialist, there is no doubt that a multivariable control system would be preferred for that type of boiler system.

3. Utilizing simulation in error detection and fault diagnosis

Errors in the instrumentation system or process equipment may influence the plant behaviour in many different ways. Some errors react over a long period of time while others give a sudden reaction. The errors may lead to normal shut-downs or in the worst case to hazardous situations. A wrong installation of a safety valve or a plugged pipe will give an immediate response, whilst wear of components or leakages will gradually cause the plant performance to deteriorate until some components break down.

Error detection is taken care of by the alarm handling system, and it is of course of crucial importance that the alarm system is able to detect the errors before a hazardous situation occurs. The ideal situation would be, however, that the alarm system could be able to detect errors during development such that necessary repair or replacement could be performed at the right time, avoiding down time of the plant.

Error detection systems are generally based on state monitoring and trend analysis technique and have been utilized in industry for a long time. The simplest versions apply direct measurement and equipment performance calculations, while the more advanced error detection systems utilize process knowledge in the form of a mathematical model combined with measurements such as the input and the reference variables. Letting the model be simulated in parallel with the real process, it would be possible to compare and predict the development of the output variables. If the deviation between the model response and the process measurement was not within prescribed limits, it would be natural to state that an error had occurred in the process itself or in the instrumentation system. The quality of the model would then determine if the real cause for the deviation could be traced.

Applying estimation technique, for instance Kalman filtering, it would be possible to estimate states and also parameters in the process (such as heat transfer coefficients) that are not measurable. This could be utilized in the search for the error cause.

When an abnormal situation appears, the operator is warned by flashing or buzzing devices, each of which normally corresponds to one state variable alarm. If only one alarm occurs, there is no problem. The problem starts when several alarms start simultaneously and the operator has to identify the first cause of the system failure.

Fault diagnosis of a complex plant is not a straightforward task because of the close interactions between the process equipment, the protective system and the feedback-feedforward control system. The process itself influences all the different

components and the feedback loops make it possible that one component failure could actuate another, etc. Feedback loops are the only situation in which variables can come back on themselves, i.e. generate themselves in an inconsistent manner. The importance of automated diagnosis of system failures has increased remarkably as plants have grown in scale and complexity. Accidents such as the Three Mile Island accident and the Bhopal accident are examples that clearly indicate the necessity of improved fault diagnosis and error detection systems.

There are basically two different approaches to computer-based failure diagnosis, and Lee (1984) gives a review of the two methods and discusses several applications.

One is the experience-oriented method based on decision tables where the pattern met in practice is searched in the list of probable candidates. The other is based on a logic oriented method which uses the cause–effect relationship where all possible elementary cause–effect relationships are prepared, and an attempt is made to explain the observed failure pattern from a set of probable cause–effect relationships. The relationships are described by means of fault trees or signal flow graphs where nodes represent the variables involved, and directed branches represent qualitatively the functional dependency (' + ', ' − ' indicate promoting and suppressing influence, respectively). The level of influence can take only three values +, 0, and −. The models are thus very simple and the dynamic properties of the process and the control system are completely neglected.

In a system of realistic complexity the number of signal graphs may be very large and many faults may initiate the same alarm, even though the development over time will be different.

Using process models similar to the models applied for evaluation of control systems, one could simulate the development of all possible error candidates, compare this with the actual error propagation, and then effectively eliminate events that do not fit into the given pattern. Such a system would require an automatic updating and storage of all important variables over a prescribed time horizon.

Tsuge *et al.* (1982) apply very simple dynamic models (delays) in their directed graph diagnosis algorithms and demonstrate the advantages, compared with the traditional directed graph method, on a practical example (Three Mile Island). O'Shima (1984) discusses how dynamic simulation can be applied in a computer-aided diagnostic system, but he concludes that dynamic simulation is not practically feasible due to lack of appropriate models and an effective method for identifying the failure origin.

The modeling problem may be solved as indicated in § 6, assuming that every instrument and equipment has a necessary set of failure models. The identification of the error candidate is the key problem, however, and the only solution is to use some on-line estimation technique where dynamic models and logical failure models are combined.

4. Simulation of safety shutdown systems

With the recent emphasis on plant safety, safety shutdown systems are being installed more frequently on critical operation equipment. A safety shutdown system may be divided in two parts, the one which diagnoses the unsafe condition of process operation and, when necessary, generates the specific shutdown signals, and the other which executes the shutdown. A shutdown may often cause undesirable

transient conditions and therefore simulation may play an important role when designing safety shutdown systems for a plant. This is so because experiments on the plant sites are in general not feasible.

When simulating a shutdown system, it is of crucial importance to describe the transient conditions properly. In many chemical processes and energy systems, transients of a few seconds immediately after initiation of shutdowns are often critical. The process model must therefore also include the dynamics of the sensing elements, the actuators, the final control elements such as valves, and the control system.

Different control strategies may influence the shutdown system drastically. In some cases conventional single loop PID controllers may operate satisfactorily but when it turns out to be difficult to maintain the prescribed shutdown transient response, a more advanced control system such as a multi-variable control system must be considered. Otherwise, a new shutdown procedure must be designed.

The procedures for carrying out the simulation may vary depending on the process and on specific objectives of the safety shutdown system. However, some basic steps are considered to be common:

(*a*) Select the operating conditions which will yield the largest foreseeable span in the critical state variables.

(*b*) Specify control system and equations for the valve sizing and the actuator- and sensor-dynamics.

(*c*) Obtain transient responses from the simulation system and adjust the unknown control parameters to obtain the desired response.

(*d*) Simulate the process under abnormal disturbances and particularly check the reliability with respect to errors in control and sensing devices.

5. Simulation as a tool in decision support

Even though most processes are controlled automatically there are situations where the operator has to take over the control function. This is the case where there occur scheduled stops for maintenance or unscheduled stops caused by a process error or unbalance in the flow of material (tank overflow). If the process happens to have long time constants, internal recycling, large variations in the input variables or some degree of positive feedback, it may be very complicated to perform the manual control properly, and the operator could come in the situation that his/her manipulation forces the process to a shutdown of either spurious or hazardous character.

In order to be able to predict the influences of the manual control, one could run a simulation in parallel with the real plant. By applying different initial conditions one could check the consequences of alternative manipulations and end up with an acceptable solution. The simulation model must contain a complete description of the process material flows including the protective and alarm handling system.

There are also processes, particularly in the metallurgic industry, where the operator plays an active role in the feedback loop. That is so because it may be very difficult to obtain reliable measurements or design adequate models for control purposes, and the operator may have to adjust set points or feedback gains based on pure observations of the process behaviour. There may be large variations in the quality of feedstock and it may therefore be hard to perform the controller function properly. Thus it would be beneficial to utilize on-line simulation as a tool for

supervisory control. Such uses for dynamic models have been proposed over a long time, but only in recent years has there been enough computing power available to make practical use of the methods. The computer, through on-line simulation of the process, supplies the plant operator and control system with important process information (parameters, state variables) that is not available by direct measurement. The simulation could be run on a time scale exactly matching the process itself or faster, in order to be able to answer questions such as 'what if'. In Stuan (1981) and Onshus (1981) it is shown how these techniques, combined with advanced estimation methods (Kalman filtering), could be applied for control of a basic oxygen furnace and a sponge iron process.

6. Simulation as a tool for operator training

Even though the process and process control system may be well designed, the overall performance is strongly dependent upon well trained operating personnel.

Computer simulation has proved to be an efficient tool for plant operator training. In the course of one day the operator may have to handle more difficult operating conditions and emergency situations than during years of on site training. Their ability to diagnose potential equipment failure is a particularly important aspect of simulation training.

It must be emphasised that the simulation system must include a realistic model of the process and the complete instrumentation system with alarms and shutdown systems in order to simulate the actual plant behaviour to a sufficiently high degree of fidelity. Such a system will be so close to reality that the operator regards it as the 'real plant'. It is 'hands on' experience. It does not matter if the operator makes errors, unless the company wants to monitor the trainee's performance and check if he or she fails to achieve the required level of competence. A safe and reliable plant operation is dependent on the operator's confidence in his or her abilities to come up with the correct response when faced with a hazardous plant situation. A simulation-trained operator has more experience with such plant performances and will thus be more likely to make the correct manipulations.

To develop simulation models to be used in training systems considerable expertise is needed, and this is therefore taken care of by companies that specialize in the design of simulators. The simulators most often also include a replica of the real plant interface system. This makes it possible to simulate instrument and equipment failures but it also makes simulators expensive. It appears that this is the reason that has limited their use in the process industry. In most cases the simulators are included as part of major contracts only. It is reasonable to believe that a more efficient modeling tool and the availability of inexpensive but highly interactive microcomputer systems will make the use of training simulators more common in industry. A microcomputer based system, though not as powerful as the larger simulators, is more ideally suited for the simulation of individual plant units and for processes of moderate complexity.

7. Simulation in evaluating reliability

When analysing the total cash flow spent on instrumentation and control systems during the life of a plant, it often turns out that maintenance and repair costs far exceed the money spent on the original design. Reliability has become a

key factor in the design and operation of processes, and the final objective for the purchaser as well as the designer is to install a system with high availability. Competition in the market dictates that it is no longer economically feasible to introduce excessive redundancy and one has to balance the reliability and maintainability questions vs. the life cycle cost of the process plant equipment and instrumentation.

Maintenance is a primary function in an operating plant and properly planned maintenance strategies will serve to reduce failure rates and therefore influence total plant availability. The designer has to solve the reliability question and he/she needs a tool which makes it possible to estimate plant availability and to predict the effect of maintenance activities and policies on system availability.

There are several approaches to the calculation of reliability, for instance, by the application of probability theory and its combined properties (reliability flow graphs, fault trees, etc). But when the complexity of the system increases these methods become increasingly difficult to apply. Simulation based on Monte Carlo technique can be used to find the reliability of a complex system with relative ease but requires substantial computer resources. Both techniques are described in Lane (1985).

The usual approach in Monte Carlo simulation would be to generate random variables with known statistical distributions to describe particular properties (time-to-failure distribution) of the components which comprise the system. By allowing these properties to interact with a mathematical model describing the overall system, system reliability can be assessed. Through a Monte Carlo simulation it is possible to estimate length of satisfactory operation time of a system or to study alternative maintenance and repair policies.

The functional structure of the system to be studied can be represented by a so-called reliability flow graph or a fault tree, which in turn can be established directly from the piping and instrumentation diagram, (P & Id), Lapp and Powers (1977). Each component of the system under consideration is characterized by a specified probability distribution for the times-to-failure. To simulate the system operation, a failure time can be generated for each component from its corresponding time-to-failure distribution. Each of these failure times can then be converted to a Boolean state representation of success or failure. From the reliability flow graph is it thus very simple to identify whether the system is a success or failure. If all the components along a given path in the graph are a success, the system is successful. If at least one of the components is a failure, another path needs to be checked. This procedure is continued until either the system success has been identified or all the relevant paths (minimal tie sets) have been checked, with each path having at least one failed component. If this happens, the system is a failure.

Repeating this procedure will result in n_s successes and n_f failures of the system. Consider now that T is the required length of satisfactory operation time for a given system. The reliability estimate corresponding to T would then be

$$R(T) = \frac{n_s}{n_s + n_f}$$

This approach works very well when looking for the potential weakest point in a system, but the problem becomes more complicated when one wants to simulate the availability of control systems or processes from the point of view of maintenance,

repair and inspection. In addition to the failure distribution of each component one has to specify:

the repair distribution of each component

replacement policy (age)

start-up delays of each component

start-up failure risk

details of policy relating to resources, etc.

These problems are discussed further in the papers by Deans and Mann (1982) and Lane *et al.* (1985).

8. Description of tomorrow's modeling and simulation tool

Simulation has so far not had a real breakthrough in industry because it is time consuming, and considerable expertise is needed to develop adequate mathematical models of realistic processes. What is needed is a tool that actually solves the modeling and simulation problem in a straightforward manner. The outstanding properties of such a system can be characterized as follows:

A database containing models of standard unit operations (valves, vessels, heat exchangers, etc.); the user may choose the complexity according to his/her specific application.

Highly interactive operation; the user links the unit modules together using a mouse device or a touch sensitive screen.

A library of control algorithms, interlocks, and safety routines.

No program coding; the user may add models of specialized apparatus by applying a high level model generating language.

Flexible solution methods; modular and equation based algorithms.

The hardware configuration of the system is illustrated in Fig. 3. The use of graphical input-output devices offers great flexibility and user-friendly operation. One of the easiest ways to interact with a computer is through a touch activated display. A less expensive version could utilize mouse devices.

The design philosophy behind the proposed system, which was originally presented by Balchen *et al.* (1983), is based on the fact that most plants in the process industry (paper & pulp, chemical, oil, gas-refining, food industry) comprise standard unit operations, unit processes, which are relatively easy to model separately, but when put together make a system of high complexity. Typical unit operations or unit models are valves, flashes, pumps, vessels, heat exchangers, evaporators, driers, pipes, compressors, etc.

The unit models will be contained in a database and one could think of the database as a library of numerical models. There will be different versions of the library, each version dependent on the user's specific application. If the model is to be used for process design, one may need high precision models describing steady state properly. If the simulation has to do with evaluation of control system performance, it is necessary to use models that represent the dynamic properties adequately. In training simulators, rather simple models are used but both dynamic and steady state descriptions must be available.

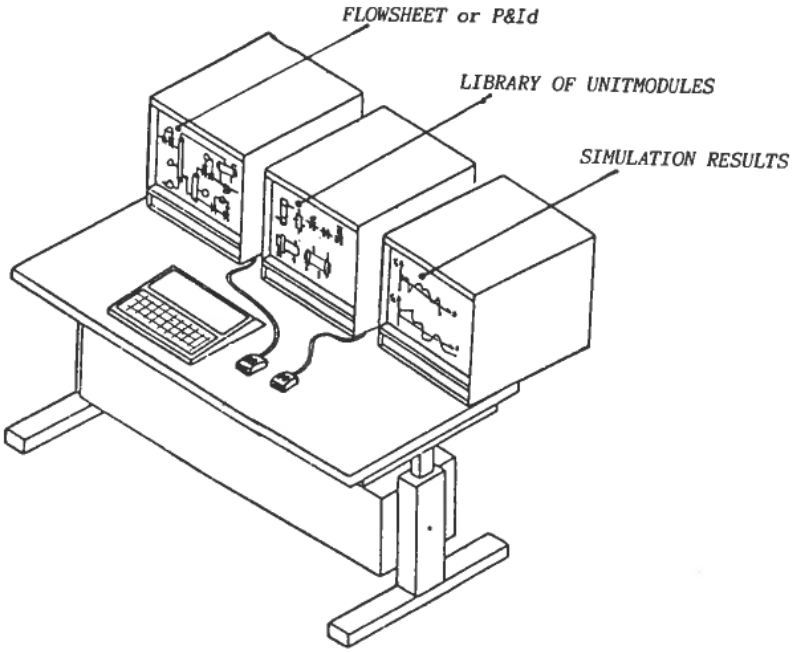


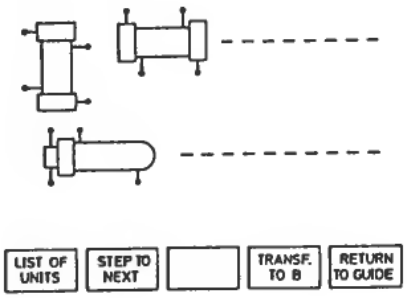
Figure 3. A workstation for modeling and simulation.

For each type of standard unit there are also several alternatives dependent upon physical shapes, capacities and types of substances involved. There may be more than ten different models of heat exchangers, depending on the way tubes and shells are arranged.

The user may add models of specialized apparatus of less general nature using traditional program coding or, in the more advanced case, use a high level, model-generating tool based on ideas from expert system considerations. Utilizing a sophisticated knowledge base, the user is guided through the complete modeling procedure and ends up with a model without writing a single code of program.

As discussed in the introductory section all the different tasks in a complete plant design, such as process design, control system design, start-up–shutdown system design, are closely interrelated and cannot be regarded as separate problems. It is well known that a process with a control and protective system reacts totally differently from a process without one. The protective system acts as a feedback element, and is activated by a plant malfunction or an abnormal disturbance, forcing the process to shut down to ensure safety. The protective system may react differently in a transient plant condition than in steady state because there exists dynamic interaction between the process variables and the logic variables of the protective system.

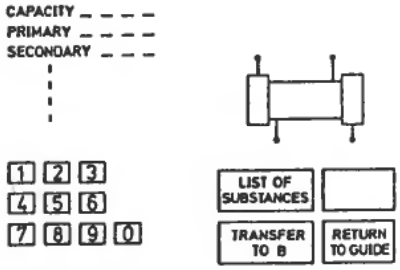
Corresponding arguments may be used when it comes to the process design problem. Traditional tools have been steady state simulation, but the processes today are characterized by highly complex plants where process equipment and apparatus are highly integrated with advanced control and protective systems. In such situations the designers require dynamic simulation. They need answers to 'how fast?', 'does the control system handle the transients properly during an emergency shut down?' etc.



SCREEN IN "UNIT" MODE

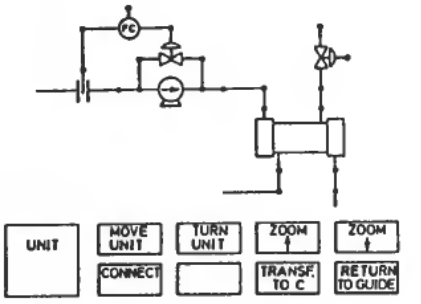
Figure 4

The user operates on the database through a menu of commands which allow him/her to link the different unit models together, interactively, using either a mouse device or a touch sensitive screen. The unit models are all identified by their corresponding graphic symbols and may appear on the screen as shown in Fig. 4 (this example shows heat exchangers). The user picks the particular unit model and then enters the thermodynamic and other physical coefficients. Figure 5 shows how the screen may appear in the data specification mode. When the necessary models have been selected, the user links them together according to the Piping and Instrumentation diagram (P & Id). The final simulation model may then appear as indicated in Fig. 6. Finally the test conditions are set, and the simulation can be performed.



SCREEN IN "DATA" MODE

Figure 5



SCREEN IN "CONNECT" MODE

Figure 6

The choice of solution method is dependent on the specific application, but both modular and equation based algorithms must be available, see for instance Brosilow (1985) and Mitchell and Gauthier (1981).

As indicated previously the final model complexity may vary from application to application, but the user in most case starts the modeling procedure from the topological information given in the process flow or Piping and Instrumentation diagrams (P & Id). These diagrams are today developed on graphic work stations and could therefore be the natural input for the modeling and simulation study.

9. Conclusions

The paper discusses how simulation combined with computer assisted methods can be utilized for different tasks in a plant design with emphasis on the control, safety and reliability problem.

Through simulation one achieves a better understanding of the process behaviour and the complex interactions between the process, the control and the instrumentation system, and thereby is able to design improved processes and control systems.

Software simulation tools have long been available but have not gained wide acceptance among industrial users before today. The main reason is that it is time consuming and requires considerable expertise to develop mathematical models of realistic processes. The industry needs a tool that solves the modeling/simulation problem in a straightforward manner, and specifications for this tool are very briefly outlined. When available the system will be essential among engineering companies, vendors of control systems and industries' control and process design departments. Simulation is the key to increasing productivity and safety in the process industry in the future.

References

Balchen, J. G., Fjeld, M. and Saelid, S. (1983). Significant problems and potential solutions in future process control. The annual AIChE-meeting in Washington D.C., 1983. Available from the symposium.

Brosilow, C. B. (1985). *Modular Integration.* Modeling, Identification and Control, **6,** 3, 153–179.

Deans, N. D. and Mann, D. P. (1982). *The development of a new hardware reliability simulator* (Robert Gordon's Institute of Technology, Aberdeen, U.K.).

Herman, D. J. (1985). *Integration of process design, simulation and control systems* (Department of Chemical Engineering, University of Waterloo, Canada).

Lane, G., Grundt, H. J. and Malloy, K. (1985). Miriam: Software for system effectiveness evaluations. Reliability 85, Birmingham, U.K. National Center of Systems Reliability , Warrington, U.K.

Lapp, A. S. and Powers, G. J. (1977). Computer-aided synthesis of fault-trees. *IEEE Transactions on Reliability*, **R-26,** 2–13.

Lee, F. P. (1984). Process computer alarm and disturbance analysis: Outline of methods for systematic synthesis of the fault propagation structure. *Computers and Chem. Engng.*, **8,** 91–103.1.

Mitchell and Gauthier, Assoc. (1981). ACSL: Advanced Continuous Simulation Language. Users Guide Reference Manual, Concord, Mass, U.S.

Onshus, T. (1981). Control of the Sponge Iron Process. Report STF48A81010. The Foundation of Scientific and Industrial Research at the Norwegian Institute of Technology, Automatic Control Division. Trondheim, Norway.

O'SHIMA, E. (1984). Process computer alarm and disturbance analyis: Outline of methods for systematic synthesis of the fault propagation structure. *Computers & Chem. Engng.* **8,** 91–103.

STUAN, V. (1981). Control of the L–D converter. Report STF48F81039. The Foundation of Scientific and Industrial Research at the Norwegian Institute of Technology, Automatic Control Division. Trondheim, Norway.

TSUGE, Y., SHIOZAKI, J., MATSUYAMA, H. and O'SHIMA, E. (1982). Fault diagnosis Algorithms based on the signed directed graph and its modifications. The International Symposium on Process Systems Engineering, Kyoto, Japan, August 23–27 1982. The Society of Chemical Engineers, Japan.

TYSSØ, A. and BREMBO, I. C. (1979). Installation and operation of a multivariable ship boiler control system. *Automatica* **14,** pp. 213–221.