nks

Nordisk kerne-sikkerheds-forskning | Nordisk kärn-säkerhets-forskning | Pohjoismainen ydin-turvallisuus-tutkimus | Nordic nuclear safety research

RAK2

NKS/RAK-2(95)TR-B1

THE CAMS PROTOTYPE

P. Fantoni, G. Meyer, P. Nurmilaukas, M. Sirola, A. Sørenssen

Institutt for Energiteknikk (IFE)
OECD Halden Reactor Project
Halden, Norway

March, 1995

The CAMS Prototype

by

Paolo Fantoni, Geir Meyer, Pekka Nurmilaukas, Miki Sirola, Aimar Sørenssen

March 1995

Abstract

CAMS (Computerized Accident Management Support) is a system that will provide support in normal states as well as in accident states. Support is offered in identification of the plant state, in assessment of the future development of the accident, and in planning of accident mitigation strategies. It does not give support in execution of the chosen mitigation strategy.

We imagine different types of users: operators and shift leaders, the staff in the technical support centre, and people in the national safety authorities. These different types of users need different types of support.

CAMS picks up information from the plant and transforms it into a more digestible form before presenting it to the users. The transformation process can be controlled by the user.

CAMS consists of a signal-validation module, a tracking simulator, a predictive simulator, a strategy generator and a critical function monitor. Much work has been put into the man-machine interface. The prototype does not yet contain all these features, the present version comprises the predictive parts of the system.

The purpose of the prototype is to test out the possibilities and also the difficulties of the chosen design. The present prototype has been made for a boiling-water reactor, but the possibility of making a version for pressurized-water reactors will be investigated.

1. INTRODUCTION

1.1 The Purpose of CAMS

In case of a severe accident, or an event which may develop into a severe accident, the plant personnel must perform various tasks before they can start to counteract the incident:

- identification of the plant state,
- assessment of the future development of the accident,
- planning accident mitigation strategies.

The CAMS system (CAMS = Computerized Accident Management Support) will provide support in all these tasks. However, it will not support execution of the chosen accident mitigation strategy, which is also an important task for a complete process control system, but is considered outside the frame of CAMS.

CAMS is an information system: it picks up information from the plant, and transforms it into a more digestible form before presenting it to the user. The transformation process can be controlled by the user. The information given by CAMS is also useful in a normal situation.

1.2 Project History

A cooperative project between the Nordic countries was started in 1990. The subject was reactor safety, abbreviated SIK. The subprogramme SIK-2 addressed severe accident phenomena, and subsubprogramme SIK-2.7 was on computerized accident management support. Coordination of Halden Project activities in this area and the first phase of the SIK-2.7 programme resulted in a feasibility study report, see ref. [11].

An important milestone in the further work was a workshop on computerized accident management support [20] which was held in Halden in November 1992.

An extension of the cooperative project into a prototype phase is being carried out, financed in part by the Halden joint programme and in part by Nordic money in a continuation of the SIK-2.7 programme and its successor RAK-2.2.

The CAMS work can be seen as an extension of the work on the critical function monitoring system SAS-II which was finished in 1993. Both SAS-II and CAMS are made using the Forsmark 2 BWR as a reference plant. It was decided to make all the functionality and all the pictures of SAS-II available to CAMS users. (This is not integrated into the present version.) While the rest of CAMS has the main emphasis on physical description of the plant, through pressures, temperatures, flows etc., SAS-II has its main emphasis on logical descriptions: "why will this pump not start?"-"Because you have forgotten to open the valve, and the pump is interlocked with the valve." The two types of information supplement each other.

The SAS-II has been described in detail earlier [9], so we shall say no more about it here.

1.3 What Sort of Information Do Different Users Need in Different Situations

We have asked a group of experts from Sweden and Finland to give their advice on what sort of information different users would need in different accident situations.

The original idea for CAMS was to make a system to assist in accident handling. We were advised *not* to do that. In an accident situation, the user would be reluctant to jump to a system with which he is not completely familiar, and he would probably not ask for assistance from the support system before he is far into the accident. CAMS should have something to offer also in a normal situation, and its accident-handling capabilities should come as a natural extension. The sort of information wanted from CAMS will depend upon the nature of the accident.

Another point is that different users need different sort of information. Operators have a tendency to think mainly in terms of the individual components of the plant, shift leaders think more in the terms of systems, the staff in the command centre think in terms of functions, and people at a national safety centre take an even more global view. These different viewpoints come from the different roles these groups of people have in case of an accident. Ideally, all these user groups should be able to get the type of support they need in any situation.

Most studies on information needs have been paper studies. We hope to collect some experimental data on this question by evaluation of the CAMS prototype.

1.4 Why Make a Prototype

The purpose of the prototype is to test out the possibilities and also the difficulties of the chosen design, and recommend design changes where appropriate. In order not to be too abstract, the CAMS prototype is being made not for "a typical plant", but for a specific example plant. The Forsmark 2 plant in Sweden, which is of the boiling-water type, is our example plant. We believe that ideas from the prototype may be adapted to other boiling-water reactors with a modest amount of modification. With somewhat more modification, the same principles may also be adapted to pressurized-water reactors. Some of the principles will also be relevant for other kinds of industrial plants, as many problems of an accident situation are similar regardless the type of plant.

The prototype will not be as complete as is required from an industrial system, and it will not have the program quality either. An industrial system would need much more resources than available for the CAMS project. The purpose is therefore not to develop an industrial system, but to find out how an industrial system should be designed. However, a number of tools have been used, like Picasso-3 for the man-machine interface, the simulator-building tool APROS for the predictive simulator, ORBIX for the data communication, and G2 for the strategy generator. This means that industrialization will go much faster than starting from scratch.

This report describes the present status of the prototype, as well as development plans for the future.

2. THE CAMS DESIGN

Figure 1 shows the main components of CAMS and the data flow between them. Not all of these components exist in the present prototype, we shall come back to that later.

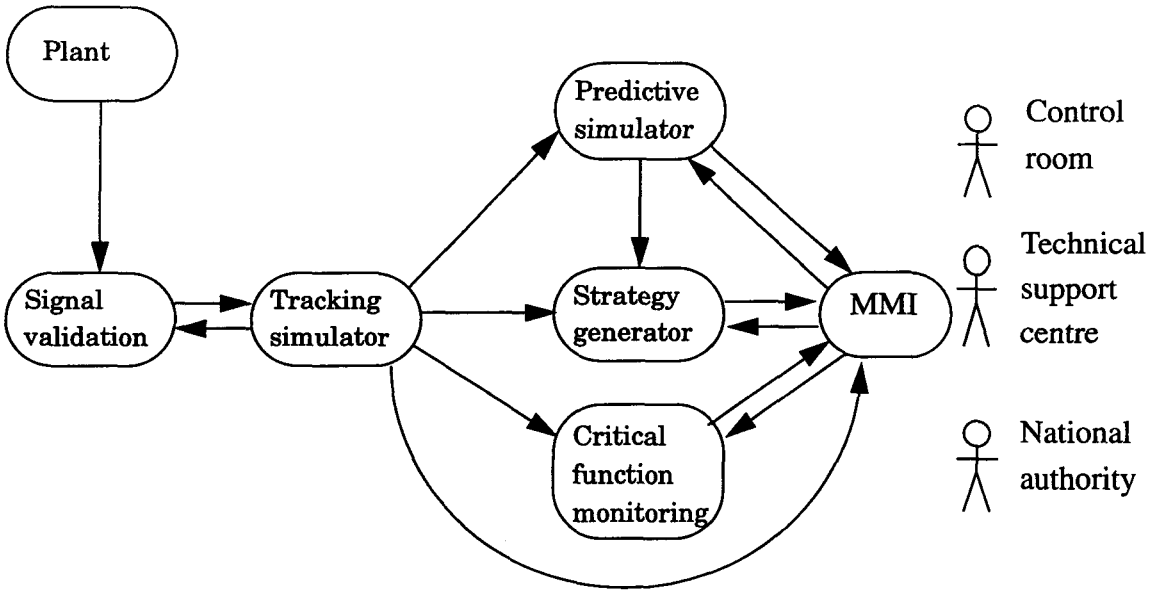


Figure 1 CAMS main components and data flow between them

Measurement data from the plant flow to the signal validation module. Here some of the signals have a tag with OK or NOT OK attached to them. We do not think it is realistic to validate all the data.

Validated data flows to the tracking simulator, which calculates physical quantities that are not measured, but which can be worked out from measurements, using mathematical models of plant processes based on first principles.

The man-machine interface can request data available from the tracking simulator, both measured and calculated. An example of the measured data is the pressure in the reactor tank. An example of calculated data that the user would like to know, is the temperature in the middle of a fuel element.

The user can tell the predictive simulator that he has a tentative plan, and instruct the predictive simulator to find out what will happen if he carries out that plan. The predictive simulator will then request data from the tracking simulator, to have a description of the present state as a basis for the predictive calculations.

The user may ask the strategy generator to propose a strategy that will bring the plant to a safe state. To do this, the strategy generator also has access to all the data describing the present state. The user may ask the predictive simulator to work out the consequences of a proposed strategy, and the strategy generator will pick up the future state and attach a quality number to the strat-

egy. The predictive simulator has a more precise description of the plant than has the strategy generator, therefore the strategy generator will rely upon the predictive simulator to do the calculation.

The CAMS user has also access to the critical function monitoring system SAS-II and all the pictures and functionality of that system.

We imagine three types of users. The operators in the control room, the engineers in the technical support centre, and people in the national authorities (in Sweden that is *Statens kärnkraftinspektion* and *Statens strålskyddsinstitutt* in Stockholm).

CAMS has been designed by first asking questions about what sort of information different users will need in different situations, and how this information should be presented to be as understandable as possible. Then questions have been asked how this information should be calculated, and finally what sort of raw data from the plant these calculations should be based on. That is, we have followed the flow of information through the system, but in opposite direction.

You could say that the purpose of CAMS is to provide the user with a tool which enables him to see what happens inside the plant.

Figure 3 (in the Appendix) shows how CAMS relates to other operator support systems.

3. THE COMPONENTS OF THE CAMS PROTOTYPE

3.1 The "Plant"

A future industrialized CAMS will receive its data from a plant. During development and test-out of the prototype, a computer program will play the role of the plant.

At the present time, a copy of the predictive simulator for Forsmark 2 is our "plant". The model is the same, but it works with different data. This makes life *too* easy, because, as a consequence of this, the predictive simulator will be able to predict exactly what is going to happen. In real life, the properties of the plant are not completely known.

In the future, to come closer to a real situation, a compact training simulator for Forsmark 2, written by EuroSim, will be our "plant". We do not have access to the source code of the EuroSim simulator, and we do therefore not know its exact properties. The predictions will then not be exact any more, and this is a more realistic situation. Before it can be used for our purpose, the EuroSim simulator must have its panel controls replaced by software equivalents. Work on this replacement has been started, but this has turned out not to be a trivial job, and the job is not yet completed.

3.2 The Signal Validation

An operator support system cannot give reliable and useful informations if the signals it takes from the process are not validated. Past operating experience shows that instrument malfunctions may cause the staff to misunderstand the plant status. Such misunderstandings constitute an important starting point of accident scenarios.

Signal validation means to pinpoint faulty instruments, and also to find the best estimate of a measured quantity in the presence or absence of instrument faults. Signal validation is always based on some a priori knowledge of the plant. This a priori plant knowledge may be in any form, equations, rules, or other ways of description.

A widely used technique to avoid human errors induced by instrumentation malfunctions is redundancy: four independent channels for critical process variables are quite common in nuclear power plants, but the reactor operators could be confused in a possible scenario where two out of four instrument readings give wrong values.

The CAMS system also can give misleading informations when fed with wrong process variables status: future development of the transient and mitigating strategies are strongly correlated to the plant current status and components availability.

Redundant instruments are always needed for those signals that trigger the safety systems activation. Examples are reactor water level (high and low level scram, activation of emergency cooling systems), high neutron flux scram, core pressure (high core pressure scram and recirculation pumps trip), and others.

An alternative approach for signal validation is to calculate process variables through independent methods and compare the calculated value with the measured one. Work has been done at the Halden Reactor Project on signal validation [1], [2], [3] and early fault detection [4] through parameter estimation using physical models. Current research [5] on the application of neural network models for signal validation shows promising results. Figure 2 illustrates how an auto-associative neu-

ral network used for signal validation very closely estimates the true value of the feedwater flow signal. 8% random noise was superimposed to make the test more realistic.

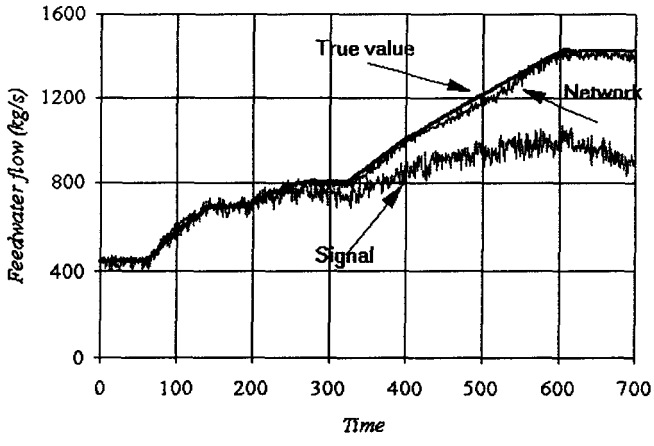


Figure 2 A neural network can estimate the true value and thus find an instrument error.

We think the most promising method is to use a neural network to find an erroneous signal, and then carry on from there with equation-based methods. The necessary calculations will be carried out by a specialized CAMS module, the tracking simulator.

A signal validation module has not been implemented yet in the CAMS prototype at the present date. Nevertheless, the work referenced means that we do not have to start from scratch.

3.3 The Tracking Simulator

The tracking simulator contains a priori knowledge of the plant, in the form of equations. The information calculated by the tracking simulator is used for three different purposes:

- The tracking simulator can calculate a quantity that the user would like to know, but which is not measured. An example is the temperature in the middle of a fuel element.
- A measured quantity can be calculated from independent measurements. The calculated value is sent back to the signal-validation module, which can compare the two. For example, the flow out of a heat exchanger can be calculated from mass and energy balances, and this flow is also measured.
- The tracking simulator can compute starting values for the predictive simulator, which we shall discuss in a moment. For example, when the predictive simulator will need initial values of temperatures inside the fuel elements for its neutronics calculation, the tracking simulator will calculate these.

As mentioned there is some experience in Halden in using mathematical equations describing plant components for signal validation [1], [2], [3] and early fault detection [4]. But these have been systems with limited scope. Some studies have been made [6], [7] to find if APROS can be used to establish the necessary equations, in order to derive a tracking simulator from a predictive simulator in a systematic way. The problem is not solved, but we have a platform to start from, which may lead to a method for signal validation on a larger scale, but we do not envisage to validate *all* signals.

No tracking simulator module exists in the present prototype, but again, we do not have to start from scratch.

3.4 The Predictive Simulator

Given the present state of the plant and given an operation strategy, the predictive simulator is able to calculate what will happen in the future. Thereby the user can test the consequences of a strategy, before carrying it out. To be of any value, the predictions must be several times faster than the real world.

Say the user wants to know what will happen if he does nothing. The predictor will then run at the accelerated speed while the plant follows after it at a lower speed, doing approximately what was predicted. If something drastic happens to the plant while the prediction is going on, say there is an operator intervention or a fault occurs, which may falsify the prediction, a signal will be given to the user so that he may decide to start a new prediction from the new plant state.

Say the plan is to open a valve. While the prediction takes place, the valve of the predictive simulator is open while the valve of the plant remains at its old position. Only if the plan turns out to be a good one, the operator will open the valve of the plant.

The current predictive model comprises the reactor including the downcomer divided into five subvolumes, the lower plenum divided into three subvolumes, the core divided into ten axial subvolumes and the upper plenum divided into four subvolumes. All the eight internal recirculation pumps are modelled, too. For the core a one-dimensional neutronics calculation is used.

The model includes the high pressure and low pressure emergency injection systems and the boron system. The containment is described with three subvolumes and it has also the necessary spray and condensation pool cooling systems.

Both parallel turbine plants are modelled in a simplified scale including the high and low pressure turbines, the steam reheaters, the condensers and the condensate and feed water systems with pumps and preheaters.

The thermal hydraulics calculation handles steam and water separately in the reactor and a mixture of steam and water elsewhere in the model.

The electrical system including the generators, transformers and on-site network is modelled. Some process components, e. g. the recirculation and feed water pumps are connected to the electrical system so that the simulation of a black-out is possible.

The automation system includes the most important controllers, like the reactor pressure and water level controllers as well as the most important protection systems, like the scram logic.

In general, the degree of detail is higher at those parts of the plant that are important in an accident situation. The scale of the model is a compromise between the speed and accuracy of the calculation.

The predictive simulator has been made with the simulator building tool APROS [10].

The model is built in a hierarchical way. At the top level, the plant is composed of the reactor, the high pressure turbines, the low pressure turbines, the condensers, etc., a manageable number of components. On the next level, you can open up say the high pressure turbine and find that it is composed of several turbine sections with steam extractions between the sections. Turbine sec-

tions are supplied with APROS as ready-mades, you only have to give the relevant parameters. Below this level, the turbine section creates automatically the calculation level structure, where all the state variables are calculated and then updated upwards. The user rarely has to care about the calculation level.

In the present version of the prototype, running on a HP 735 workstation, the speed is about 5 times higher than real time, without optimization. This can be speeded up by improved modelling, by improved coding, or by using a faster computer.

3.5 The Strategy Generator

The strategy generator [8] is rule-based and has been written in the real-time expert system shell G2. It is based on the idea of safety objective trees [16], a little simplified. Following different branches of the tree, each accident case is specified in more and more detail. On the highest level the safety objective is defined. One level down the objective is divided into several safety functions. Each safety function can be threatened by several challenges, and each challenge is connected to several mechanisms. The strategy planning will give different proposals, depending on for instance reaching some limits of physical quantities and the availability of different componens.

The strategy generator will attach a severity to each problem and to the corresponding advice. If there are several problems at the same time, this helps the user to concentrate on the most serious problem first.

The strategy generator gives its advice in qualitative form, for instance: "Open valve 314 a little". The user must translate this hint into a more precise form, and decide to increase the position of the relevant valve by say 10%. He may either directly put the strategy into action at the plant, but he may prefer to test out the consequences of the proposed strategy using the predictive simulator.

The consequences calculated by the predictive simulator are sent back to the strategy generator, and the strategy generator will calculate a quality number, taking into account the distance from the desired safe state. This quality number then describes the quality of the proposed strategy (open the valve) and the user's translation of the strategy into a precise form (open by 10%).In the present version of the protoype, this feature is present inside the strategy generator, but the result is not shown in the man-machine interface.

It has not yet been possible to test the validity of the advice produced for a large number of scenarios.

3.6 The SAS-II Critical Function Monitoring System

As mentioned in Section 2 on the CAMS design, the SAS-II shall be integrated into the CAMS system, as the logical information from SAS-II and the physical information from the rest of CAMS complement each other. This coupling between SAS-II and the rest of CAMS does not yet exist.

3.7 The Man-Machine Interface

Simplicity is always a key point when designing the picture hierarchy of a man-machine interface, but we think that simplicity is never more important than in an accident situation. It is always easy to lose the track, especially if you are running through a set of pictures that you do not use every day. If you are stressed, you will strongly dislike to run through complicated picture hierarchies.

The man-machine interface of CAMS consists of a relatively small number of basic pictures, but these pictures often have small windows that are put on top of them. The fact that the main pictures are so few means that you may access any main picture by one single click at the mouse. Everything is at your fingertips.

A number of the pictures are there to provide information on the present state of the plant. Figure 4 (in the Appendix) shows the **CAMS overview picture**, one of these pictures describing plant state. You can see if a pump is running or not, and you can see if the pump is available or not. That is, you can see if a stopped pump can be started, or if a running pump can be stopped. The corresponding information is given for many valves too.

Below the **CAMS overview picture** (and all other pictures) on the screen you have the **Picture selector**, shown in Figure 5.

There are also pictures that show where the energy is and how it is flowing, and where the water is and how it is flowing. The **Energy motorway** in Figure 6 is an example.

A general principle has been followed: we show what we think is useful in order to understand what is going on in the plant, independent of whether this piece of information is a measured quantity or something that has to be derived from several measurements. Availability is not measured, energy is not either, but we believe that users think in such terms. The man-machine interface has been designed according to how people think, not according to which physical quantities can be measured by one single instrument.

Prediction plays an important role in CAMS. The same pictures that give a snapshot of the present state of the plant, are also suitable to give a snapshot of a future state, or a past state.

In addition there are pictures that do not give snapshots, but trends of important quantities with time. Particular to CAMS is that these trends do not only cover the past and the present, but also the future. We call these Janus diagrams (named after the Roman god who had two faces, one looking forward and one looking backward). There is an important difference between the past and the future: you may have several possible futures depending on what plan you put into action, but you only have one past. The **Core trend diagram** in Figure 7 is an example of a trend diagram showing the future development as well as the past.

The man-machine interface also contains several pictures to operate the predictive simulator and the strategy generator. The **Strategies** picture in Figure 8 shows an example of output from the strategy generator.

4. DATA COMMUNICATION BETWEEN THE COMPONENTS

In the original design [11], the various software components of CAMS were arranged around a common database. This is not the case in the present design [12], [13].

The design now is more distributed and object oriented:

- Data is kept with the component that produces it and not transmitted until asked for.
- The components are made in a client/server style.
- There is no large common database that every component must use, data is distributed.
- The design is modularised to improve flexibility.

By doing it like this we get several advantages:

- It is easy to add a new component when needed.
- Data is distributed and this makes it easier to recover from system failures.
- There is no waste of bandwidth by transmitting data at all times, this reduces load on the network.
- The overall system design is easy to understand and therefore easy to maintain.
- Each component is isolated from the others and only known to the other components through its interface. A component can therefore not accidentally destroy or change some other component's data.
- Object-oriented methods makes it easy to implement new functionality.
- The components are very independent of each other.

Small-scale programs are built by defining procedures. As the size of programs increases, modules and classes allow larger components to be defined.

However, a very different approach normally has to be used when components of a system cannot be linked into a single address space - either because multiple nodes in a distributed system are used or because the executable programs of existing applications have to be integrated into the system. In CAMS we have several components made in different systems, the strategy generator in the G2 shell, the predictive simulator and the tracking simulator in APROS, the user interface in Picasso-3. The process module made by Eurosim we only have in binary form. These, quite different, components need to communicate and share information and resources.

Due to license agreements, and also due to the capacity of the computers, the different components in the prototype must run on different computers. This implies that the communication system must be able to cope with distributed processes.

The direct use of network sockets or protocols is a tedious approach and frequently one that is difficult to standardise across different platforms and different applications. Furthermore, it is very different from the familiar, simple, procedural approach.

By using Orbix[14], [15], software interfaces can be defined in a standard language, and these interfaces can be accessed from anywhere in a distributed system across different platforms. Orbix is a full implementation of the Common Object Request Broker Architecture (CORBA) which has been published by the Object Management Group (OMG) and is sponsored by many companies world-wide.

One of the problems at an earlier stage of the prototype was that exactly what kind of information and what functionality we needed were not clear. This meant that whatever solution we chose should be easy to modify and to develop further.

It seems that this distributed object-oriented design is very well suited for prototype purposes.

5. CAMS TESTING IN SEVERE ACCIDENT SCENARIOS

The CAMS prototype has presently been tested and demonstrated with only a small number of accident scenarios. Although a complete functionality test must consider a wider spectrum of possible events, the complexity of the selected scenarios is such that one can have a right feeling of the support to the end user and the efficiency of the whole system. The selected scenarios for the CAMS prototype are: LOCA (Loss Of Coolant Accident), ATWS (Anticipated Transient Without Scram), and PRFO (Pressure Regulator Fails Open). In this report, the ATWS will be discussed in more detail than the other two scenarios.

5.1 LOCA (Loss Of Coolant Accident)

5.1.1 LOCA frequencies

Loss Of Coolant Accidents are probably the most analyzed events both in PWR and BWR nuclear plants. The main reason for this is that the Large LOCA events are the Design Basis Accident for the emergency core cooling system requirements and design. In the 1990 PRA (NUREG-1150,Ref. [21]) LOCA is the third contributor to the internal core damage frequency, for USA BWR reactors, where the first two are the Station Blackout transient and ATWS events. For Swedish BWRs, LOCA is known to have a smaller contribition to the internal core damage frequency, due to the internal recirculation pumps design.

5.1.2 LOCA sequence in the CAMS scenario

In our scenario we postulate a break in the vessel bottom (a leakage in the control rods penetrations for example) that results in a leakage flow of 200 kg/s at 70 bar. In addition to that, a failure in the high reactor water level switch is assumed. The no-operator action sequence of events is as follows:

- LOCA initiation. 220 kg/s of water exits the vessel into the drywell.
- Reactor scram is triggered by high drywell pressure. All control rods are in. The reactor core is subcritical.
- The reactor is isolated.
- The leakage is not large enough to reduce the vessel pressure. So the core pressure is around 70 bar.
- The reactor water level start to decrease, due to the water loss through the leakage.
- A wrong high water level is sensed. The high water level protection is activated. The feedwater pumps are tripped. The Auxiliary feedwater system is inhibited.
- Since there is no water entering the vessel to compensate for the leakage, the reactor water level decreases sharply.
- After about 10 minutes the core is completely uncovered. The cladding temperature start to increase. The core pressure is about 70 bar.
- After 10 more minutes core damage starts.

In CAMS, the diagnosis and plant state identification module detects the LOCA event in few seconds, so that the operator is expected to operate the plant to achieve a safe shutdown.

Here, the expected action is to depressurize the reactor as soon as the Auxiliary feedwater system fails (no automatic ADS is considered available), in order to make possible the low pressure injection systems to start.

The CAMS predictive simulator can answer the following questions:

- How long can we delay the vessel depressurization (trying to fix the high water level sensor problem), without causing core damage ?
- After the depressurization, will the suppression pool and drywell cooling systems be able to maintain the pool temperature and the drywell pressure below the limits ?
- If the drywell pressure cannot be maintained, when will the pressure peak be reached and when will the operator be forced to ventilate the containment? (This event can be possible only if we postulate a partial failure in the pool cooling system, since this system is designed to sustain a large LOCA).

5.2 ATWS (Anticipated Transient Without Scram)

5.2.1 ATWS frequencies

ATWS is considered to have the highest frequency of occurrence of all severe accidents, together with the Station Blackout, in a USA boiling water reactor nuclear plant. In USA boiling water reactors, severe accidents that cannot be clustered in Station Blackouts or ATWS sequences give a very mild contribution to the overall core damage probability.

The probablity of an ATWS is smaller in Swedish plants. In addition to the main SCRAM system, which will insert the control rods by hydraulic actuators, Swedish reactors have an emergency SCRAM system that will insert the rods by electromechanical actuators. It is highly unlikely that both these systems should fail simultaneously, but we shall nevertheless assume that this happens.

ATWS behaviour, as most of the anticipated transient and accident events, is plant dependent. Though the general features of the transient and the required operator actions may be generalized, a detailed step-by-step sequence must consider a reference plant.

In this report the reference plant considered is the Swedish BWR reactor Forsmark 2, but the model is not identical to Forsmark 2, due to the lack of detailed data.

5.2.2 Description of ATWS Sequence

A transient that triggers the RPS system (Reactor Protection System) and results in an electric or mechanical failure of the scram system, is considered an ATWS event.

As the purpose of the RPS is to shut down the reactor, the safety functions threatened in this scenario are as follows:

ATWS ----> reactivity control ---> heat removal ----> heat sink ----> containment integrity.

The degree at which each safety function is involved and the possible core damage that can result is highly dependent by the actions that the operators are supposed to initiate and the time at which those actions are performed. In most cases alternative methods to shut down the reactor (after the scram failure) can terminate the transient at the first step of the safety chain, before substantial damage to the core has occurred. Additional failures and/or incorrect operator actions may result in different and worse scenarios.

5.2.3 Initiating Events

Any event that triggers the RPS may initiate an ATWS transient. Turbine trip, load rejection or MSIV closure (Main Steam Isolation Valves) are considered the most common initiating events of an ATWS. The main concern in evaluating initiating events is the main condenser and feedwater system availability. During a turbine trip or load rejection (there is no long term difference between these two transients, as long as electric failures are not assumed) with bypass, the main condenser is not lost and can be used as the main heat sink during the transient.

In some plants with 100% bypass capacity, a turbine trip with bypass does not even result in a RPS excitation, so that no ATWS is initiated.

MSIV isolation is the most general and bounding initiating event in this category.

A faulty signal in the steam tunnel radiation monitoring will be assumed for CAMS testing, that results in a spurious MSIV isolation.

The plant is supposed to be operating at 100% core power, 100% core flow. Fuel exposure is not relevant.

5.2.4 ATWS Without Operator Actions

A general description of an ATWS scenario follows, in the unlikely event that the operators take no action to mitigate the transient consequences. The following sequence of events considers the Swedish reference plant and is not directly valid for USA plants.

MSIVs close in about 3 seconds; when they reach the 90% open position the first scram signal is generated. We have assumed that both of the SCRAM systems fail. As the RPS is supposed to fail, the control rods remain in their withdrawn position and neutron flux and core pressure start to increase. Redundant scram signals on high neutron flux and pressure also fail, but the recirculation pumps trip on high pressure. The relief valves setpoint is reached, so the produced steam is flushed into the suppression pool, that starts to be slowly heated.

The thermal power should stabilize at about 20%-25% of rated power, with the core in natural circulation and pressure controlled by the relief valves (actually one or more relief valves should open and close cyclically because of the negative feedback between void and flux).

Feedwater flow still continues to pump water into the reactor, as long as the water level in the condenser is controlled. We assume that no external source of water is available, so that after about 8 minutes the feedwater pumps trip for low suction pressure.

With the reactor isolated and the produced steam flushing down into the suppression pool, the core level decreases until it reaches the low-low level setpoint.

At this point the high pressure cooling system is activated. In Forsmark, the Auxiliary Feedwater System (System 327) is composed of 4 independent motor-driven pumps and circuits, with suction from the CST (Condensate Storage Tank). The total capacity is 22.5×4 kg/s = 90 kg/s. Assuming that the stabilized core power will be 20% of rated, the produced steam is 0.2×1345 kg/s = 269 kg/s, that is obviously not sufficient to maintain the core water level at this power. Power and level should find a stability point at about 5% of rated thermal power and the water level below the top of active fuel.

The cold water injection produces a power spike that increases the core pressure and the amount of steam discharged into the suppression pool.

As the suppression pool temperature increases, the containment spray system and suppression pool cooling system start, attempting to maintain the pool water temperature below 23 degrees C.

As the low pressure cooling systems cannot start, because the core pressure is well above the intervention setpoint for core spray and LPCI (Low Pressure Cooling Injection), core damage for high fuel temperature or drywell failure for high pressure is expected. Calculations performed by APROS code shows that the suppression pool reaches the saturation temperature within 20 minutes and the containment fails consequently for high pressure after 10 more minutes, in these conditions.

In summary, the sequence of events is as follows [17], [18], [19]:

Event	Time (min.)
MSIVs closure	0
Recirculation Pump Trip	0.1
Safety Relief Valves open	0.2
Feedwater trip	8
Aux. Feed Sys. starts	10
Core uncovers	13
Containment failure	> 30

5.2.5 ATWS With Operator Actions

The operators should try to insert negative reactivity using alternative methods, as soon as they recognize that both of the automatic scrams have failed.

The following is a list of actions and controls that an operator is expected to perform, in an ATWS in a Swedish BWR reactor:

- Activate the manual scram signal (if it succeeds the reactor can be safely shut down).
- Insert rods by the electromechanical system (screw). It is assumed that this action also fails. This system is actually unique to the Swedish BWR reactors.
- Activate the boron system. This system is designed to shut down the reactor in about 20 minutes from activation.
- Manually insert control rods, one at the time. As the average time to completely insert a control rod from a fully withdrawn position is about 45 seconds, this action is considered a backup of the boron system.
- Activate the ADS (Auto Depressurization System) to depressurize the reactor, so that the low pressure injection system can be activated (if the Auxiliary Feedwater System is not sufficient to maintain the water level).
- Keep the reactor water level low (near the top of the core), so that the natural circulation core flow and power stabilize at a lower level.
- Monitor the suppression pool water temperature and level.
- If the MSIV closure was caused by a false signal, the operator can try to open the valves, in order to re-establish the link between the reactor and the main condenser (improve heat sink capability).

In summary, a complete ATWS scenario in a Swedish BWR could be as follows:

Swedish BWR, ATWS scenario, 100% core power, 100% core flow

- MSIVs close for a false high radiation isolation signal.
- Scram fails (ATWS). The recirculation pumps trip on high dome pressure. APRM neutron flux peaks sharply.
- Relief valves open on high pressure and the produced steam flushes down to the suppression pool.
- The reactor water level is controlled by the feedwater control system.
- The water level in the main condenser decreases, because the condenser is isolated.
- The reactor is in a nearly steady state condition at about 20% power, natural circulation, normal water level and steam discharged to the suppression pool. Level and temperature in the suppression pool are almost linearly increasing.
- Other methods to insert control rods quickly into the core fail.
- Further development of the scenario is dependent by what action the operators perform:
- The boron system is activated

The boron system takes some time to become effective. As the main feedwater system is supposed to trip after few minutes for low suction pressure, the auxiliary feedwater system is the only supply of water to the reactor. If this is sufficient to compensate for the steam loss through the relief valves or not, depends on the thermal power behaviour. If CAMS prediction for this strategy fails, the operator may try to reopen the closed MSIVs in order to rise the main condenser level and utilize the main feedwater pumps to maintain the reactor level. Supply of water to the main condenser from the CST (Condensate Storage Tank) is also a recommended solution.

If the main condenser cannot be restored, and the CAMS system anticipates core uncovery, the ultimate strategy is the reactor depressurization through ADS, so that low pressure emergency systems can be activated.

- The boron system is not activated or fails

The same considerations as above apply in this case. However, if the main condenser is lost, the CAMS system should make a prediction on the capability of the suppression pool cooling system to maintain the temperature and pressure below the alarm setpoint. If the containment is predicted to fail (because the power is too high), the anticipated time of the failure may well represent the time allowance to restore the compromised safety systems.

5.2.6 Strategy Generator Requirements at an ATWS

The strategy generator will be able to generate the operator actions described above, when applicable. These include:

- ADS actuation if the reactor water level is not likely to be maintained by the high pressure emergency systems.
- Boron system actuation, if available
- Main condenser function restoring, through re-opening the MSIVs valves
- Lower the reactor level to the top of active fuel, to reduce the core thermal power to the minimum possible.

5.2.7 The CAMS in ATWS Accident Scenarios

CAMS can provide valuable informations during the ATWS sequence. Key points that are demonstrated are:

- Anticipate ADS depressurization strategy, if required. Late activation of this strategy result in a temporary uncovery of the core.
- Anticipate strategies to avoid the use of the low pressure cooling systems. The large amount of cold water delivered by these systems frequently causes problems in stabilizing the power and pressure.
- Avoid the use of the boron system. The use of this system results in a very long shutdown period, to recover the plant. Many EOP prescribe to activate the boron system when (and if) the suppression pool temperature exceeds the high level setpoint.

If the one-by-one manual control rod insertion works, CAMS evaluates the time left for alternative actions and propose procedures in order to shut down the reactor safely without the boron system.

5.3 PRFO (Pressure Regulator Fails Open)

5.3.1 PRFO frequency

Small transients are normally considered perturbations in the reactor power-flow conditions that do not threaten the fuel elements and the primary containment above the design values.

Though small transients are not normally considered from a safety standpoint, their importance should not be underestimated, for the following reasons:

- One of the TMI and Chernobyl lessons is that many severe accidents scenarios originate by a small transient not clearly identified that promotes one or more operator errors, that eventually bring the reactor into an accident condition.
- Small transients often result in a quick plant shutdown (reactor scram). That has a great impact on the availability factor and then on the economic return.

5.3.2 Classification of small transients

Small transients that have some operational impact are generally classified as:

- pressurization events,
- cold water events.

To the first category belong all those transients where there is a relatively large increase or decrease in the reactor pressure, that usually results in a high neutron flux or high pressure scram. Examples are:

- Load rejection
- MSIV's closure
- Pressure regulator failure (closure)
- Relief valve opening.

Cold water events are those transients where a large and unexpected amount of cold water enters the vessel. Scram usually occurs for high neutron flux or high reactor level. Examples are:

- Loss of feedwater heating
- Feedwater controller failure

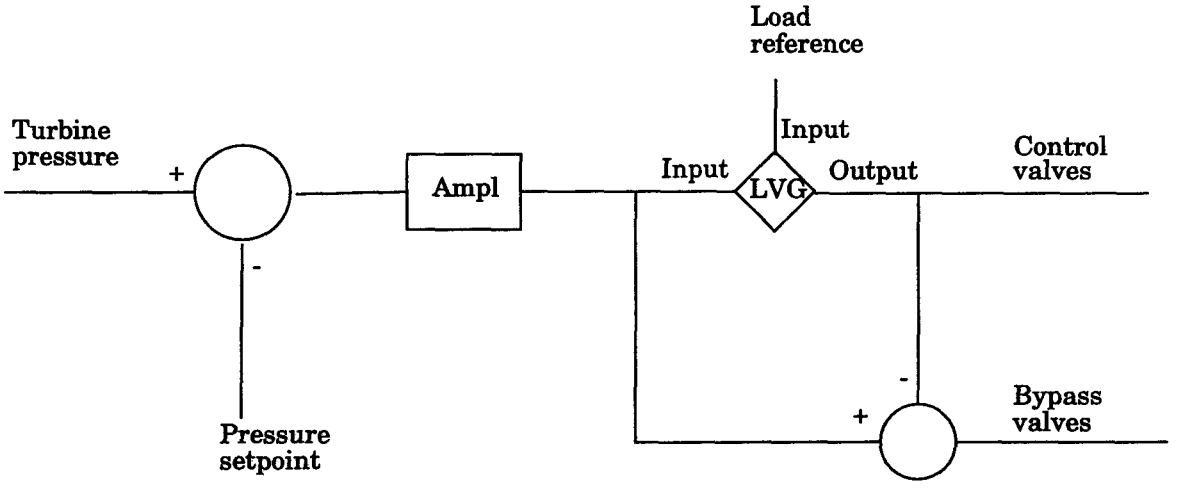
- Inadvertent HPCS (or Auxiliary Feedwater System) startup.
- PRFO (Pressure Regulator Fails Open

Pressurization events usually result in a high flux scram in few seconds, so that no time is left to the operators to initiate any action in order to avoid the shutdown. Some of the cold water events instead are very slow transients that, if promptly identified, can be mitigated with no or low impact on the availability factor (no scram).

The PRFO has been incorporated into the repertoire of CAMS scenarios.

5.3.3 Description of PRFO

The pressure regulator logic controls the opening position of the turbine control valves and bypass valves, in order to maintain the reference load and the inlet pressure at the setpoint value. A simplified diagram of the control logic is as follows:



Normally, at 100% power, the difference between the sensed turbine pressure and the pressure setpoint is 30 psi. The amplifier has a 3.33 gain, so the signal from the amplifier to the LVG (Low Value Gate) is 100. The LVG is a circuit that gives an output signal equal to the smaller of the two input signals.

As the diagram shows, if the load reference is for example 80%, the output signal from the LVG to the control valves is 80% (80% opening), and the difference 100-80=20% to the bypass valves.

During normal full power operation, the load reference is set to 100%, so that the LVG output is 100 and Bypass signal is 0.

The PRFO originates from a failure in this logic or in the pressure sensors. For example, a failure in the linear amplifier could generate an output signal of 200, instead of 100. In this case the LVG output should not change, but the signal to the bypass valves would sharply increase to 100, opening the valves completely.

In this simulation we have supposed a failure in the summation amplifier of the bypass line, thus generating a signal output of 100 instead of 0. The APROS diagram of Figure 9 displays the first

30 seconds of this transient for few selected variables. The sequence of events can be explained as follows:

- The bypass valves completely open as a consequence of a failure in the signal value in the pressure regulator.
- The reactor pressure sharply decreases, voids increase and the neutron flux collapses to about 40%, due to the negative void feedback.
- The reactor water level increases because of the high void content, but it does not reach the high level scram setpoint (in some plants it does happen, actually).
- The pressure regulator detects the pressure decrease and start to close the control valves (the bypass valves are blocked open) to recover the pressure to the setpoint value (see Figure 11).
- Neutron flux, level, voids and pressure return to approximately the previous steady state value, after about 50 seconds (see Figure 10).
- Since most of the steam go directly to the condenser through the bypass valves, there is a lack of steam in the feedwater preheaters, that cannot maintain the water temperature (see Figure 11).
- As the feedwater temperature decreases, the neutron flux increases slowly, because of the increased core subcooling. After about 100 seconds it reaches the high flux scram setpoint.

As APROS simulation shows, the operators have less than 5 minutes to initiate mitigation actions to avoid the high flux scram. The required action in this case is to reduce core power to stay away from the scram setpoint and detect the failure.

There are two ways to reduce power in a nuclear power plant:

- Reduce core flow,
- Insert control rods.

The first method is much faster and is usually the preferred method when the requested power reduction is less than 50%. If the operator chooses to reduce the core flow to mitigate the PRFO transient, that could be very frustrating, because the high flux scram setpoint is dependent on the core flow value (it is 20% above the 100% rod line). Moreover, the ratio between core flow and feedwater flow lowers, so that the core subcooling get even worse.

Figure 12 and Figure 13 show the PRFO simulation with 10% power reduction by inserting control rods, after 60 seconds from the failure. The amount of power reduction to avoid scram is plant and initial condition dependent, and could be optimized by the strategy generator of CAMS.

5.3.4 The PRFO scenario in CAMS

The PRFO scenario in CAMS is as follows:

- Start the PRFO event (snapshot file)
- The operator recognize that something is happening and run the predictive simulator with no actions.
- The operator is informed that the plant will be shutdown in about 100 seconds for high neutron flux.
- The operator run the strategy generator to get the possible solutions.
- The strategy generator informs him that he should decrease the core power by 10 % inserting control rods.

- After the new steady state condition is reached, the operator detects the failure in the pressure regulator controller.

6. FUTURE DEVELOPMENT

The Halden joint programme for 1995 lists the following research activities in the future CAMS development:

- signal validation and tracking simulation,
- strategy generation and predictive simulation,
- user interface and testing.

The possibility to make a PWR version of CAMS will be investigated. It is important to have close cooperation with a utility. The work will be coordinated with the plans for an ISACS-2 prototype and with the Nordic project RAK-2.2. (ISACS-2 is a project at the Halden Man-Machine Laboratory.) The RAK-2.2 effort will concentrate on testing and evaluation of the system. An important test will be carried out in cooperation with SKI at the 4th of May 1995.

7. REFERENCES

[1] Andreas Bye, Aimar Sørenssen, Knut Tiseth:
Principles of early fault detection and signal validation.
HWR-279. March 1991.

[2] Andreas Bye, Aimar Sørenssen:
Implementation and first experience with a signal validation system for flow sensors.
HWR-280. May 1991.

[3] Kjell Arvid Ådlandsvik, Aimar Sørenssen, Andreas Bye, Øivind Berg:
Signal validation for feedwater flow sensors.
HWR-328. February 1993.

[4] Aimar Sørenssen:
An early fault detection system running on a live power plant.
HWR-261. January 1990.

[5] Paolo Fantoni, Alessandro Mazzola:
Applications of auto-associative neural networks for signal validation in accident management.
Proc. of the IAEA specialist meeting on "Advanced Information Methods and Artificial Intelligence in Nuclear Power Plant Control Rooms", Halden, September 1994.

[6] Bård Moum:
Using APROS as tracking mode simulator.
Halden Project Internal Note, MMSR-Note 1877. October 1993.

[7] Lars Petter Endresen:
CAMS tracking simulator.
Halden Project Internal Note, MMSR-Note 1809. June 1994.

[8] Miki Sirola:
Strategy generator in computerized accident management support system.
VTT Publications 163. 1993.

[9] Fridtjov Øwre, Conny Holmström, Svein Nilsen, Paul van Gemst:
Safety assessment and post trip guidance -
The SAS II Project for the Forsmark NPP: - A final report.
HPR-342. February 1993.

[10] Eero Silvennoinen, Kaj Juslin, Markku Hänninen, Olli Tiihonen, Jorma Kurki, Kari Porkholm:
The APROS software for process simulation and model development.
VTT 618. May 1989.

[11] Fridtjov Øwre, Jan Porsmyr, Ari Kautto, Erik Söderman:
CAMS - Computerized accident management support system - A feasibility study.
HWR-287. May 1991.

[12] Geir Meyer:
A proposal to the coupling between the modules in CAMS.
MMSR-Note 1884. May 1994.

[13] Geir Meyer:
The CAMS data structure. Preliminary.
MMSR-Note 1885. August 1994.

[14] IONA Technologies:
Programmer's Guide" and "Advanced Programmer's Guide"
(These are manuals for Orbix.)

[15] Geir Meyer:
orbix^{TM}, distributed object technology. An impression after the first few days of use, including some benchmarks.
MMSR-Note 1886. June 1994.

[16] W. C. Arcieri, D. J. Hanson:
Instrumentation availability during severe accidents for a boiling water reactor with a Mark I containment.
NUREG/CR-5444, EGG-2661. 1992.

[17] R. M. Harrington, S. A. Hodge:
ATWS at Browns Ferry Unit One - Accident Sequence Analysis.
NUREG/CR-3470, ORNL/TM-8902. July 1984.

[18] S. A. Hodge, J. C. Cleveland, T. S. Kress, M. Petek:
Identification and Assessment of BWR In-Vessel Severe Accident Mitigation Strategies.
NUREG/CR-5869, ORNL/TM-12080. October 1992.

[19] Forsmarkverket, Vattenfall:
Forsmark 1, 2, 3.
ISBN 91-7186-272-2.

[20] Øivind Berg, Miki Sirola, Aimar Sørenssen, Fridtjov Øwre, Kjell-Arvid Ådlandsvik:
The Halden Reactor Project Workshop Meeting on Computerised Accident Management Support.
HWR-335. January 1993.

[21] Nuclear Regulatory Commission:
Severe accident risks: an assessment for five US nuclear power plants.
NUREG-1150. Nuclear Regulatory Commisssion, Dec 1990.

APPENDIX I

This appendix gives some examples of pictures in the CAMS man-machine interface, and some APROS pictures from an accident scenario:

- Figure 3 - Overview of the relation between CAMS and other operator support systems
- Figure 4 - CAMS Overview Picture
- Figure 5 - Picture selector
- Figure 6 - Motorway diagram for energy
- Figure 7 - Trend diagram for the core
- Figure 8 - Output from the strategy generator.
- Figure 9 - PRFO, the first 30 seconds, reactor variables
- Figure 10 - PRFO, the first 200 seconds, reactor variables
- Figure 11 - PRFO, the first 200 seconds, turbine variables
- Figure12 - PRFO, with power reduction to 90 %, reactor variables
- Figure 13 - PRFO, with power reduction to 90 %, turbine variables

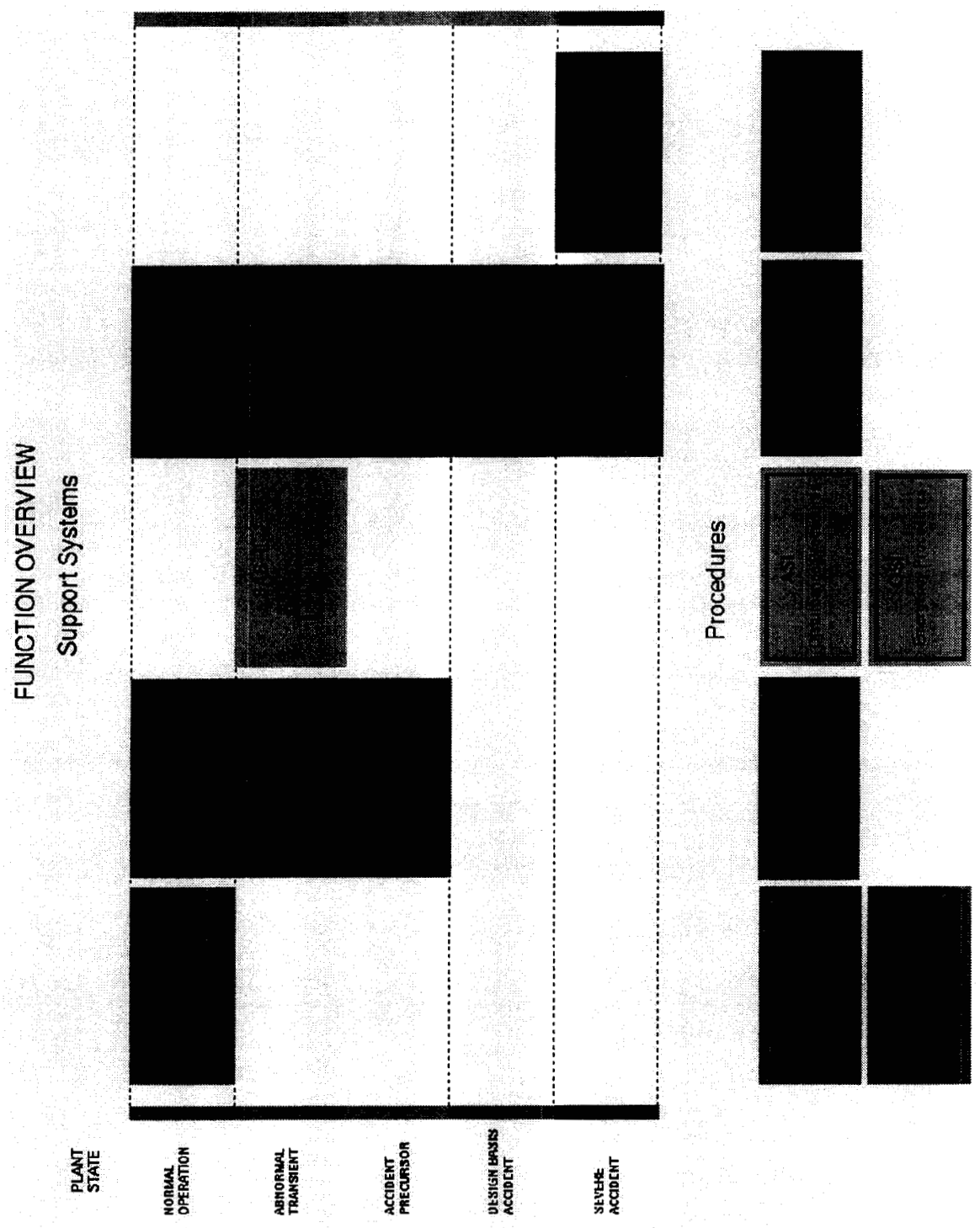


Figure 3 Overview of the relation between CAMS and other operator support systems.

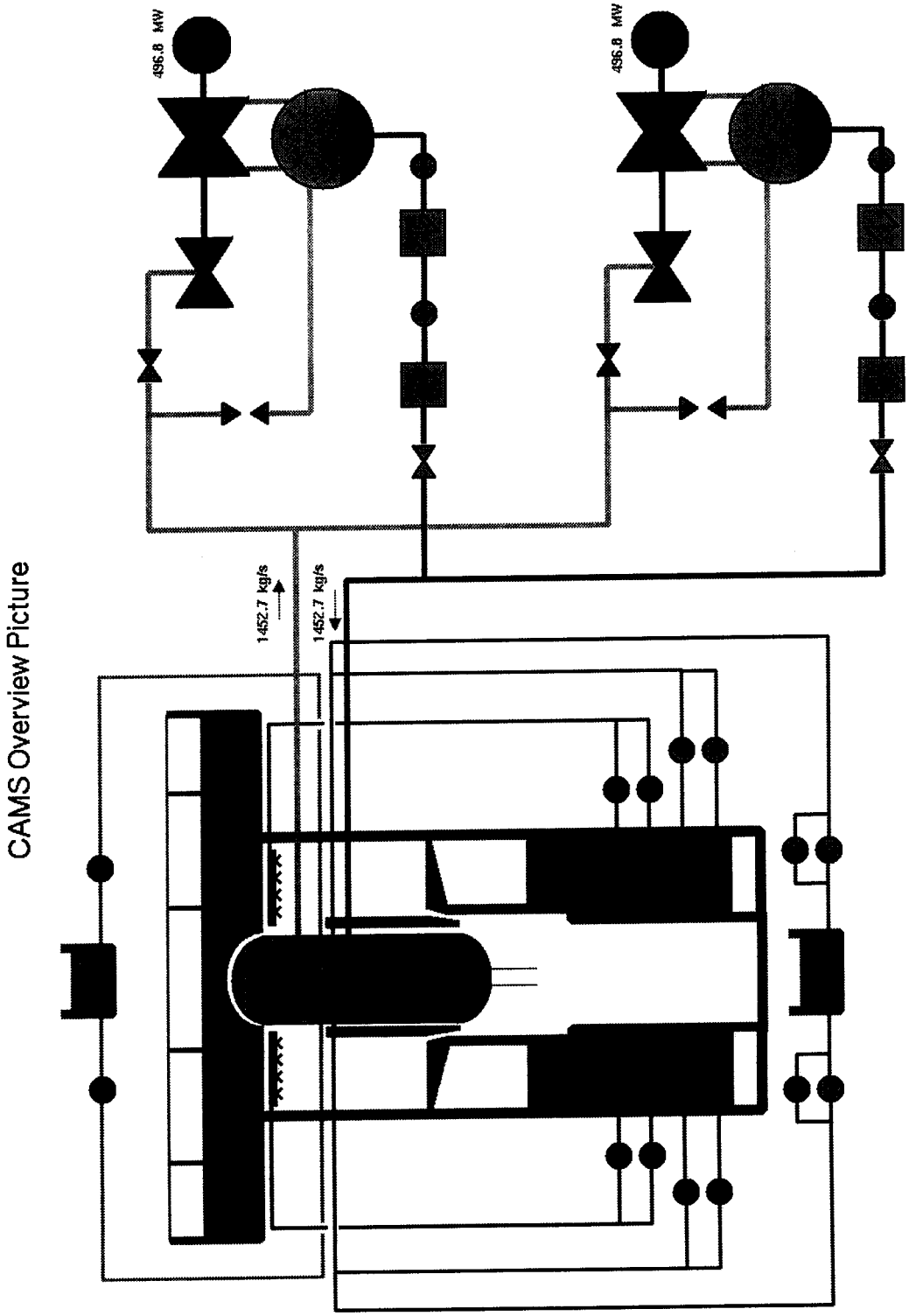


Figure 4 CAMS Overview picture

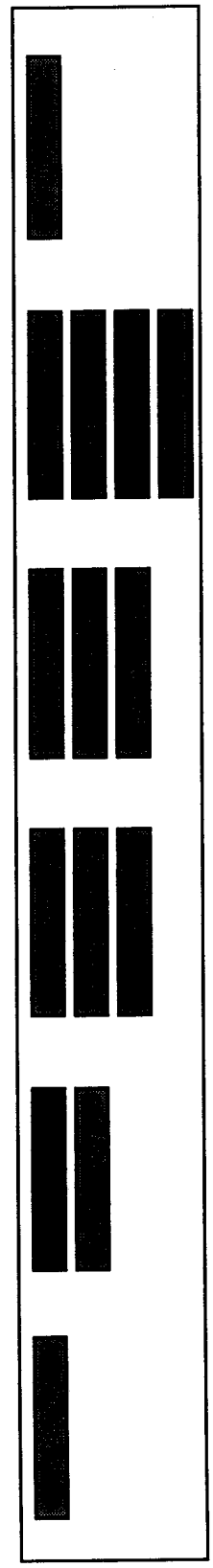


Figure 5 Picture selector

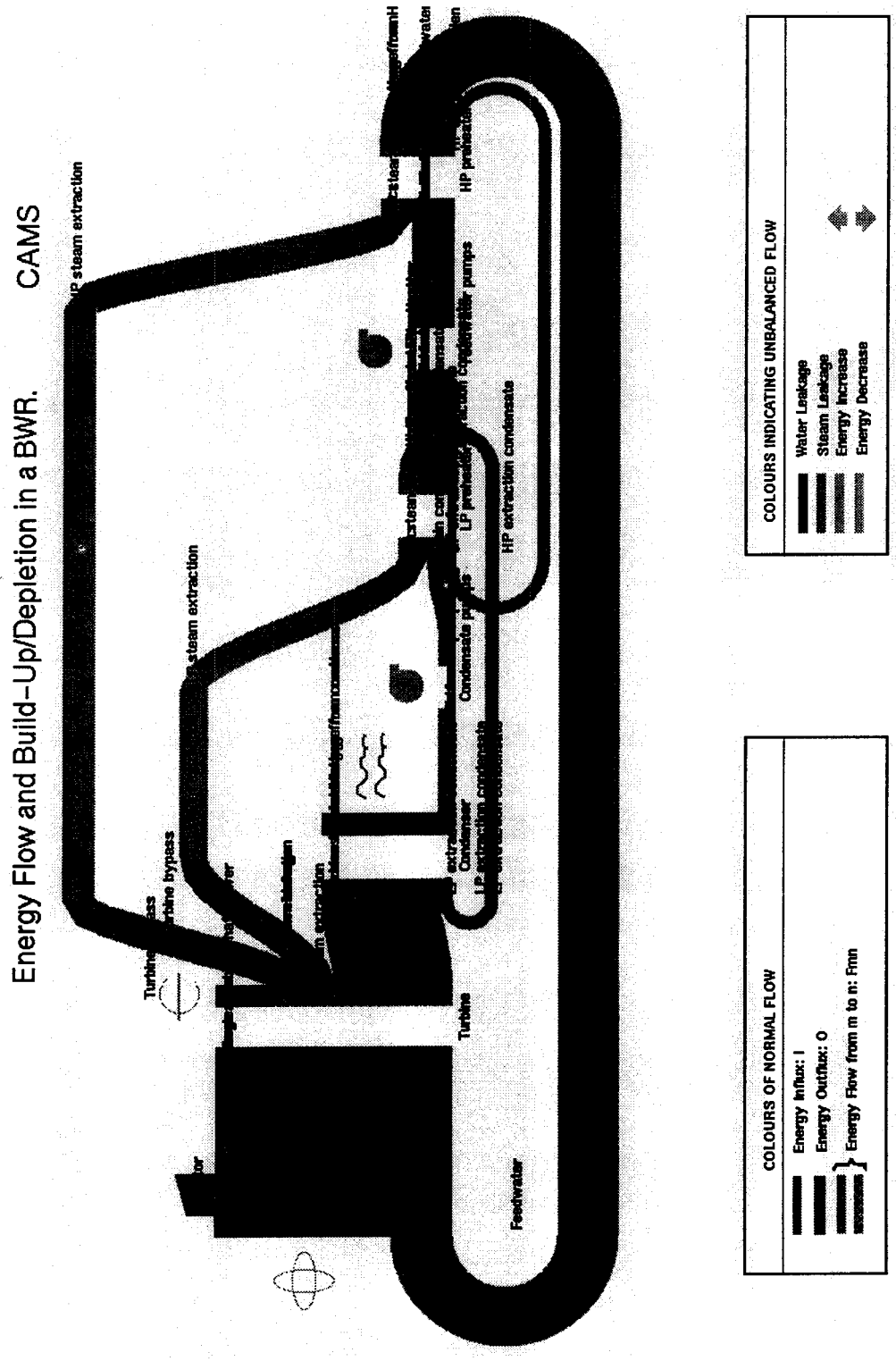


Figure 6 Energy motorway

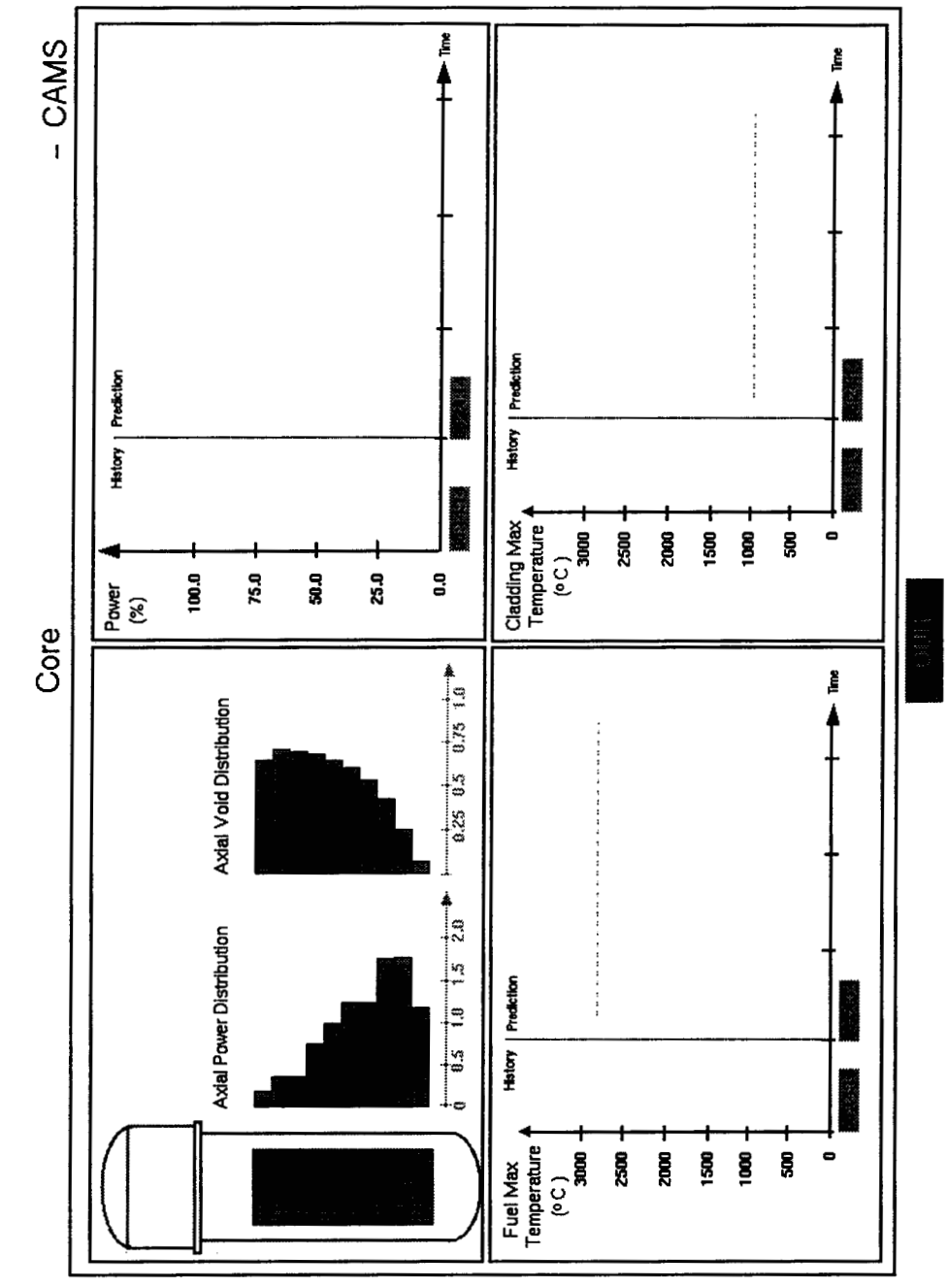


Figure 7 Trend diagram for the core, showing future as well as past

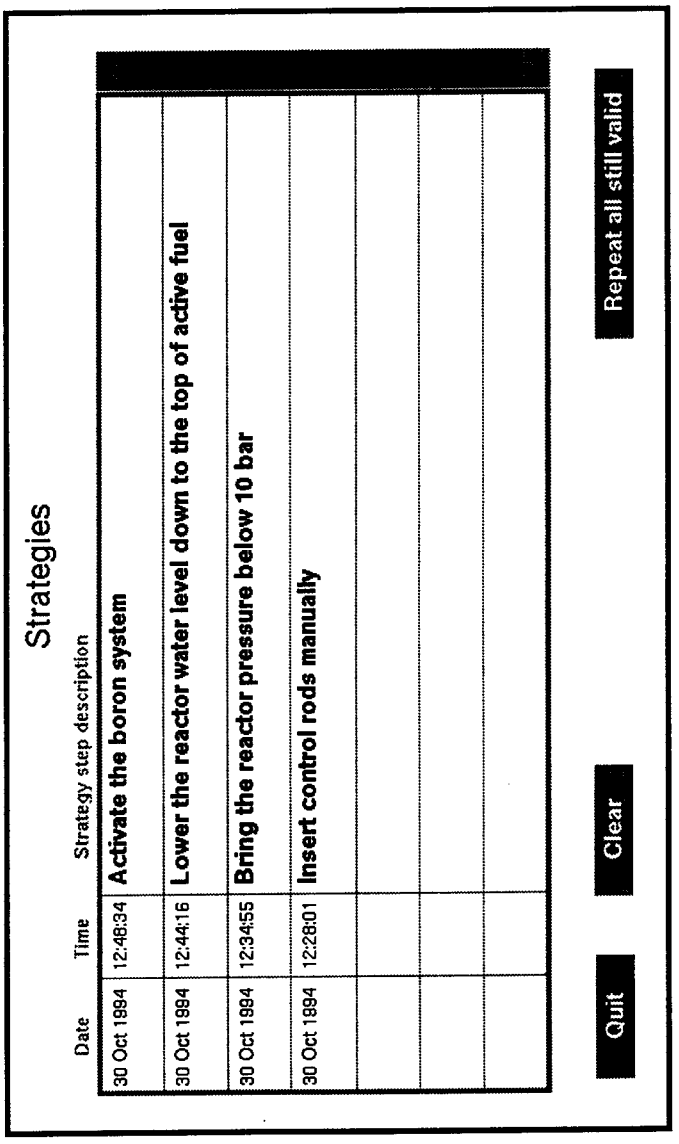
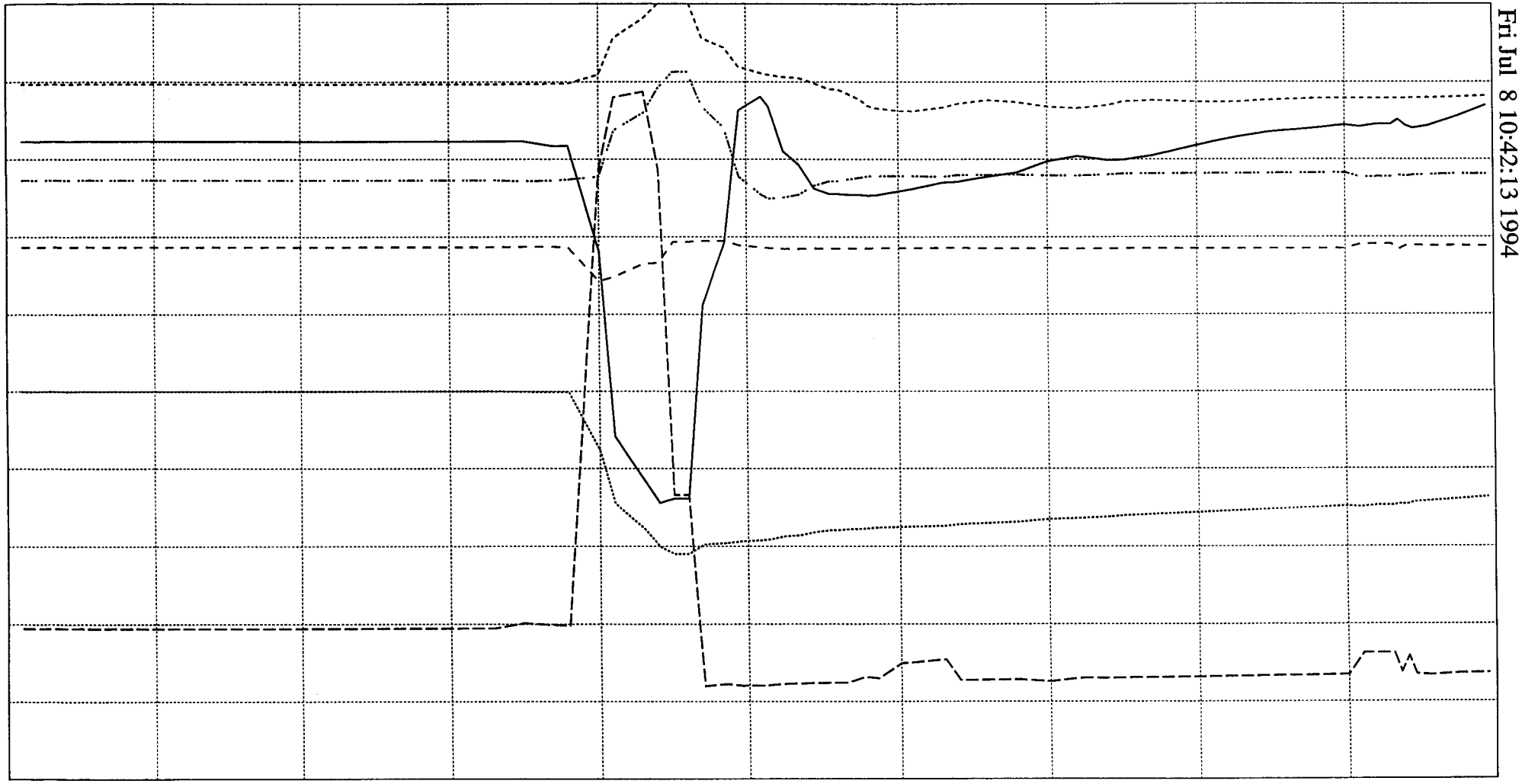


Figure 8 Output from the strategy generator

APROS

TURBINE BYPASS FAIL OPEN



Core average neutron flux	0.000e+00	1.250e+00
Core flow (kg/s)	0.000e+00	1.500e+04
Reactor dome pressure (Bar)	6.000e+00	8.000e+00
Reactor water level (m)	3.000e+00	4.000e+00
Total steam flow (kg/s)	1.200e+03	2.500e+03
Core exit void fraction	4.000e-01	8.000e-01

Figure 9 - PRFO, the first 30 seconds, reactor variables

APROS

TURBINE BYPASS FAIL OPEN

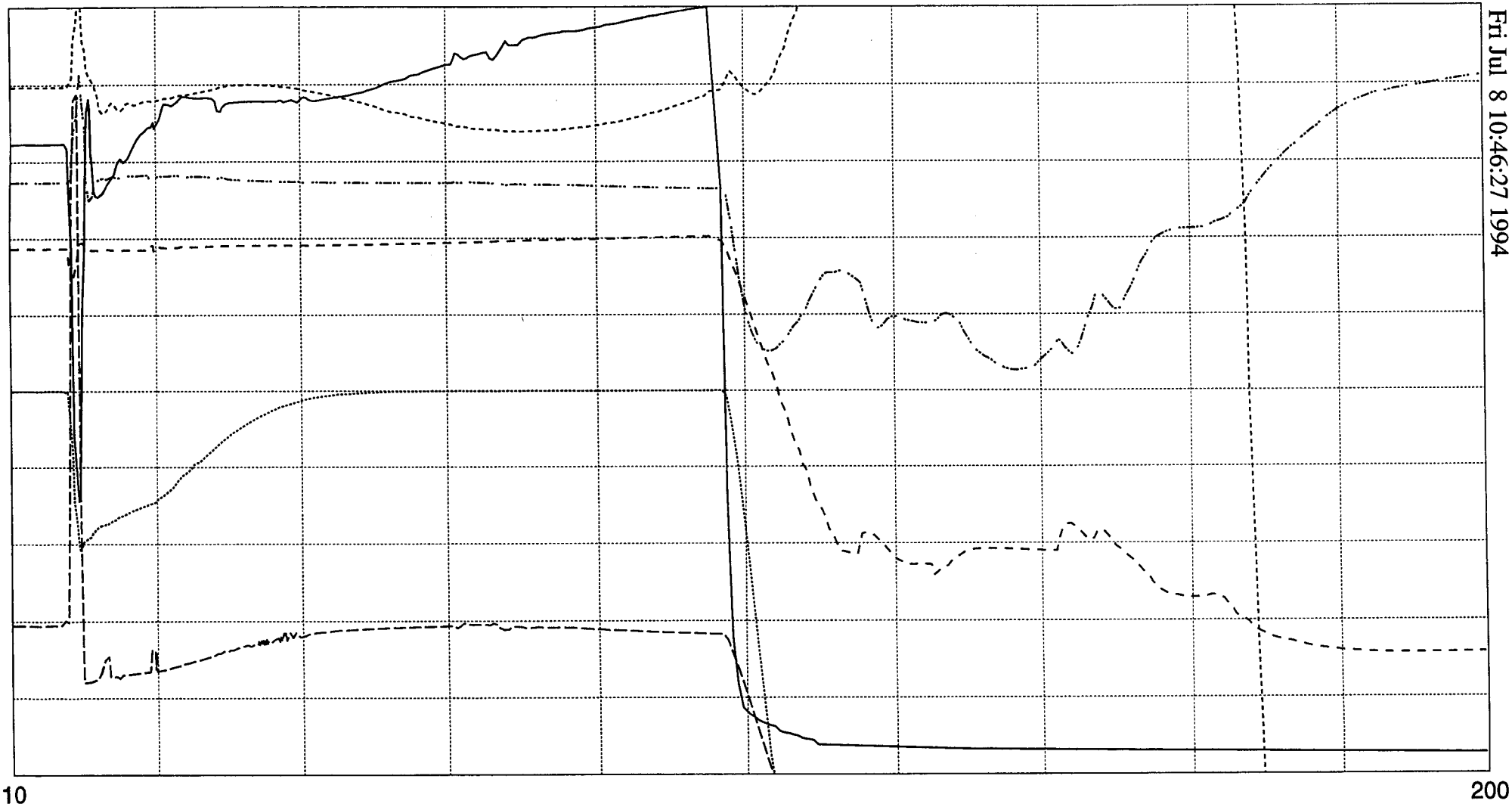
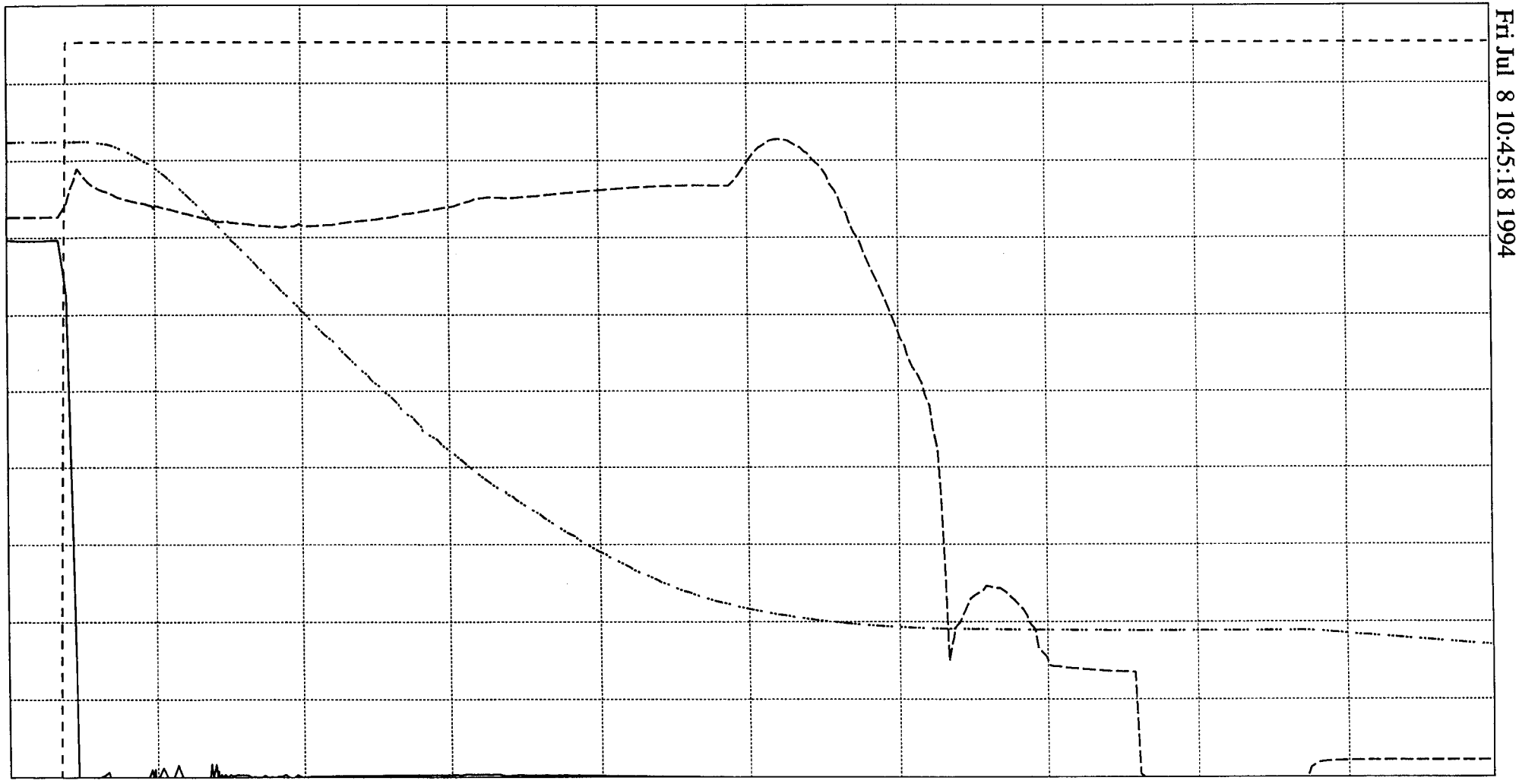


Figure 10 - PRFO, the first 200 seconds, reactor variables

Core average neutron flux	0.000e+00	1.250e+00
Core flow (kg/s)	0.000e+00	1.500e+04
Reactor dome pressure (Bar)	6.000e+00	8.000e+00
Reactor water level (m)	3.000e+00	4.000e+00
Total steam flow (kg/s)	1.200e+03	2.500e+03
Core exit void fraction	4.000e-01	8.000e-01

APROS

TURBINE BYPASS FAIL OPEN

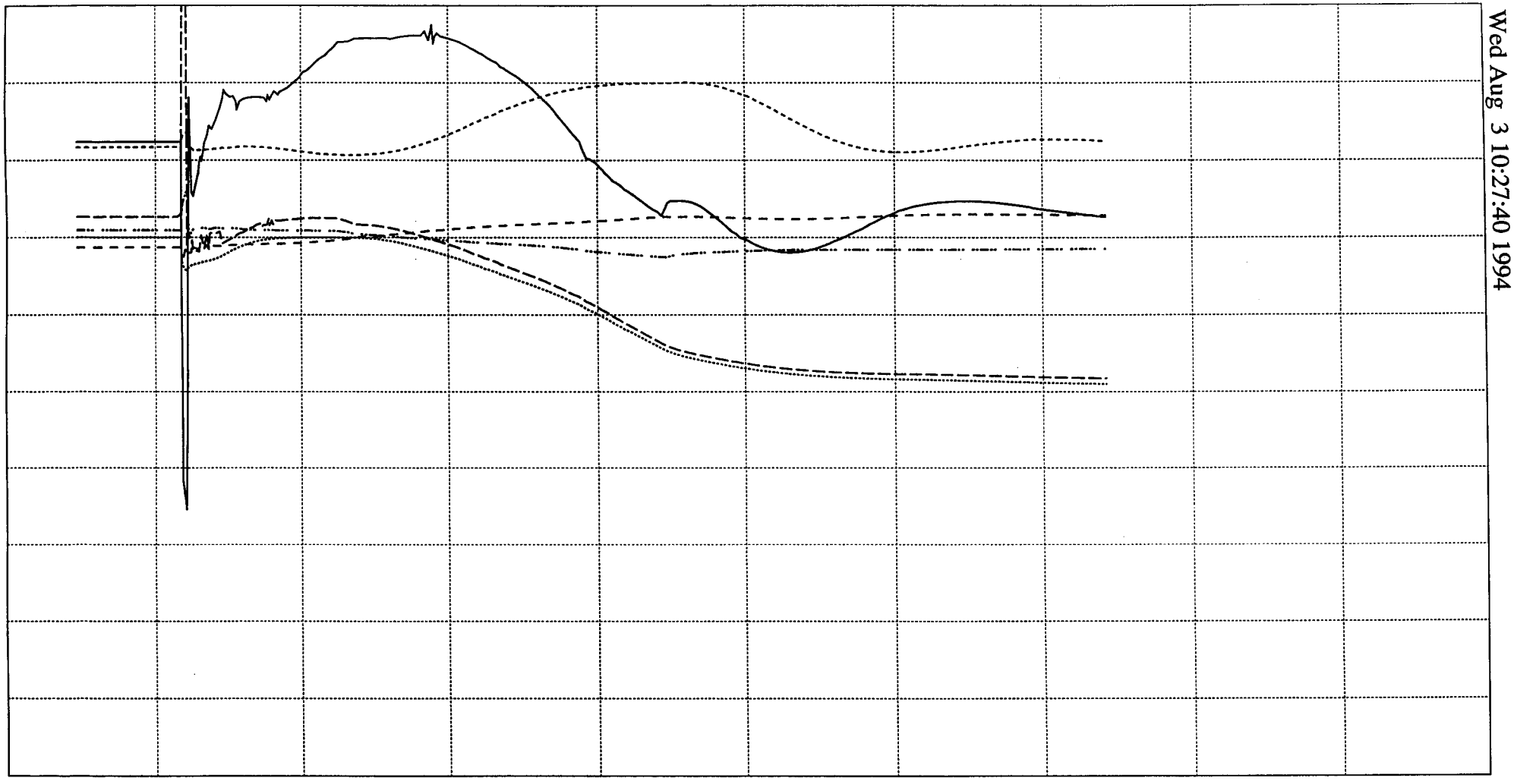


Control valves position	0.000e+00	1.050e+00
Bypass valves position	0.000e+00	1.050e+00
Relief valves flow (kg/s)	0.000e+00	1.000e+02
Safety valves flow (kg/s)	0.000e+00	1.000e+02
Feedwater flow (kg/s)	0.000e+00	2.000e+03
Feedwater temperature (C)	3.000e+01	2.000e+02

Figure 11 - PRFO, the first 200 seconds, turbine variables

APROS

TURBINE BP FAIL OPEN AND POWER REDUCTION TO 90%

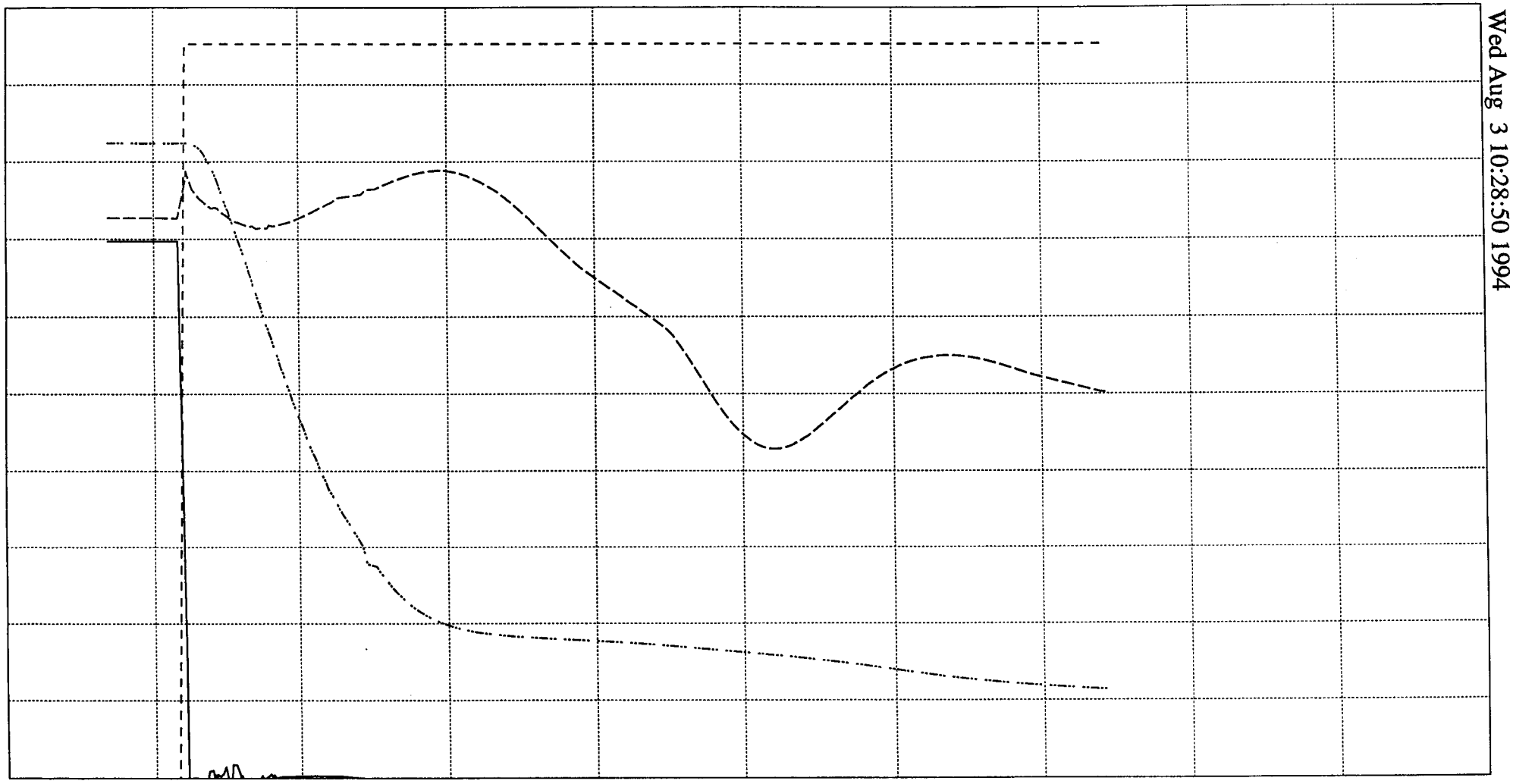


Core average neutron flux	0.000e+00	1.250e+00
Core flow (kg/s)	0.000e+00	1.500e+04
Reactor dome pressure (Bar)	0.000e+00	1.000e+01
Reactor water level (m)	-1.000e+00	5.000e+00
Total steam flow (kg/s)	0.000e+00	2.000e+03
Core exit void fraction	0.000e+00	1.000e+00

Figure12 - PRFO, with power reduction to 90 %, reactor variables

APROS

TURBINE BP FAIL OPEN AND POWER REDUCTION TO 90%



Control valves position	0.000e+00	1.050e+00
Bypass valves position	0.000e+00	1.050e+00
Relief valves flow (kg/s)	0.000e+00	1.000e+02
Safety valves flow (kg/s)	0.000e+00	1.000e+02
Feedwater flow (kg/s)	0.000e+00	2.000e+03
Feedwater temperature (C)	3.000e+01	2.000e+02

Figure 13 - PRFO, with power reduction to 90 %, turbine variables