CONF-8711245--3

DE89 770344

CONF-8711245--3

88001744 IT

R. BRUSCHI, P. DI PORTO, R. PALLOTTELLI

ENEA-PEC/PRO/PEA/SIM, P.O. box 2400 - 00100 ROMA (Italy)

An expert system for nuclear plant malfunctions consequences, implemented and tested on a reactor simulator

ABSTRACT

The proposed system is composed of different phases. In the first phase the early detection of malfunctions is realized, to identify the origin of malfunctioning conditions. In the second one "previsional" methods are developed, showing very rapidly the probable evolution of an uncontrolled accidental condition.

These techniques are implemented on a nuclear power plant simulator.

INTRODUCTION

Aim of the work is to describe the activity we are carrying on, in order to improve safety in Man-Machine Interface, by means of automatic diagnosis and analysis of malfunctions consequences.

Some definitions are given, to allow the best understanding of this paper.

- Module -

Any plant can be divided into several parts, whose characteristics are: input variables, produced (output) variable, transfer function.

We refer to each of this parts as "real module".

A real module can correspond to a plant component or to a more complex process. We can then identify a plant and simulate it by means of "software modules" in which the transfer function is realized by means of analog or logical deterministic equations, or can correspond to a set of probabilistic relations.

- Accidental Conditions -

Recuperable and Not Recuperable Accidental Conditions (RA and NA) are considered. RA are generated by wrong actions and plant can be carried again in normal conditions. NA (malfunctions) are generated by plant faults, and there is no action to put plant again in normal conditions.

- Malfunctions (NA) Stability -

We define stable a malfunction when its evolution depends on the present conditions. Thus stability of a malfunction corresponds to the possibility to foresee its evolution.

- Operator behaviour -

In the plant control system a mayor role is played by the operator. In an accidental condition operator can react with: Correct Response (CR), No Response (NR) and Wrong Response (WR).

So there are the following possibilities

RA+CR - safety conditions are reached
RA+NR - accidental conditions remains with probability to generate malfunctions (NA)
RA+WR - accidental conditions remains with high probability to generate malfunctions (NA)
NA+CR - malfunctions remains and consequences are controlled
NA+NR - malfunctions remains and consequences are not controlled
NA+WR - malfunctions remains and consequences are amplified

So by improving operator behaviour, we improve whole plant reliability and safety.

DIAGNOSTIC

Plant is identified and simulated by software modules. Each s.m. simulates a real module of the plant (e.g. a component, a physical process, a logic procedure). A programm called DIAGNOSTIC makes all modules run, processing the plant variables ("real variables") and generating a "computed variable" (fig.1). Diagnostic function is then achieved by comparison between computed and real variables (fig.2). Real and Software modules process the same input variables (i.e. real variables). If a difference arises between output variables, a real transfer function must be changed, due to a malfunction.

The comparison must be carried on in such a way to avoid false alarms, but also to perform rapidly its task. It can be based on more or less sophisticated techiniques, to avoid errors due to noise, to wrong identification, to numerical errors etc.. We performed comparison as in fig. 3, by means of several controls of variables and derivatives values.

PREVISION

When a malfunction occurs and is detected by diagnostic, a second phase starts where

- DIAGNOSTIC continues its job, with the exclusion of the Software Module (s) where malfunction was detected.

- PREVISIONAL starts using the same Software Modules of DIAGNOSTIC, but with different connection (fig.4). So we have a Simulator, starting from Initial Conditions corresponding to the plant variables values at the time of the malfunction detection and processing a linear extrapolation of the wrong variables; it runs faster then real time, thus providing a forecast of the main plant variables values after a certain time (Prevision Time - PT). When the forecast at PT is furnished, PREVISIONAL reads present values from the plant again, computes new extrapolation of malfunctioning variables and starts for a new prevision.

PT is an important parameter of the quality and usefulness of the forecast.

It can vary from PTmax to PTmin, depending on the stability of the malfunction, as defined before.

If the transfer function of the malfunctioning variable does not change, that is when the malfunction is stable, PTmax can be selected.

The stability of the malfunction evolution is evaluated by comparing two consecutive forecasts. If the values are equal (in a fixed band) PT is increased to PTmax , otherwise it must be reduced; if the malfunction evolution changes from a stable to an unstable condition, PT is forced to decrease every cycle. It stops decreasing when it reachs PTmin or if a new stable condition occurs; this behaviour is described in fig. 5.

The initial values of PTmax and PTmin must be selected considering that:

- PTmax must be not too long:
  to avoid the growth of the extrapolation error.

- PTmin must be not too short:
  to give the operator time enough to take right decisions and to react against the malfunctions consequences.

Then their value can be changed following experience.

OPERATOR ACTION

As we have seen before, not only "sponteneous" malfunctions can occur, but also "generated" malfunctions, which are due to wrong actions of the operator, and not to a sudden change of a transfer-function.

An interactive program called OPERATOR is proposed, by means of which, during operation in normal condition, the operator selects a prevision time PT. OPERATOR reads and stores, under operator request, the initial conditions and calls PREVISIONAL, thus realizing a whole plant simulator, running faster than real time. These previsions allow the operator to know if the current sequences can bring the plant to a perturbated condition, and where a perturbation can occur, to avoid these troubles.

TOWARD AN EXPERT SYSTEM - FUTURE TRENDS

Fig.6 shows the behaviour and the possibility of the proposed techniques, to operate as an Expert System.

Functions already implemented are described by continuous lines, while dotted lines refere to functions to be realized, e.g.:

- providing diagnosis and prevision informations in an improved ergonomic way, by means of real time mimics;

- performing automatic analysis of consequences for the plant safety due to malfunction free evolution or wrong intervention, by means of a knowledge base (treesholds, known accidents, experience from other plants etc.);

- automatically on-line suggesting operational procedures;

- automatically increasing and improving the knowledge base.

APPLICATION

The proposed methods were implemented and tested on a Nuclear Reactor Simulator, instead that on a real plant; PEC Reactor Simulator was utilized. PEC (Prova Elementi di Combustibile - Test of Fuel Elements) is a 120 MWth experimental Fast Breeder Reactor under construction by the Italian Atomic Organization (E.N.E.A.).

The PEC Simulator (Pict. 1) is characterized by:

- Principal Operator Console exact replica;
- Plant identified by a 400 differential equations mathematical model, with 50 msec minimal integration step;
- Package implemented on SEL 32/77 system;
- Multipurpose instructor desk.

Implementing and testing the proposed techniques on a Simulator, instead that on a real plant, allows to apply and verify them in any possible malfunction. Their validity on the real plant must, obviously, be verified, but it will depend essentially on reliability of the Simulator itself. Plant variables under control of DIAGNOSTIC and PREVISIONAL are the following (see also fig.7 - controlled parts of the plant are in the circles):

WRI1	primary inlet flow rate north
WRI2	" " " south
WRO1	" outlet " " north
WRO2	" " " " south
WXP1	IHX primary flow rate north
WXP2	" " " " south
WEP	emergency circuit primary flow rate
AHV	reactor vessel coolant level
AHCV	component vessel coolant level
AHX1	north IHX coolant level
AHX2	south " " "
VRP1	north primary pump velocity
VRP2	south " " "
ASS1	north " " absorption
ASS2	south " " "
TCV	components vessel coolant temperature
TXPO1	north IHX outlet coolant temp. primary
TXPO2	south " " " "
TXSO1	north " " " secondary
TXSO2	south " " " "

Results are displayed on a colour CRT, where flow rates, levels, pump velocities and absorptions, temperatures are shown. For each variable there are, from high to low, name, computed value and real value. The colour code is: blue - normal, green - prealarm, red - alarm, white - prevision values. In the b/w pictures of this paper **P** indicates prealarm and **A** alarm.

An example is shown:

Pict. 2 — Plant is in normal conditions. Computed and real values are equal.

Pict. 3 — In the north pump a malfunction occurs: prealarm signal (green=P) is shown in the absorption variable, and a difference between real and computed values arises.

Pict. 4 — The malfunction is confirmed and alarm is given (red=A); fault origin is early detected; prevision can start.

Pict. 5 — First prevision: probable values after 30 sec (PTmin) are shown.

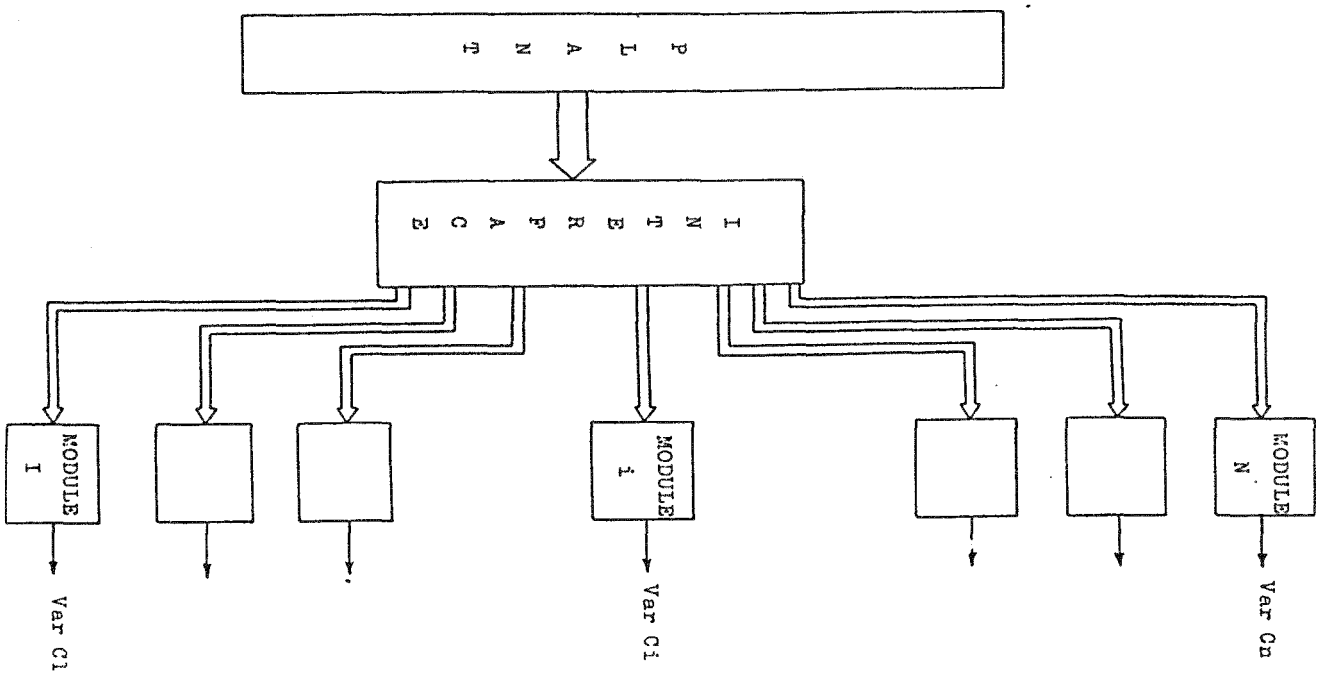
Pict. 6,7,8 — Further prevision are provided, with different PT values, depending on malfunction stability.

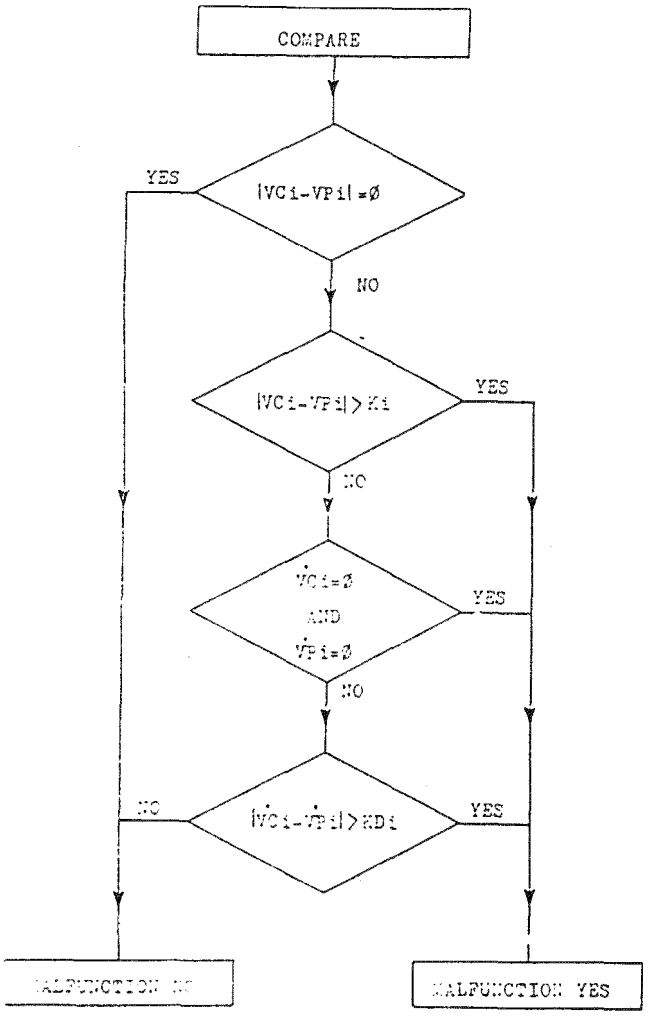
References

R. Bruschi, P. Di Porto, C. Dolciami
"Malfunction fast detection and analysis by numerical simulation". SCS Simulator Conference "All about simulators" - 18/20 April 1984, Norfolk USA.

R. Bruschi, P. Di Porto, R. Pallottelli
"Automatic analysis of malfunctions consequences - A method developed on a nuclear simulator" IAEA Seminaire international sur le diagnostic et la résponse en cas d'anomalie dans les centrales nucléaires - 12/15 June 1984, Dresden DDR.

R. Bruschi, V. Casasanta, R. Pallottelli
"DCTF: a dynamic on-line correction method of simulation models, for nuclear plants malfunctions fast detection". Enlarged Halden Program Group Meeting on Computerised Man-Machine Communication - 3/7 June, 1985 Gotheborg Sweden.


PLANT
INTERFACE
MODULE 1
MODULE i
MODULE N
Var Ci
Var Ci
Var Cn


COMPARE
|VCi-VPi|=Ø
YES
NO
|VCi-VPi|>Ki
YES
NO
V̇Ci=Ø
AND
V̇Pi=Ø
YES
NO
|V̇Ci-V̇Pi|>KDi
NO
YES
MALFUNCTION NO
MALFUNCTION YES

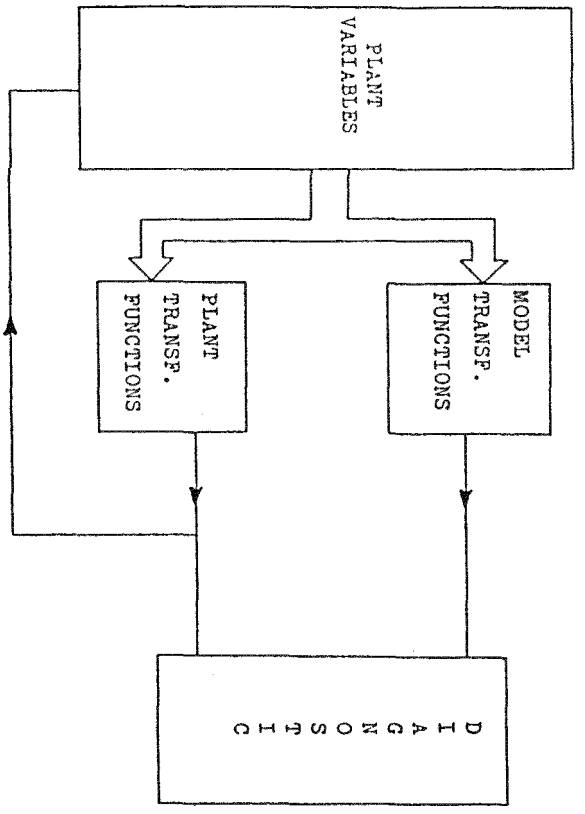
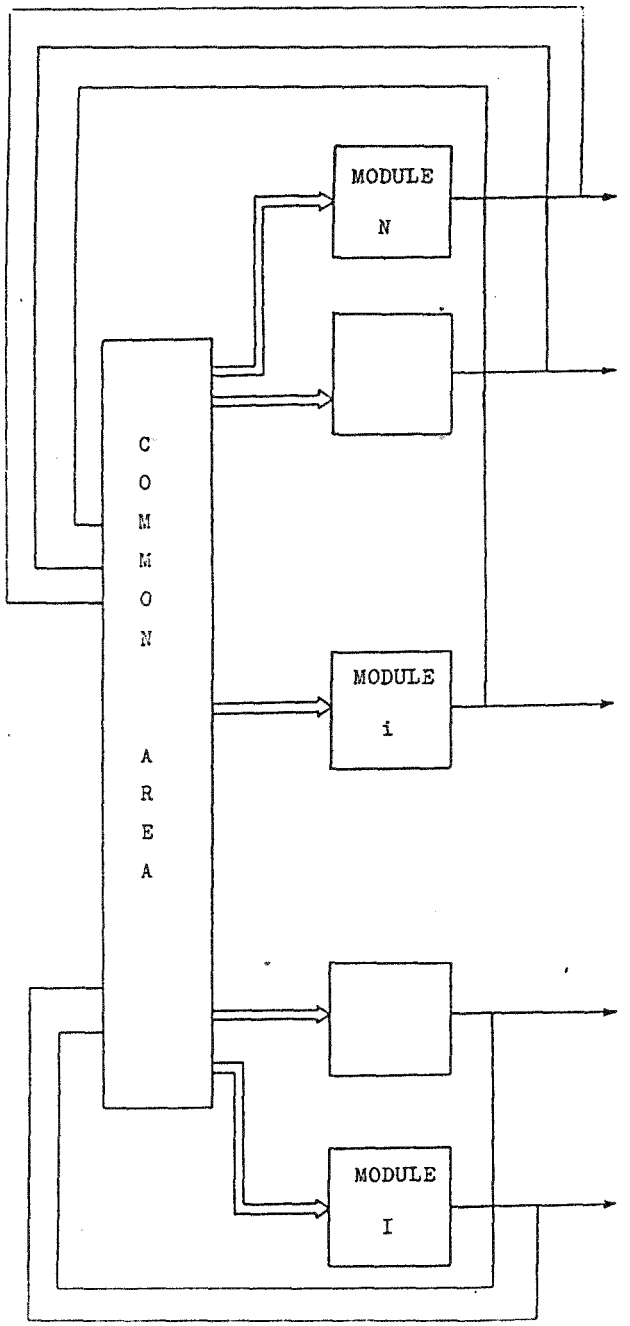

PLANT VARIABLES
PLANT TRANSF. FUNCTIONS
MODEL TRANSF. FUNCTIONS
DIAGNOSTIC

Fig. 2

Fig. 3



DCP- Difference between two consecutive previsions.

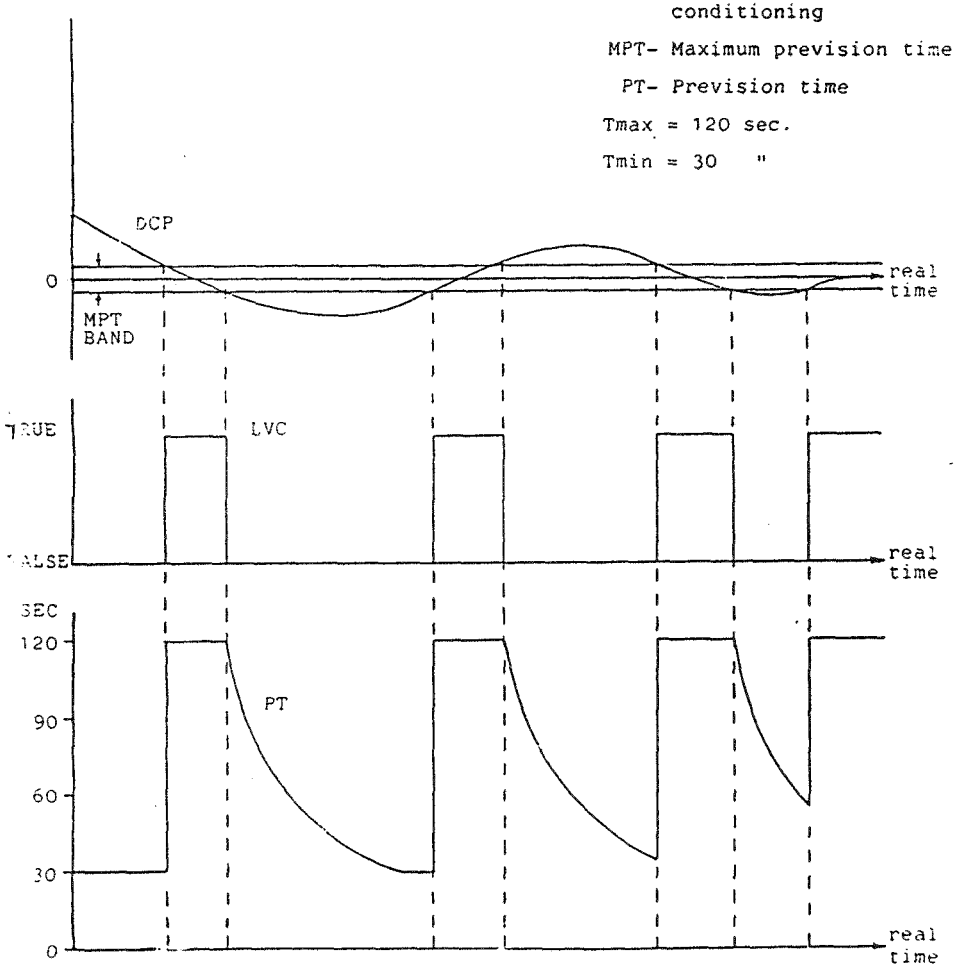
LVC- Logical variable of conditioning

MPT- Maximum prevision time

PT- Prevision time

Tmax = 120 sec.

Tmin = 30 "



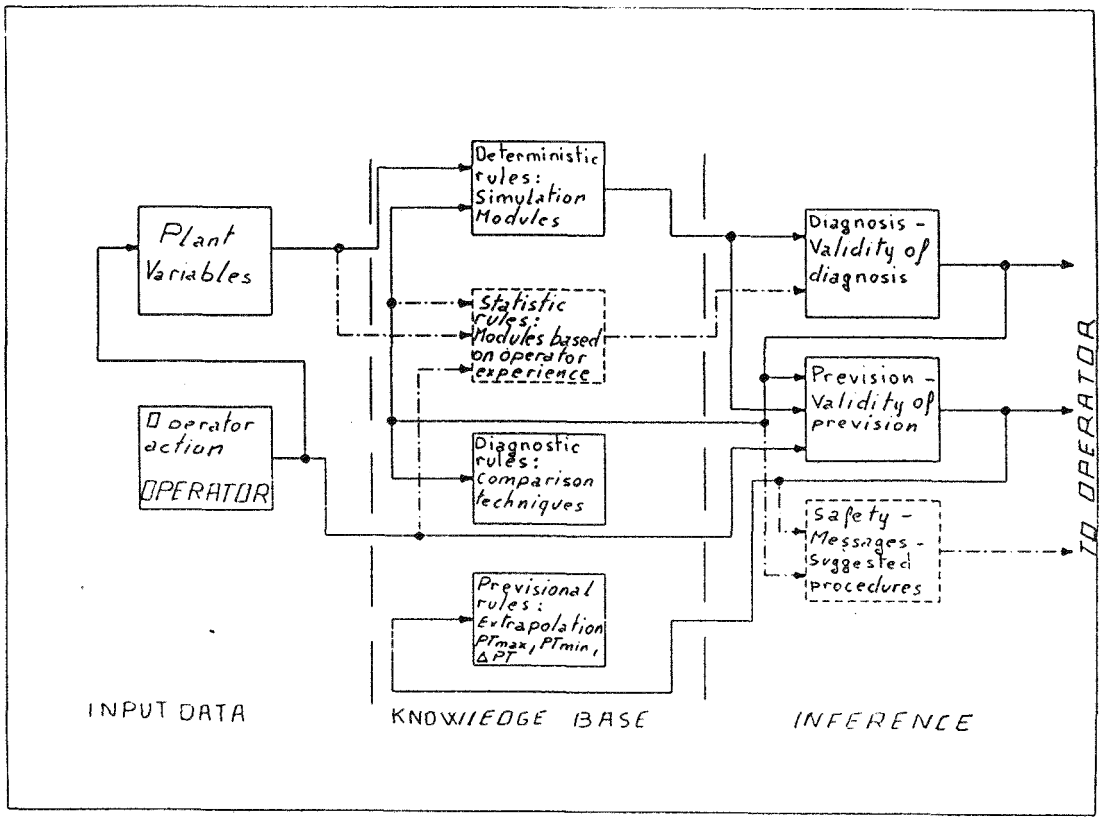

Plant Variables
Operator action
OPERATOR
Deterministic rules: Simulation Modules
Statistic rules: Modules based on operator experience
Diagnostic rules: comparison techniques
Previsional rules: Extrapolation PTmax, PTmin, ΔPT
Diagnosis - Validity of diagnosis
Prevision - Validity of prevision
Safety - Messages - suggested procedures
TO OPERATOR
INPUT DATA
KNOWLEDGE BASE
INFERENCE

Fig. 6

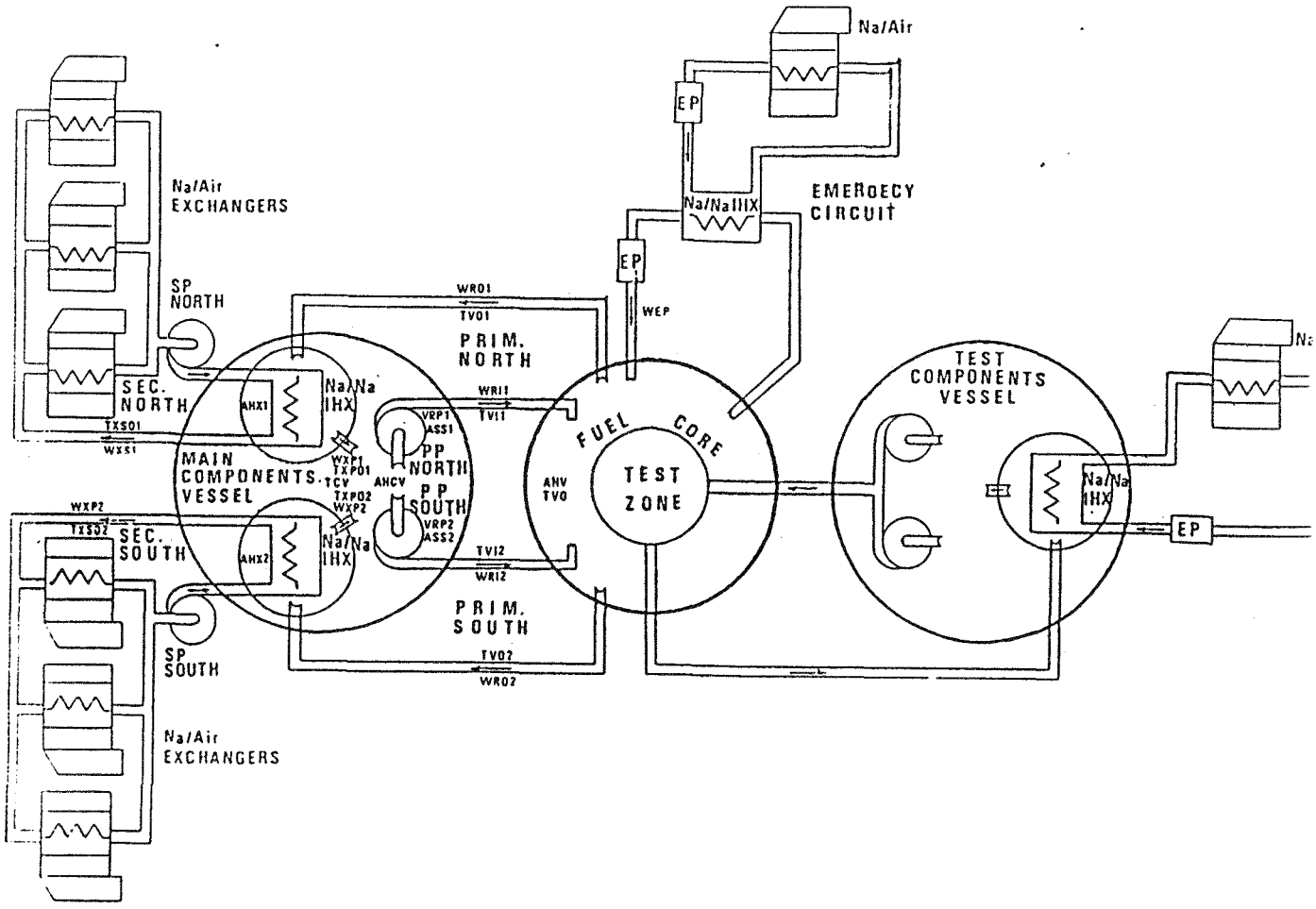
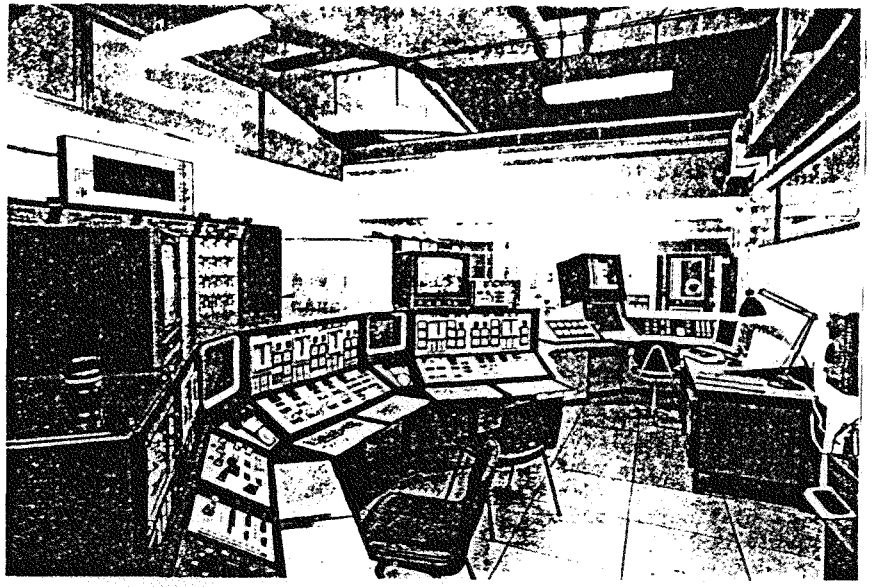
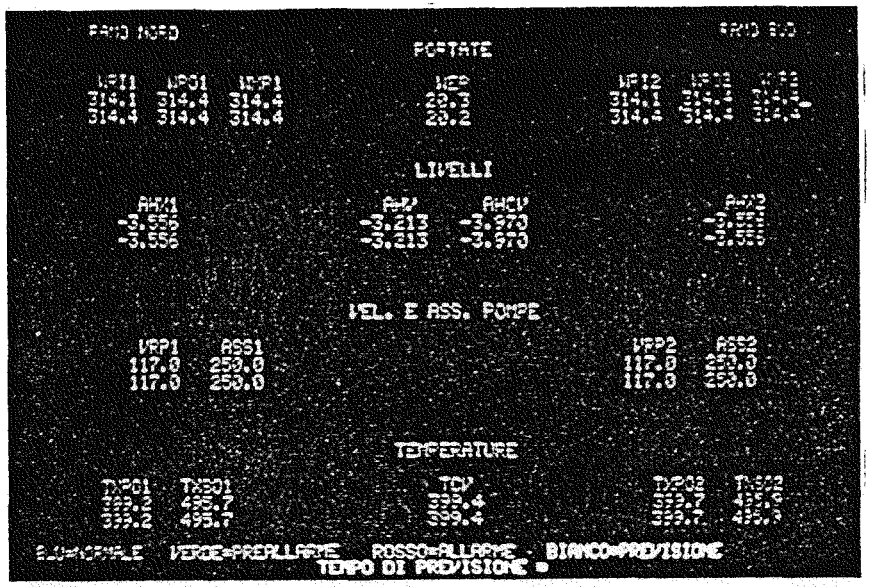

Na/Air
EP
Na/Na IHX
EMERGECY CIRCUIT
Na/Air EXCHANGERS
SP NORTH
SEC. NORTH
AHX1
WRO1
TVO1
WEP
PRIM. NORTH
WRI1
TVI1
VRP1
ASS1
PP NORTH
MAIN COMPONENTS VESSEL
WXP1
TXP01
TCV
AHCV
TXP02
WXP2
PP SOUTH
VRP2
ASS2
TVI2
WRI2
FUEL CORE
ANV
TVO
TEST ZONE
TEST COMPONENTS VESSEL
WXP2
TXS02
SEC. SOUTH
AHX2
PRIM. SOUTH
TVO2
WRO2
SP SOUTH
Na/Air EXCHANGERS

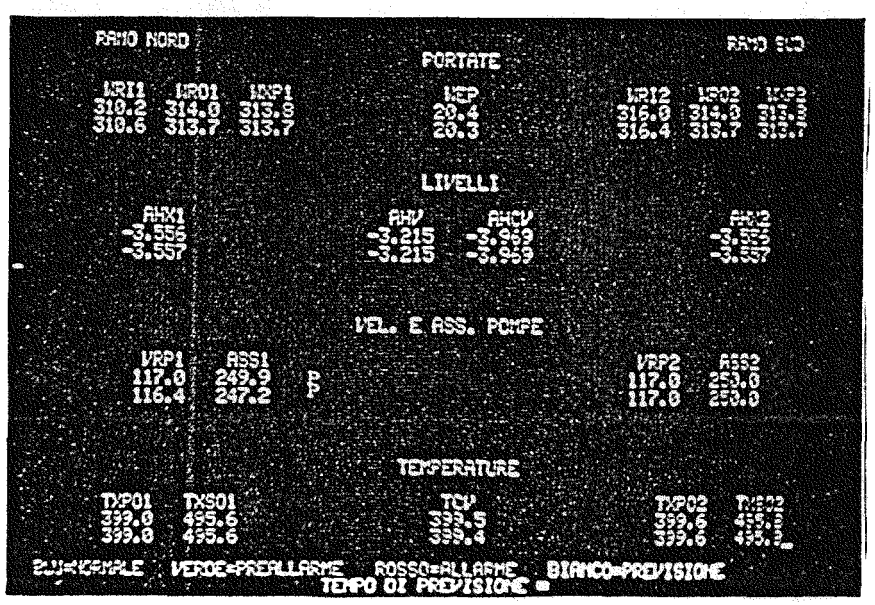
Fig. 7



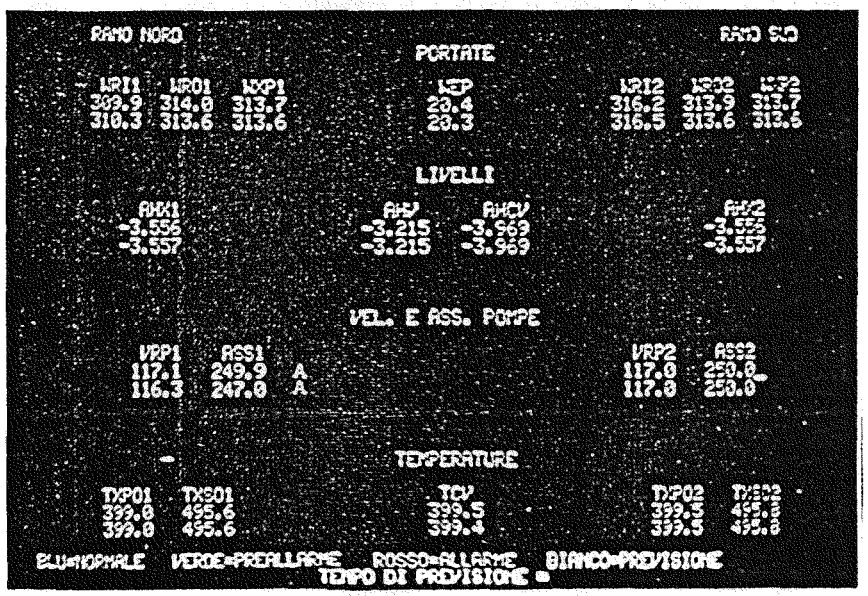
Pict. 1



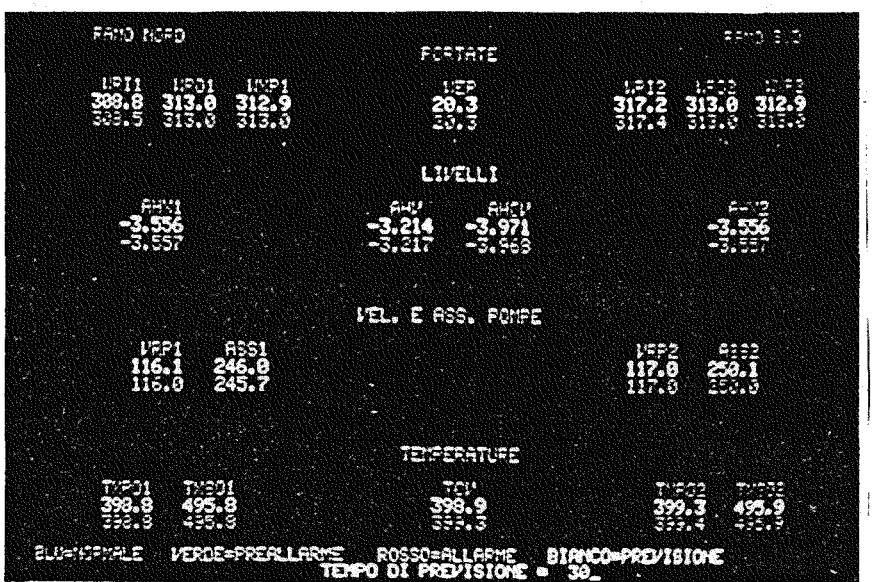
Pict. 2



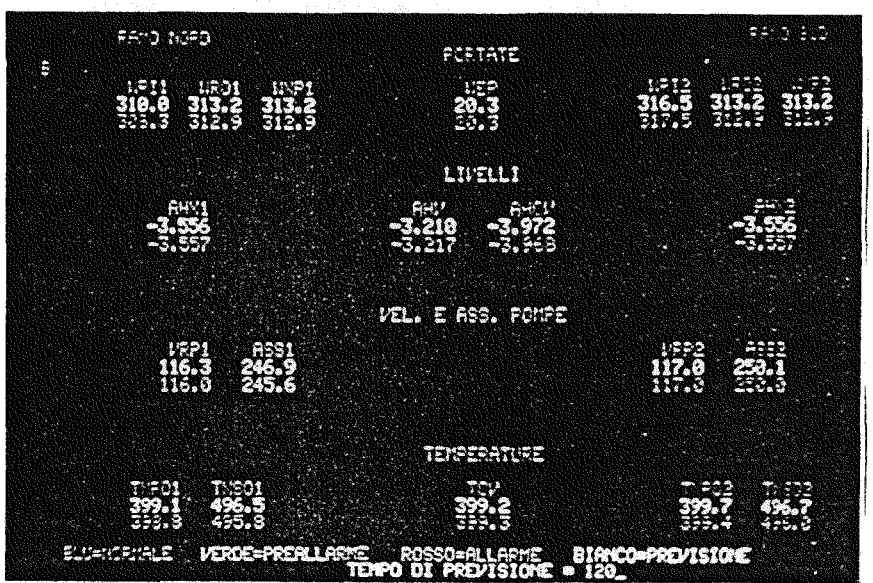
Pict. 3



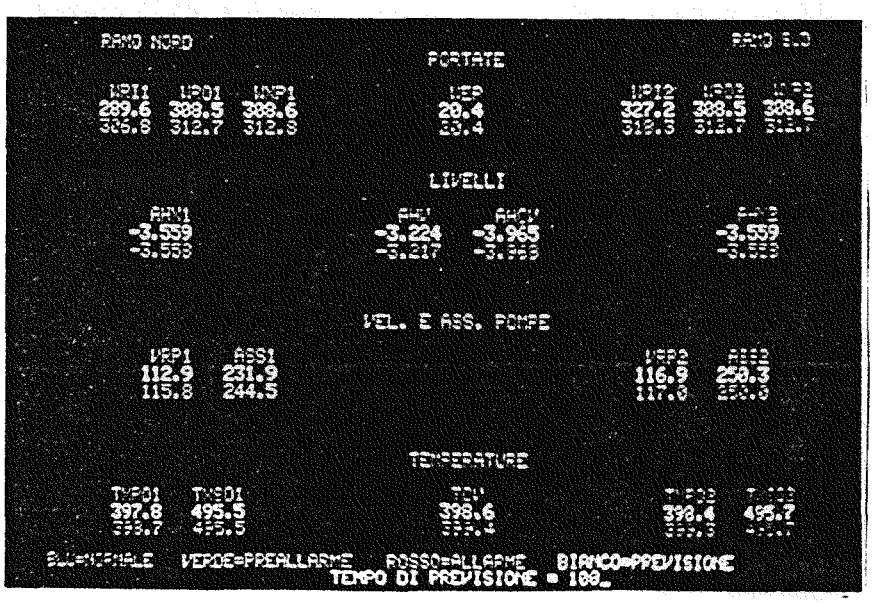
Pict. 4



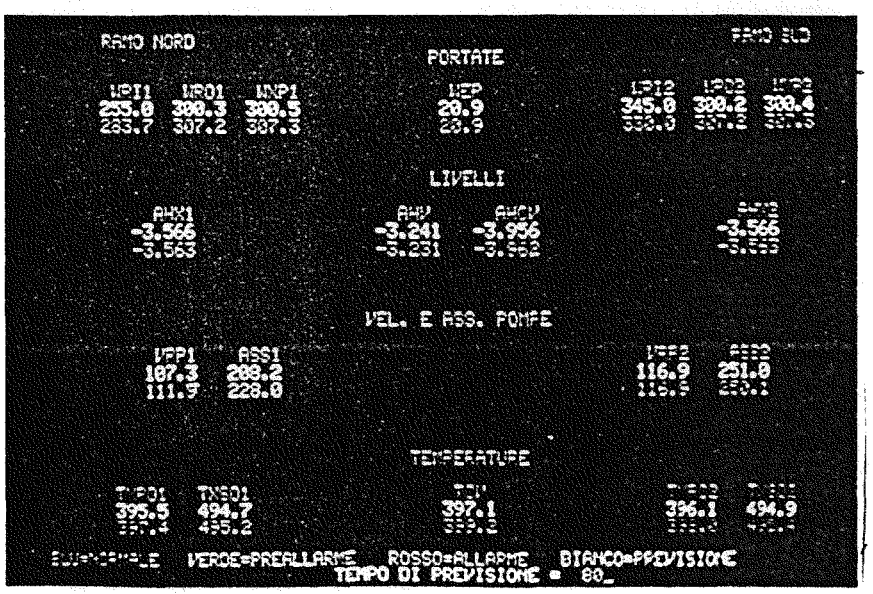
Pict. 5



Pict. 6



Pict. 7



Pict. 8