INTERNATIONAL ATOMIC ENERGY AGENCY

WORKING GROUP ON NUCLEAR POWER PLANT CONTROL
AND INSTRUMENTATION

SPECIALISTS' MEETING ON THE USE OF
DIGITAL COMPUTING DEVICES IN
SYSTEM IMPORTANT TO SAFETY

SACLAY, FRANCE, 28-30 NOVEMBER, 1984

COMPRESS - A COMPUTERIZED REACTOR SAFETY SYSTEM

BY
E. VEGH

CENTRAL RESEARCH INSTITUTE FOR PHYSICS
BUDAPEST, HUNGARY

224

Introduction

Reactor safety equipments have traditional structures and their design is quite conservative. However, the computer technique in this field also begins to break in because this technique offers several advantages as:

- very compact construction,
- easy change of the logic,
- simple realization of different self-testing methods,
- extreme high reliability,
- event logging after shut-down.

Due to the above reasons microprocessor based reactor protection systems have been developed in different countries [1,2,3 4,5] . In the Central Research Institute for Physics, Budapest several safety systems were developed for different reactors and critical assemblies in the last 20 years [6] , and last year the development of a microprocessor based reactor protection system called COMPRESS / COMPuterized REactor Safety System/ started. It is planned to be used after the reconstruction of the 5 MW research reactor of the Institute. This summer COMPRESS-1, the first version of the system, begun to operate parallel to the actively operating hardwired protection system in open-loop. The paper describes the structure of this protection system.

Basic requirements

Since COMPRESS is a reactor protection system its main function is to break the current of the safety rod magnets when a safety violation is detected. Moreover, it provides three additional services as follows:

- safety interlocking,
- signalization in the control room,
- event recording after shut-down.

Safety interlocking means that COMPRESS inhibits the rod movement until the proper conditions are not met. For this reason relatively large amount of digital data are measured /state of different safety amplifiers, position of isolation chambers, etc./ and displayed in the control room as signalization.

After a scram different safety limits are violated and it is sometimes difficult to determine the primary cause of the operation of the reactor protection system. Since the primary cause of the scram is very important, so the recording of the events preceding and following the safety operation is also needed. Naturally, the recorded events have to be printed out immediately after the scram.

The main technical characteristics of the COMPRESS system is presented in Table 1.

Number of safety inputs	32
Number of interlocking inputs	56
Number of interlocking outputs	16
Signalization outputs	32
Recorded inputs	64
Time resolution of the recording	10 msec
Type of the protection output	2/3 voter

Table 1.
Main technical characteristics

<u>Block diagram of the system</u>

COMPRESS is basically divided into two parts as

- event recording subsystem
- protection and interlocking subsystem.

The block diagram of the system is presented in Fig.1.

The safety input lines are received by an optoisolator unit which prevents the error propagation from one unit to the others. The safety function is evaluated by three independent

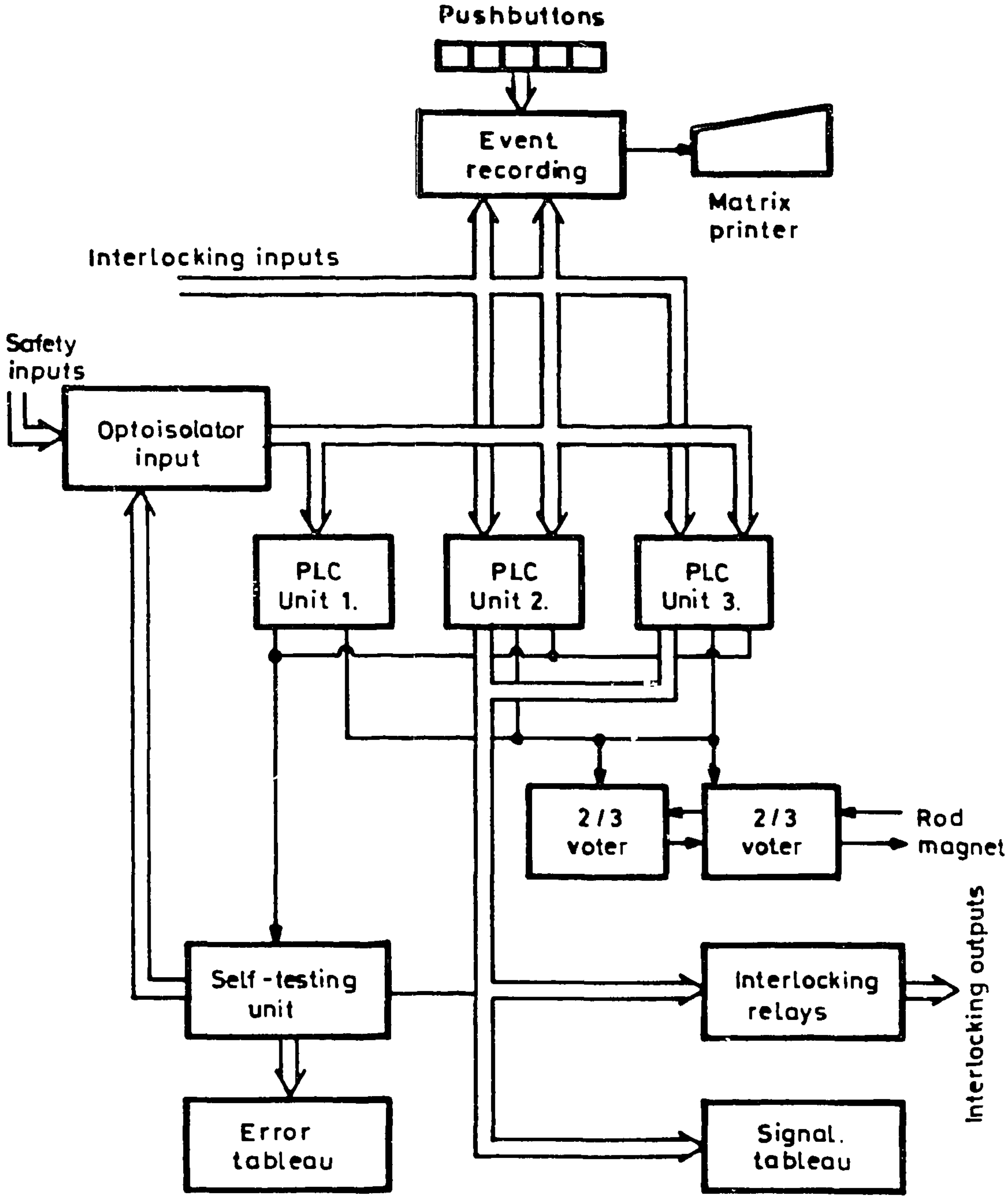

Fig.1. Block diagram of the COMPRESS system

programmed logic controllers /PLC/ whose safety outputs are connected to two 2-out-of-3 voters.
The inputs of the voters are connected parallel but their outputs form a serial circuit thus any of them can break the current of the safety rod magnet if two evaluating PLC units vote for a scram. The voters are automatically modified into 1-out-of-2 logic if any of the three PLC units is inoperating.

The interlocking inputs are connected in parallel to two PLC units which drive the interlocking output relays and the signalization tableau of the system. Again, any of the two units can be switched off without interrupting the operation of the interlocking subsystem.

All of the input lines are scanned by the event recording subsystem, which stores the events /i.e. the change of the input states/ into a cyclic buffer. Event recording continues until one second after a scram, then the content of the cyclic buffer is frozen and it can be printed out by a matrix printer. The printing is initiated by pushbuttons, and it can be repeated at any time.

The system contains an independent self-testing unit as well, which periodically checks the correct operation of the three PLC units and it switches off a PLC unit if it does not operate properly. The self-testing operates only when all of the three evaluating PLC units are switched on. This unit also checks the correct work of the 2/3 voter and the self-testing unit interrupts the current of the rod magnet, if the voter fails.

Operation

Since the reactor protection in this system is done by digital computers and their operation is basically sequential thus the used computers must be fast enough. The PLC units scan their inputs and evaluate the safety function and the interlocking relations every 3 milliseconds. The Boolean-algebraic relations of the PLC units are stored in 1 Kbyte large EPROM memories. These memories can be reprogrammed if a new logical relationship is needed. At present only 1/4 of the available memory is used. The cycle time of the PLC units does not depend on the content of their memories, thus it will not be modified until 1 Kbyte is enough.

The correct operation of the evaluating PLC units is tested by the fourth PLC : this is the self-testing unit. This unit generates a test pattern for one of the three evaluating PLC units. Because one safety signal can not propagate through the 2/3 voter, this testing does not affect the rod magnet. The self-testing unit checks whether the safety signal appears at the output of the tested PLC unit, if not, the PLC unit is regarded as wrong and it is switched off, moreover an alarm signal is generated on the error indicator. The cycle time of the self-testing is 500 msec, and length of the test pulse is about 30 msec.

The operation of the event recording is slower than that of the safety function evaluation, because this is a much more complicated program. The event recorder microprocessor scans the inputs every 10 msec. In each scanning period the present state is compared to the previous one, and if it is different, the new state with the actual time is stored in a cyclic buffer. In this buffer the oldest event is overwritten with the new event. The capacity of the buffer is about 300 items. When a scram is initiated, the content of the event buffer is printed out in the form of simple Hungarian sentences. The event log printing can be initiated at any time by the operator as well.

Construction

In the COMPRESS system normal serial production computers are used: the event recording is carried out by a Z-80 based process control terminal, the Boolean-algebraic relations are evaluated by programmed logic controllers.These equipments are severly tested before being built into the system. The optoisolator unit and 2/3 voter are realized on Eurocard-size modules and they are mounted in one rack. The whole system forms a 2 m high cabinet. The lay-out of the COMPRESS system is presented in Fig.2. At the top of the cabinet the signalization tableau and some pushbuttons of the event recording subsystem are located. The event recording microcomputer and the programmed logic controllers are also built into standardized 19" high racks and every input/output signal is displayed on the front panel by LED indicators. There are two power supply units at the bottom of the cabinet. The whole system operates with a single +24V voltage and only one power supply unit is enough to maintain the operation.

Present state and further development

The first COMPRESS system was completed this summer and it was connected parallel to the operating safety system of the 5MW research reactor of our Institute. Each input line of the COMPRESS system is isolated from the corresponding input of the old one. The system operates at present in open loop, i.e. it does not initiate a scram. During a year this system is planned to operate parallel with the old hardwired protection system; its operation is registered and compared to the operating equipment. In this experimental year the second version is to be developed in which the experiences gained during the operation of the first version will be built . The photo of the first COMPRESS versior is presented in Fig.3.

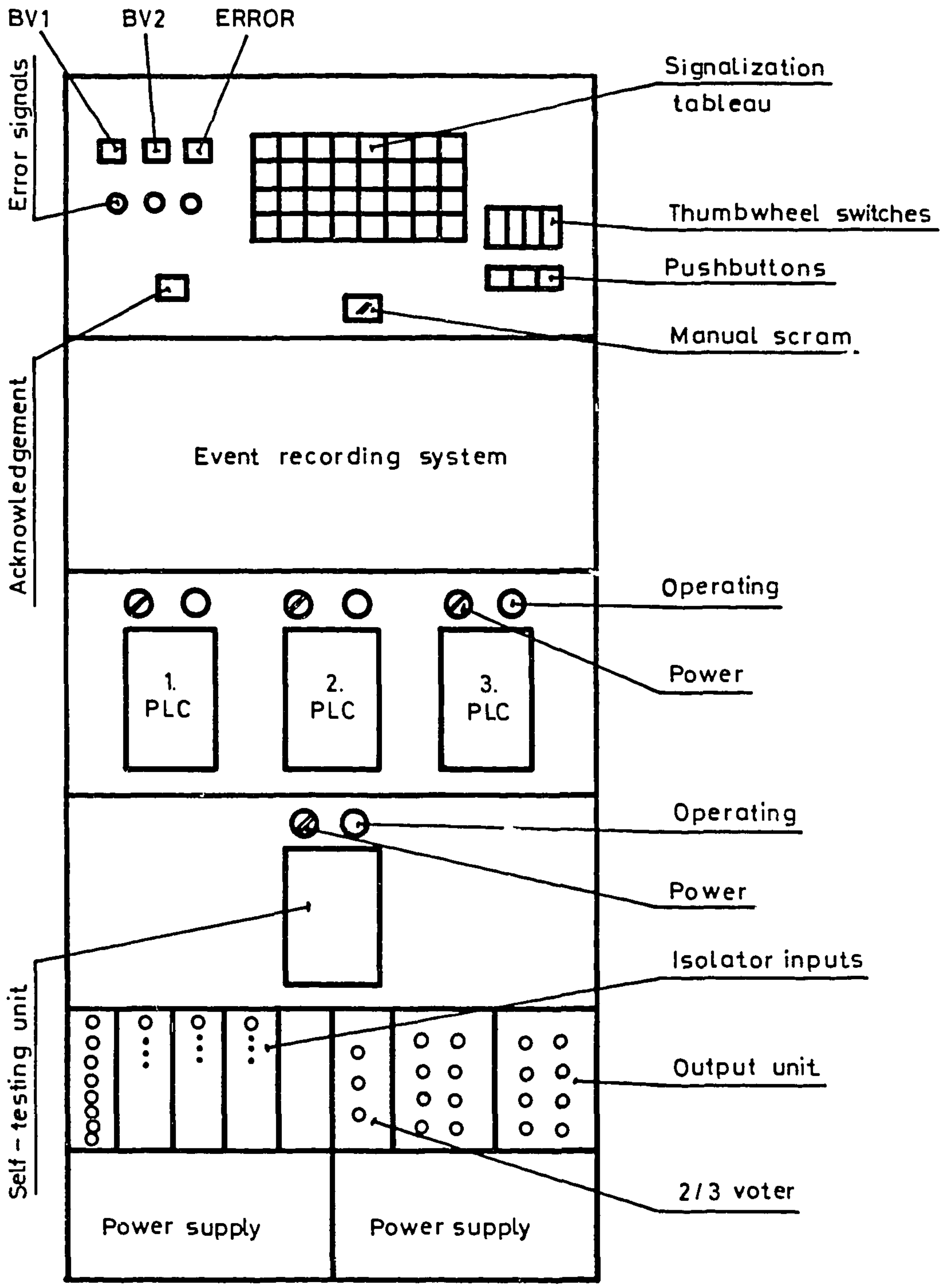

Fig.2. Lay-out of the COMPkESS system

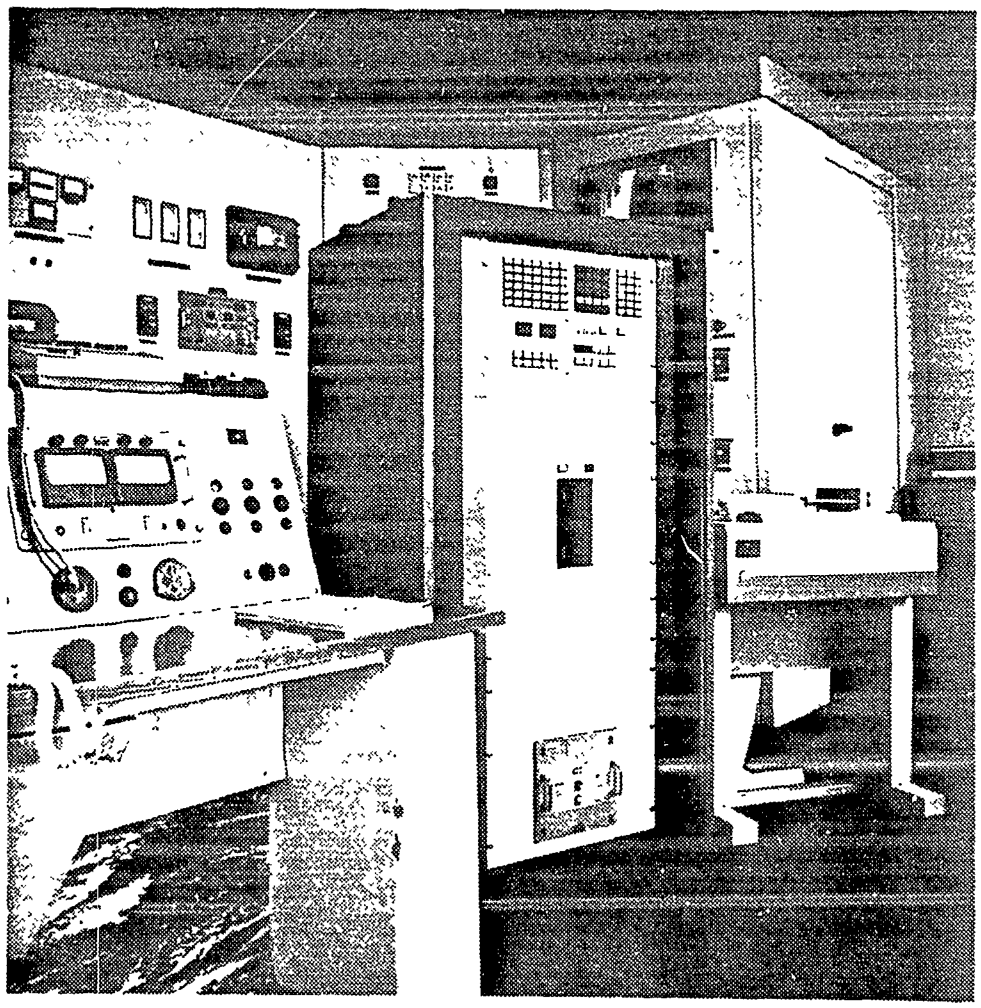

Fig.3. Photo of COMPRESS-1.

References

[1] J.M. Gallagher and G.M.Lilly: System Architecture for Microprocessor Based Protection System. IAEA Specialists' Meeting on Use of Computers for Protection Systems and Automatic Control. Munich, FRG, 11-13 May, 1976.

[2] A.B. Keats: A Fail-safe Computer Based Reactor Protection System. IAEA Specialists'Meeting on Use of Computers for Protection Systems and Automatic Control. Munich, FRG, 11-13 May, 1976.

[3] E.O. Moeack, A.J. Stirling, G.Yan: Research and Development in Control, Instrumentation, and Electronic Systems in CRNL Report AECL-7076.October, 198o

[4] K. Ishibashi, T, Ueda, A.Baba, M. Okano, H. Fukuda: Automatic Test Equipment of Protection System for Pressurized Water Nuclear Power Generating Station. IAEA Symposium in Nuclear Power Plant Control and Instrumentation. Munich, FRG, 11-15 October, 1982.

[5] H. Roggenbauer: Methods and Techniques Used in Computerized Operator Support Systems for German NPPs. IAEA Specialists' Meeting on Systems and Methods for Aiding Nuclear Power Plant Operators During Normal and Abnormal Conditions. Balatonaliga, Hungary, 4-6 Oct., 1983.

[6] E. Zobor: Design for Reliability of the Two-out-of-three Protective Systems with Automatic Testing and Repair. IAEA Symposium on Nuclear Power Plant Control and Instrumentation.
Prague, Czechoslovakia, January, 1973.