

KFKI-1981-28

Z. SZABÓ

PROBABILISTIC RISK ASSESSMENT
OF A PRESSURIZED,
PARTIAL-WATER-HEIGHT CRITICAL ASSEMBLY

Hungarian Academy of Sciences

CENTRAL
RESEARCH
INSTITUTE FOR
PHYSICS

BUDAPEST

PROBABILISTIC RISK ASSESSMENT OF A PRESSURIZED,
PARTIAL-WATER-HEIGHT CRITICAL ASSEMBLY

Z. Szabó

Central Research Institute for Physics
H-1525 Budapest 114, P.O.B.49, Hungary

ABSTRACT

Risk assessment is made on the basis of a system of emergency situations /ES/. An ES is the combination of a mode of operation /MOP/ and an initiating event /INE/. The wide range of operating parameters /temperatures up to 130°C, pressures up to 3 bar/ and the unique construction /regulation of the reactor by changing the water height under pressure/ necessitated the consideration of different MOP's. A total of 16 MOP's and 24 INE's is considered. The transients triggered by the ES's are analysed making use of cause-consequence charts. Risk is expressed in terms of reactivity addition rates and the corresponding probabilities.

АННОТАЦИЯ

Риск оценивается на основе системы исходных состояний /ИС/. ИС - это комбинация режима эксплуатации и события, которое может привести к аварии. Учетывание ИС объясняется широким диапазоном эксплуатационных параметров /температура до 130°C, давление до 3-х бар/ и уникальной конструкцией /регулировка доливом замедлителя под давлением/. Всего учтено 16 режимов эксплуатации и 24 события. Переходные процессы, возникающие за счет ИС, исследованы при помощи диаграмм причина-следствие. Риск выражается скоростью увеличения реактивности и соответствующей вероятностью.

KIVONAT

A kockázatbecslés a kiinduló állapotok rendszere alapján történik. Kiinduló állapotnak egy üzemmód és egy kiváltó esemény kombinációját tekinti a tanulmány. Ezt a tárgyalásmódot az üzemi paraméterek széles tartománya /hőmérséklet 130°C-ig, nyomás 3 bar-ig/, valamint a szokatlan konstrukciós megoldás /nyomottvízes, vízszintszabályozásu rendszer/ indokolja. A vizsgálat összesen 16 kiinduló állapotra és 24 kiváltó eseményre terjed ki. A kiinduló állapotok által beindított átmeneti folyamatokat ok-okozati sémákkal követik. A kockázatot reaktivitás-változási sebességek és az azoknak megfelelő valószínűségek fejezik ki.

TABLE OF CONTENTS

	<u>Page</u>
1. INTRODUCTION	1
2. METHODOLOGY	2
2.1 Modes of operation.	2
2.2 Initiating events	5
2.3 Emergency situations.	6
2.4 Transients.	10
2.4.1 Cause-consequence charts	10
2.4.2 Reliability data	10
2.4.3 Human factor	10
2.4.4 Emergency situations	10
2.4.5 Failure of the reactor protection system	11
3. SAMPLE CCC	13
4. RESULTS.	15
5. SUMMARY.	17
6. ACKNOWLEDGMENTS.	17
7. REFERENCES	18
APPENDIX 1. ZR-6M critical assembly	19
1.1 General description.	19
1.2 Reactor protection system.	19
APPENDIX 2. CCC Symbols, notations, abbreviations	23

1. INTRODUCTION

The ZR-6 critical assembly was built for reactor-physical measurements in WWER-type lattices. It serves as the experimental basis of a Temporary Research Collective of the CMEA countries. The assembly went critical in 1972 and operated until 1977 at atmospheric pressure. Then it was reconstructed to work at temperatures up to 130°C /ZR-6M/. The assembly is controlled by adjusting the water-height /a unique feature at elevated pressure!/ thus providing the possibility of measurements in cores unperturbed by absorbers. The reader is referred to Appendix 1 for a short description of the facility.

Versatility and accessibility - the most important features of critical assemblies in general - are at the same time the source of increased risk of nuclear accidents. With this in mind, special attention has been paid to nuclear safety problems since the very beginning of the operation of ZR-6. The reconstruction, however, necessitated the quantitative evaluation of risks - because of the unique construction and the wide range of operating parameters /critical water level, temperature, boron concentration, etc./ of the assembly.

The growing need for nuclear power and public concern about its environmental impacts were the main incentives that led to the development of probabilistic risk assessment techniques. During the last decade a large number of papers have appeared in this field. However, few complete risk assessments are known for nuclear power plants [1-3]. To our knowledge, no such analysis has been made for a critical assembly.

Risk is usually defined [1] as

$$\text{Risk} \left\{ \frac{\text{consequence}}{\text{unit time}} \right\} = \text{Frequency} \left\{ \frac{\text{events}}{\text{unit time}} \right\} \times \text{Magnitude} \left\{ \frac{\text{consequence}}{\text{event}} \right\}$$

The relative frequency or probability of events is calculated from the failure probability of individual components on the basis of logical diagrams i.e. fault trees and event trees. Accident consequences are usually expressed in terms of numbers of fatalities or damage to property. The cause-conse-

quence charts method, a further development of fault-tree and event-tree analysis, is a very convenient tool for safety evaluation.

2. METHODOLOGY

Figure 1 presents the flow chart of the work done in this study.

The reactor is supposed as being in a certain mode of operation /e.g. operation at 130°C, control rods raised, fast drain valves closed, etc./. At this moment, an abnormal event /e.g. rupture of a tube under pressure/ takes place; it is considered an initiating event. The mode of operation and initiating event together define the emergency situation which, in its turn, determines the nature of transients /in our case: depressurization, emergency shutdown by safety rods and fast drain valves, boiling of the moderator, etc./. At the end, a safe final state is reached /reactor shut down, over-pressure equals zero, etc./.

In some cases, a failure of the reactor protection system prevents it from bringing the reactor to a safe final state in which case the reactor will undergo physical transients which can be characterized by the reactivity addition rate, $\partial\rho/\partial t$. The consequences of physical transients are not treated in this work. Risk is expressed in terms of $\partial\rho/\partial t$ and the corresponding probabilities. For the sake of comparison, the probabilities of some non-nuclear events /e.g. earthquake, airplane crash/ are evaluated as well.

2.1 Modes of operation

The modes of operation are defined by the following six data /see *Fig.2*/:

	Code	
Core shut down by absorbers?	yes : 0	no : 1
PV* lid closed?	no : 0	yes : 1
PV drain valve closed?	no : 0	yes : 1
CT fast drain valves closed?	no : 0	yes : 1
Safety rods raised?	no : 0	yes : 1
Moderator temperature greater than 100°C?	no : 0	yes : 1

*See Appendix 1.

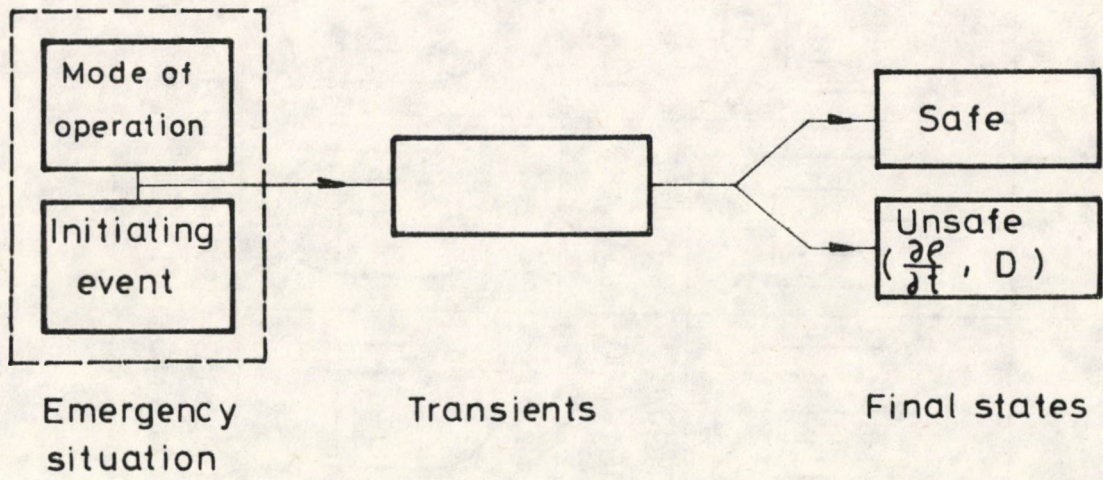
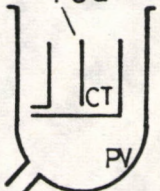
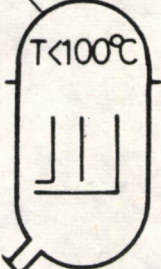



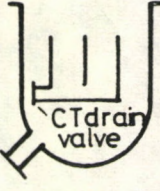





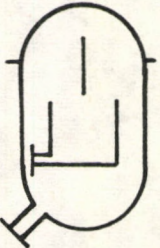






Fig 1. Flow chart of the study

Fig. 2. Modes of operation

							
Core shut down 000-000	Core shut down 011-000	T < 100°C 100-000	T < 100°C 101-000	T < 100°C 101-010	T < 100°C 101-100	T < 100°C 101-110	T < 100°C 110-000
							
T < 100°C 111-000	T < 100°C 111-010	T < 100°C 111-100	T < 100°C 111-110	T > 100°C 111-001	T > 100°C 111-011	T > 100°C 111-101	T > 100°C 111-111

For example, 000-000 means that the reactor is out of operation with the core shut down, PV lid and valve open, etc.

111-111 means that the reactor is operating under pressure with safety rods raised, CT fast drain valves closed, etc. In view of the fact that some of the possible variations of the above six data have no physical sense /e.g. moderator temperature cannot exceed 100°C if the PV lid is open/, a total of 16 modes of operation is considered.

2.2 Initiating events

Critical water heights are a function of core configuration and may go down as low as 27 cm. The active length of the fuel elements being 125 cm, it is at times practically impossible to shut down the reactor - with safety rods or extra absorbers - should there be an accidental inundation of the core. Therefore, all events that can lead - in spite of protective measures - to an uncontrolled water level rise in the core /e.g. uncontrolled pump operation, etc./ are considered initiating events.

A special case of uncontrolled level rise is that caused by bubble formation due to boiling of the water when the system is depressurized /e.g. rupture of a tube under pressure/. Special experiments were made to prove that the reactivity effect of depressurization is negative - in spite of level rise - because bubble formation decreases the moderator density in the core.

The 24 initiating events considered in this study are the following /see Fig. 3/:

- a/ Water flow from above into the space between PV and CT due to the rupture of a conduit.
- b/ Water flow into PV due to the rupture of the cooling pipe-coil.
- c/ Water flow into PV through the open drain valve due to the rupture of a conduit in the shaft containing technological equipment.
- d/ Water flow from above into CT due to the rupture of a conduit.
- e/ Flooding of a pipe containing a detector in the reflector due to its rupture.
- f/ Overfilling of PV due to the failure of the timer switch to stop the pump and to operator inadvertance.
- g/ Overfilling of CT due to similar reasons.
- h/ Filling of CT with water containing less boric acid than prescribed, in the extreme case with distilled water, due to the failure of a valve or operator error.
- i/ Overheating ΔT of water in PV due to the failure of the temperature controller or erroneous setting thereof.

- j/ Depressurization Δp of PV due to the rupture of a pipe of maximum diameter, joining the steam space of PV.
- k/ Fast level rise in CT due to an object falling into the space between PV and CT.
- l/ Fast level rise in CT due to an object falling into it.
- m/ Displacement of PV due to buoyancy caused by the flooding of the reactor shaft.
- n/ Displacement of CT due to buoyancy caused by the flooding of the space between PV and CT.
- o/ Suction of water from the storage tank due to vacuum in PV caused by erroneous valve-settings during the cooling-down procedure.
- p/ Fast removal of an absorber from the core due to operator error or water-boiling.
- q/ Simultaneous lifting of two groups of safety rods due to the failure of the interlock system, and to operator inadvertence.
- r/ Falling of 3 fuel rods, raised along with a deformed safety rod, back into the core.
- s/ Rupture of PV due to pressure.
- t/ Airplane crash.
- u/ Earthquake.
- v/ Sabotage.
- w/ Loss of power or water supply.
- x/ Cable fire.

2.3 Emergency situations

Emergency situations are a combination of modes of operation and initiating events /Table 1/. Blank spaces indicate combinations without physical sense, e.g. no depressurization can take place if the PV lid is open. A total of 60 emergency situations are considered. In addition, some initiating events are treated without respect to modes of operation /e.g. airplane crash/.

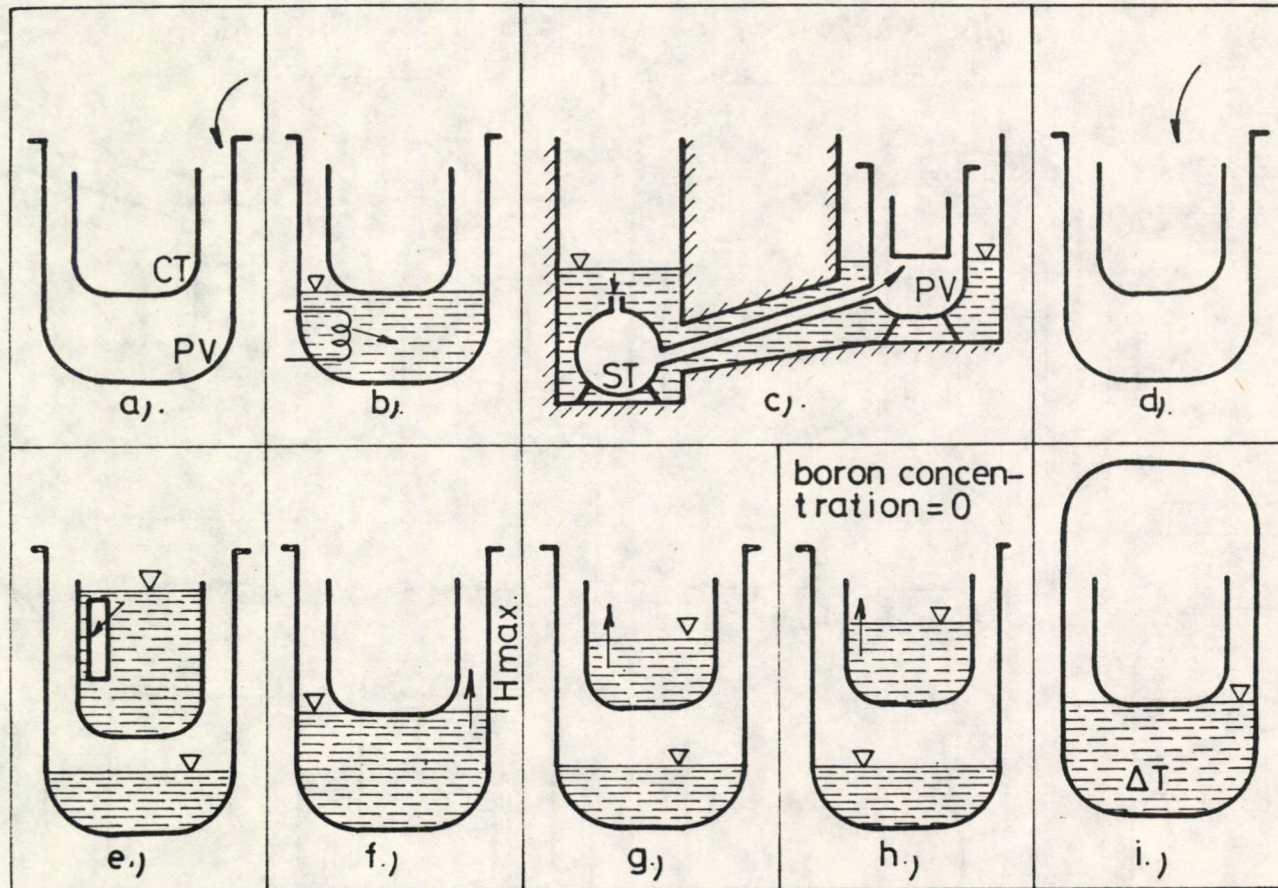
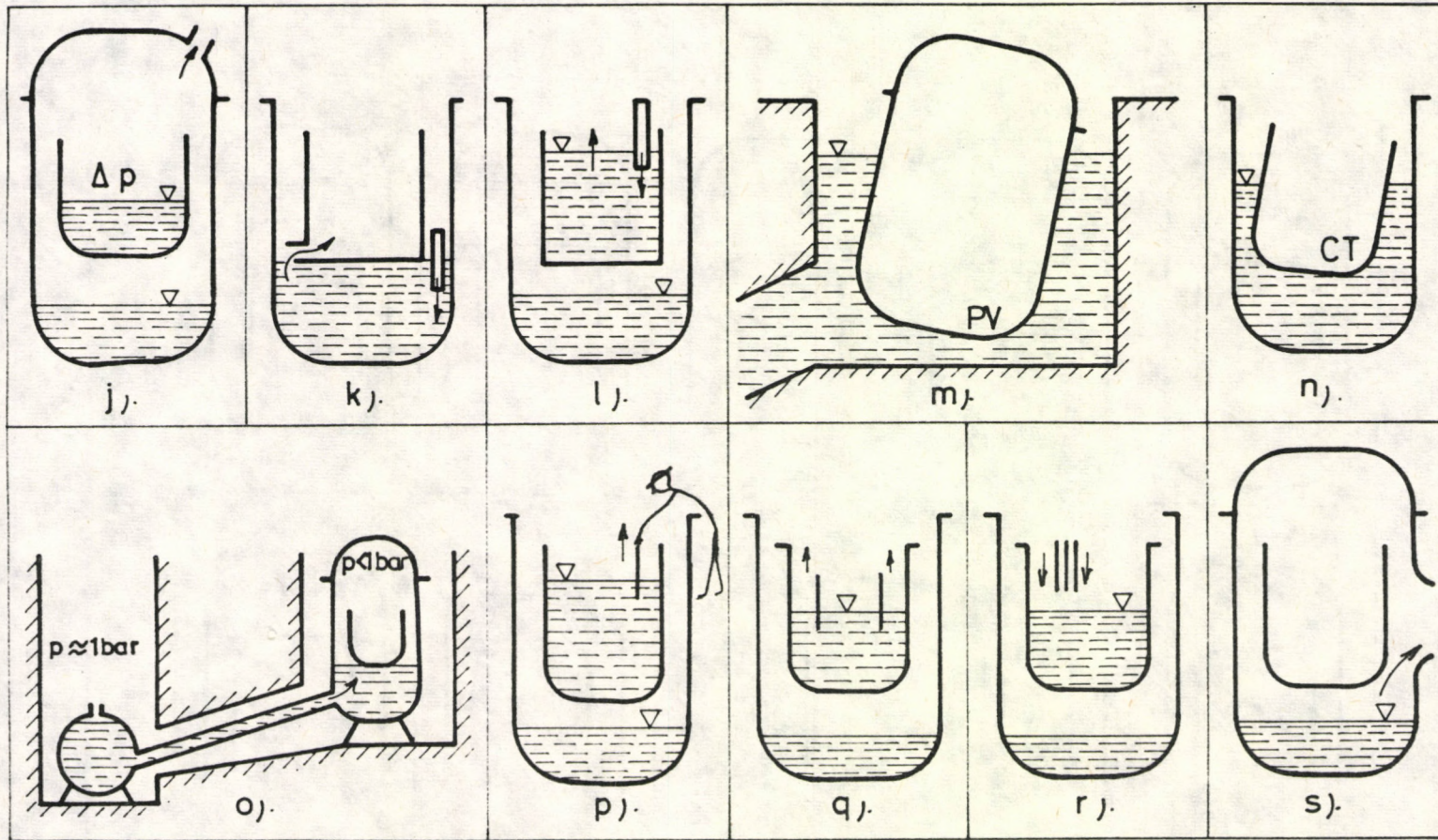


Fig 3A. Initiating events.



Events t) to x) are not depicted in this figure.

Fig 3B. Initiating events.

shutdown PV lid	PV drain v.	CT drain v.	Safety rods T > 100°C	Water into PV			Water into CT		Overfilling of			Boiling due to		Object falling		Buoyancy of		Vacuum	Absorber	6 safe-tyrods ↑	3 fuel rods ↓
				from above cooling pipe	shaft		from above detector pipe		PV	CT	CT with dist. w.	ΔT	Δp	into PV	into CT	PV	CT				
				a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
0 0 0 - 0 0 0																					
0 1 1 - 0 0 0																					
1 0 0 - 0 0 0				a/1		c/1	d/1														
1 0 1 - 0 0 0				a/2			d/1							k/1		m/1					
1 0 1 - 0 1 0				a/3			d/1		f/1					k/1							
1 0 1 - 1 0 0				a/4			d/2					i/1		k/2	l/1		n/1			q/1	
1 0 1 - 1 1 0				a/5			d/3	e/1		g/1	h/1			k/2	l/1		n/1		p/1		r/1
1 1 0 - 0 0 0					b/1	c/1															
1 1 1 - 0 0 0					b/2											m/1		o/1			
1 1 1 - 0 1 0					b/3				f/1												
1 1 1 - 1 0 0					b/4							i/1					n/1			q/1	
1 1 1 - 1 1 0					b/5			e/1		g/1	h/1	i/1					n/1				r/1
1 1 1 - 0 0 1					b/6																
1 1 1 - 0 1 1					b/7																
1 1 1 - 1 0 1					b/8							i/2	j/1							q/1	
1 1 1 - 1 1 1					b/9			e/2		g/1	h/1	i/2	j/2						p/2		r/1

Table 4. Emergency situations.

2.4 Transients

2.4.1 Cause-consequence charts

Cause-consequence charts /CCC's/ are used for analysing the transients. CCC's are a unique blend of fault trees and event trees and they permit one to get a clear, detailed picture of the sequence of events during a transient [4]. It is also possible by their help to evaluate risks - reactivity changes and their respective probabilities. A sample CCC that follows later will give the reader an idea about this technique.

A CCC is constructed for each of the emergency situations considered. The probability of an unsafe final state is evaluated making use of the probability of the emergency situation and of the failure of the reactor protection system.

2.4.2 Reliability data

No reliability data are available for components and instruments used in ZR-6M. Failure rates are therefore taken from the literature [5-8] and are modified /increased by a factor 3 to 10/ to account for the fact that the components they refer to were made to meet higher quality standards. For example, the failure rate of a time switch according to [8] equals 10^{-3}h^{-1} , in the present work it was supposed as being $3 \times 10^{-3} \text{h}^{-1}$.

The experience of five years' operation of ZR-6 before the reconstruction was taken into consideration as well.

2.4.3 Human factor

The safety of the reactor depends to a great extent on the skilled and disciplined work of the staff. It is therefore necessary to consider the consequences of human error when constructing CCC's. For the quantitative evaluation of CCC's human error probabilities were taken from [9]. Thus e.g. the probability that the operator does not stop the pump filling PV, should the time switch fail, was taken to be $Q_{\text{op4}} = 3 \times 10^{-2} \text{d}^{-1}$ /per demand/. Likewise, $Q_{\text{op2}} = 3 \times 10^{-3} \text{d}^{-1}$ is the probability that the operator does not respond to acoustic scram signals.

2.4.4 Emergency situations

The probability of an emergency situation is obtained in general by multiplying the fault exposure time /hours per week/ by the failure rate /hours⁻¹/ which corresponds to the initiating event. In some cases, however,

several probabilities /technical failure, human error, natural catastrophe, etc./ have to be combined. E.g. in the case of emergency situation f/1: fault exposure time is calculated from the frequency of the two modes of operation which are considered together: $t_{fe} = 2.2 \text{ h}$. The unavailability /failure probability/ of the time switch

$$Q_{ts} = \lambda_{ts} \quad t_{fe} = 3 \times 10^{-3} \text{ h}^{-1} \times 2.2 \text{ h} = 6.6 \times 10^{-3}$$

where λ_{ts} is the failure rate. This has to be multiplied by Q_{op4} /see 2.4.3/ to obtain the probability of emergency situation f/1:

$$Q_{f1} = Q_{op4} \quad Q_{ts} = 3 \times 10^{-2} \times 6.6 \times 10^{-3} = 2 \times 10^{-4}$$

2.4.5 Failure of the reactor protection system

The reactor protection system /RPS/ has to perform a certain safety function if a parameter exceeds a trip limit /see Fig. 8/. The RPS fails if the required safety function is not performed. Failure probability /unavailability/ of RPS refers to a certain parameter and to a certain safety function. E.g. Q_{NR} is the probability that if the neutron flux exceeds 100%, there is no emergency shutdown by safety rods.

Failure of RPS is due in this case to the failure of one or more of the following 3 subsystems: neutron channels / Q_N /; central logic unit / Q_L /; safety rods / Q_R /: $Q_{NR} = Q_N + Q_L + Q_R$ /small-probability approximation/.

The 6 neutron channels form a parallel system, any one of them is capable of producing a trip signal. $Q_N = Q_{N1}^6$ where Q_{N1} is the unavailability of one channel. A detailed reliability analysis of the RPS was not aimed at; the units are considered as a whole and their failure rates are taken from the sources mentioned above /2.4.2/.

A conservative estimate for the unavailability of one channel

$$Q_{N1} = \lambda_{N1} t_m$$

where $\lambda_D = 10^{-3} \text{ h}^{-1}$ /failure rate of a detector/

$\lambda_A = 10^{-3} \text{ h}^{-1}$ /failure rate of an amplifier/

$\lambda_{N1} = \lambda_D + \lambda_A = 2 \times 10^{-3} \text{ h}^{-1}$ /failure rate of a neutron channel/

$t_m = 10 \text{ h}$ proof test interval of the neutron channels
/time between two periodic checks/

Thus $Q_{N1} = 2 \times 10^{-2}$ and $Q_N = 0.64 \times 10^{-10}$, the unavailability of the system of neutron channels.

Unsafe failures of the central logic unit cannot remain hidden for longer than a test cycle because if such a failure is discovered the reactor is tripped. For the calculation of the unavailability of the logic unit, let λ_L be the failure rate of the logic unit and λ the rate of failure considered as an initiating event. Failure probabilities during a test cycle τ will be

$$Q_1 = \lambda_L \tau \text{ and } Q_2 = \lambda \tau \text{ respectively.}$$

The logic unit, as a part of the RPS, fails if an initiating event is not followed by the necessary safety action. A conservative estimate for this is $Q_1 Q_2$, the probability that the failure of the logic system and the initiating event take place within the same test cycle.

Let Q_L = unavailability of the logic unit

Q = probability of the initiating event

t_{fe} = fault exposure time / frequency of the corresponding mode of operation/

$$Q_1 Q_2 = \lambda_L \lambda \tau^2 = \lambda_L \frac{\tau^2}{t_{fe}} \lambda t_{fe} = Q_L Q$$

$$Q_L = \lambda_L \frac{\tau^2}{t_{fe}} = 1.45 \times 10^{-7}$$

with

$$\lambda_L = 3 \times 10^{-3} \text{ h}^{-1}$$

$$\tau = 1.03 \times 10^{-2} \text{ h}$$

$$t_{fe} = 2.2 \text{ h}$$

Two groups of safety rods are sufficient for shutting down the reactor, thus the system of safety rods fails if more than one group of safety rods is in a faulty condition.

The unavailability of the system of safety rods

$Q_R = 3\lambda^2 / 1 - \lambda / + \lambda^3$ taking into account that $\lambda^2 / 1 - \lambda /$ is the probability that two groups of safety rods are in a faulty condition and the third is not; the factor of 3 takes into consideration all possible combinations; λ^3 is the probability that all 3 groups of safety rods fail at the same time.

Substituting $\lambda = 10^{-3} \text{ d}^{-1}$; $Q_R = 3 \times 10^{-6} \text{ d}^{-1}$.

Thus the unavailability of the RPS in this case is

$$Q_{NR} = Q_N + Q_L + Q_R = 0.64 \times 10^{-10} + 1.45 \times 10^{-7} + 3 \times 10^{-6} = 3.2 \times 10^{-6}$$

If water level in PV exceeds a preset value, the required safety action is to stop the pump from filling PV. RPS unavailability in this case is

$$Q_{HP} = Q_H + Q_L + Q_{rel}.$$

where

Q_H = unavailability of two water gauges at the same time

Q_L = unavailability of logic unit

Q_{rel} = failure probability of opening a relay contact.

Substituting the corresponding values

$$Q_{HP} = 9 \times 10^{-6} + 1.45 \times 10^{-7} + 10^{-6} = 10^{-5}$$

Likewise, if the neutron flux exceeds 100%, the pump filling PV has to be stopped. In this case the unavailability is

$$Q_{NP} = Q_N + Q_L + Q_{rel} = 0.64 \times 10^{-10} + 1.45 \times 10^{-7} + 10^{-6} = 1.2 \times 10^{-6}$$

3. SAMPLE CAUSE-CONSEQUENCE CHART

A simple chart, CCC-f/1 is presented as an illustration of the method /Fig. 4/. The initiating event /f/ is the following: when filling PV, a timer switch stops the pump if the operator does not push a button every 100 seconds after an acoustic signal. There is an uncontrolled level rise in PV if the timer switch fails and the operator, due to inadvertance or some other reason, does not stop the pump either. Conditions for the operation of the pump are CT drain valves open, safety rods raised; thus the modes of operation considered here are: 101 - 010 and 111 - 010.

When the water level in PV exceeds the permissible maximum value $H_{PV \max}$ which corresponds to the height of the bottom of CT, the reactor is tripped from the level gauges. If this safety action fails, the operation of the pump continues and - in about 10 minutes - the water level in CT exceeds the critical value H_{cr} and the reactor is tripped from the neutron channels.

At the same time the operator is likely to interfere, if it is considered that the blinking light and acoustic signals of Trips 1 and 2 and the acoustic monitor of the neutron channels inevitably draw his attention to the incident.

To evaluate the risk, the reactivity addition rate and the corresponding probability have to be calculated. Level rise rate $\frac{\partial H}{\partial t} = 1 \text{ mm s}^{-1}$, reactivity worth of level change: $\frac{\partial \rho}{\partial H} = 2 \text{ } \phi \text{ mm}^{-1}$, so the reactivity addition rate is

$$A = \frac{\partial \rho}{\partial t} = \frac{\partial H}{\partial t} \cdot \frac{\partial \rho}{\partial H} = 1 \text{ mm s}^{-1} \cdot 2 \text{ } \phi \text{ mm}^{-1} = 2 \text{ } \phi \text{ s}^{-1}$$

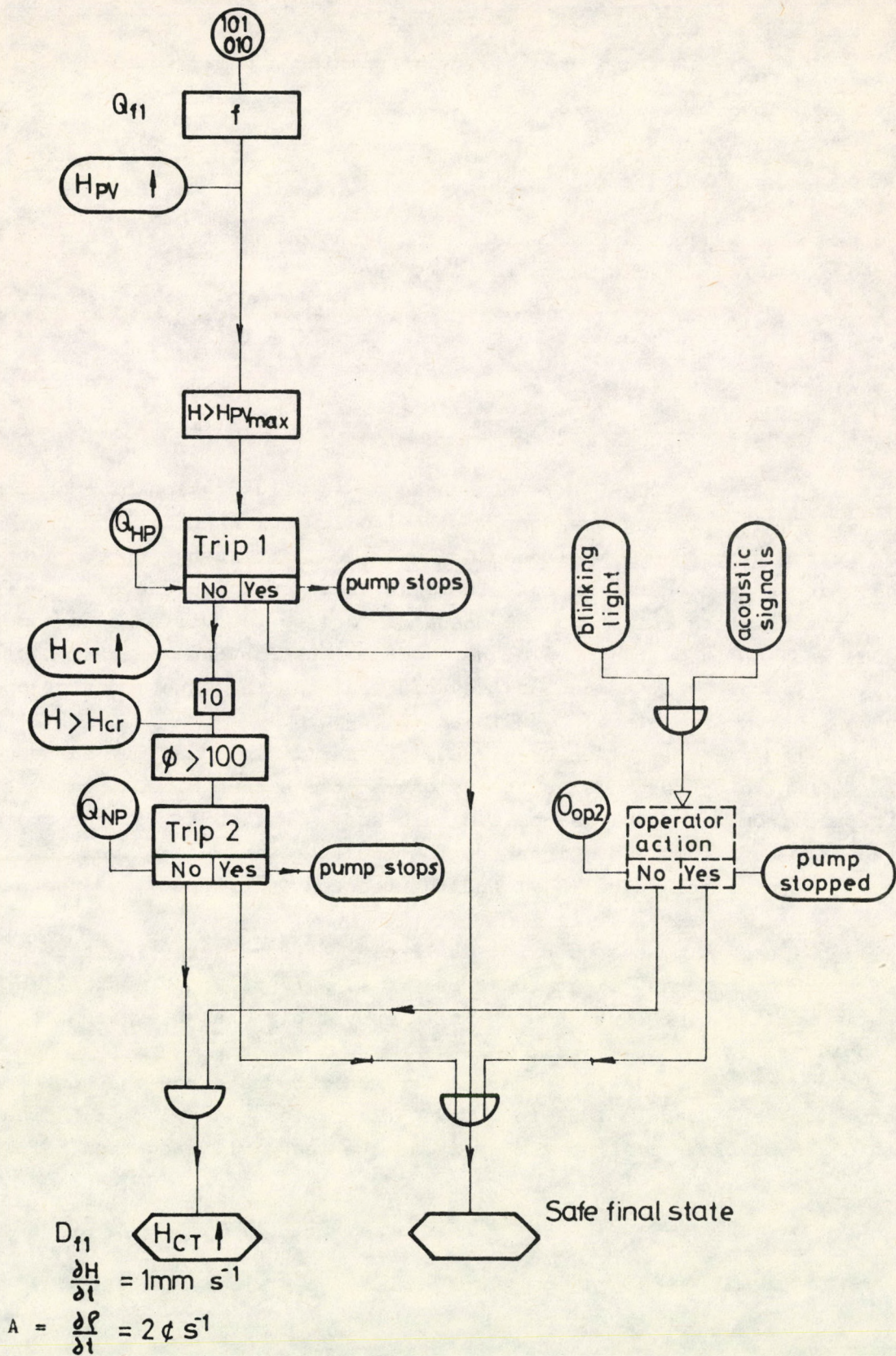


Fig 4. CCC - f/1

The Boolean equation representing CCC f/1 is

$$\begin{aligned} d_{f1} &= q_{f1} q_{HP} q_{NP} q_{Op2} = \\ &= q_{f1} / q_H + q_L + q_{rel} / q_N + q_L + q_{rel} / q_{Op2} = \\ &= q_{f1} / q_H q_N + q_L + q_{rel} / q_{Op2} \end{aligned}$$

where q_{f1} , q_{HP} , etc. are the corresponding Boolean variables of the probabilities Q_{f1} , Q_{HP} , etc.

A rare-event approximation for the probability per week of the unsafe final state is

$$\begin{aligned} D_{f1} &= Q_{f1} / Q_H Q_N + Q_L + Q_{rel} / Q_{Op2} = \\ &= 2 \times 10^{-4} / 9 \times 10^{-6} \times 0.64 \times 10^{-10} + 1.45 \times 10^{-7} + 10^{-6} / 3 \times 10^{-3} = \\ &= 7.10^{-13} \end{aligned}$$

4. RESULTS

In *Fig. 5* the subsumed per year probabilities of the unsafe final states vs reactivity addition rates are plotted. For the sake of comparison, the probabilities of two non-nuclear events /airplane crash and earthquake/ are plotted as well. It is seen in the figure that the probabilities of all nuclear events - with a single exception - are below the 10^{-7} yr^{-1} line and can therefore be considered as highly improbable.

There are two salient points in the figure: Y, representing a rather high probability and Z, a considerable reactivity addition rate. It is worth while to consider these two cases in some detail.

Point Y corresponds to initiating event "D", /see *Fig. 3B*/ . If one wants to do some work inside PV after an operation at 130°C the water has to be cooled down to about 30°C . Operating procedures oblige the operator to vent PV when the temperature goes below 100°C . Should he fail to do so, absolute pressure within PV goes below 1 bar, following the saturation curve. If, in this case, another infringement of the procedures takes place; the drain valve of PV is opened, PV is filled from ST due to the suction of the vacuum inside it. No special protecting device was built in for an incident of this type. There is an administrative limitation to the maximum permissible quantity of water in PV and ST. So the position of point Y is defined by the probability of multiple human failure.

It is very educative to consider point Z too. If water is pumped into PV with the fast drain valves of CT closed, it is possible to fill the space between PV and CT without filling CT /see *Fig. 6A*/ . If, in this case, the reactor is tripped /e.g. by a spurious signal in the RPS or by the operator manually/, the six drain valves open simultaneously and there is a rapid level rise in CT /*Fig. 6B*/ . The reactivity addition rate is great, consider-

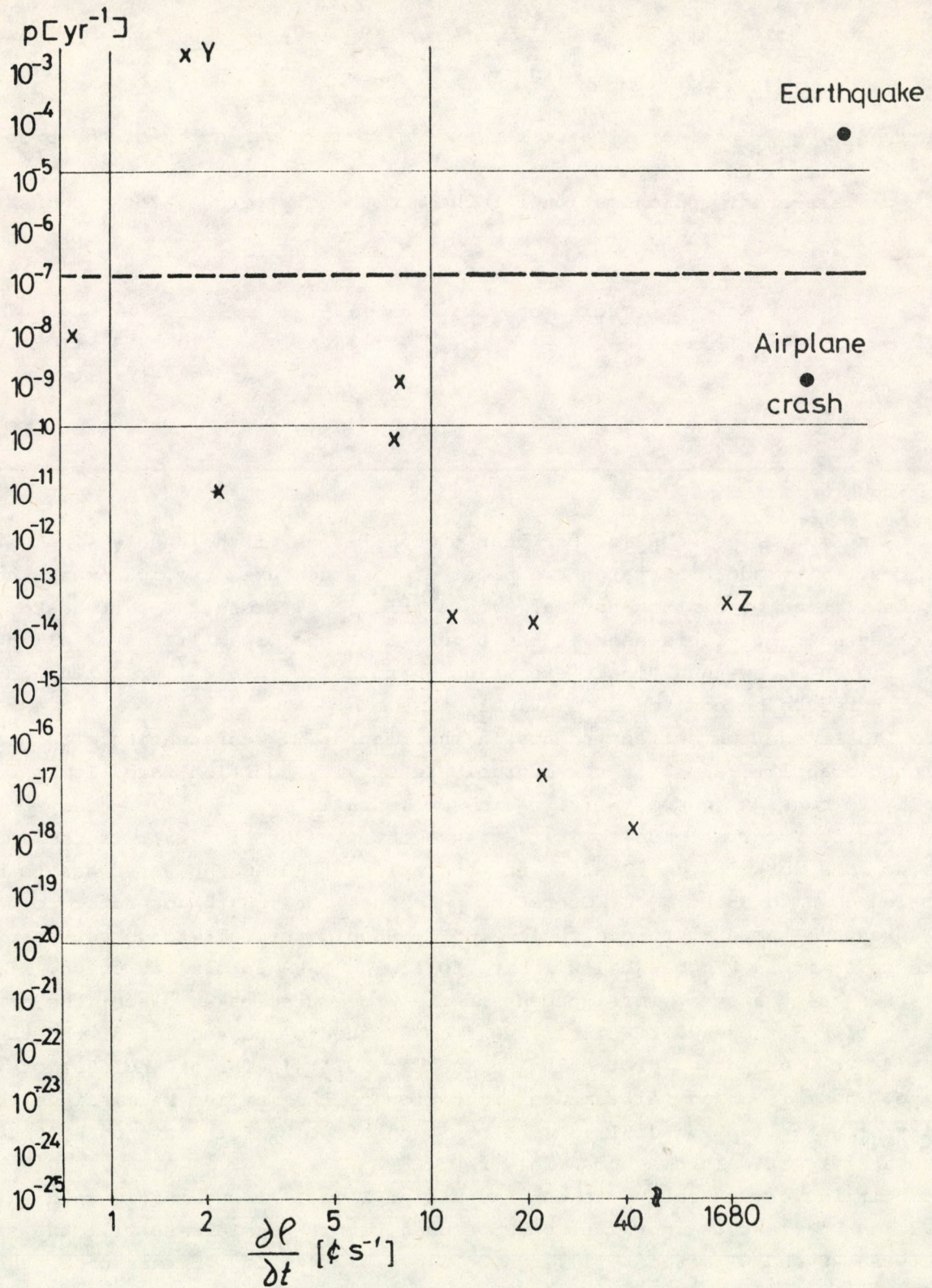


Fig.5 Results

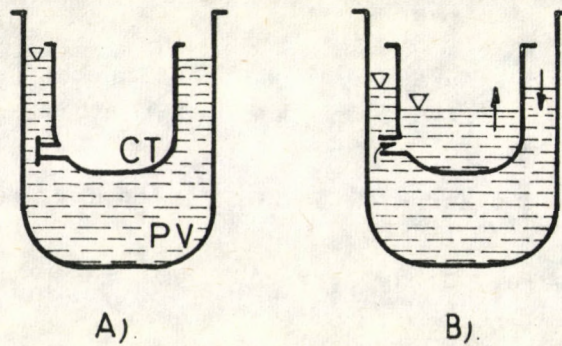


Fig 6. A special fault condition

ing that the drain valves have a diameter of 150 mm each. It is seen that in this way a protective action can, under certain circumstances, be the cause of a bad reactivity initiated accident. The associated small probability value is due to the built-in safety devices /level gauge, etc./.

5. SUMMARY

The method developed for the purpose of this study has the following features:

- it takes into account the fact that an emergency situation is characterized by the initiating event and the mode of operation;
- transients are analysed by the CCC technique which permits one to get a clear picture of the sequence of events.

The method has already proved to be a valuable tool in the design period. It was possible, with its help, to spot relative "weak points" of the RPS and to modify the construction, thereby providing the necessary safety margin.

The analysis formed part of the safety report of ZR-6M.

6. AKNOWLEDGMENTS

The author is indebted to Dr. Z. Gyimesi, Director, and Dr. Z. Szatmáry, Deputy Director of the Institute for Atomic Energy Research for suggesting the need for a quantitative risk assessment.

7. REFERENCES

- [1] Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 /NUREG 75/014/ 1975.
- [2] Deutsche Risikostudie Kernkraftwerke, Verlag TÜV Rheinland, Köln, 1979.
- [3] Swedish Reactor Safety Study, Barsebäck Risk Assessment. MHB Technical Associates, Palo Alto, California, 1978.
- [4] D. Nielsen: Use of Cause-Consequence Charts in Practical Systems Analysis, Reliability and Fault Tree Analysis. SIAM, Philadelphia, 1975.
- [5] W. Hofman: Zuverlässigkeit von Mess-, Steuer-, Regel- und Sicherheitssystemen, Verlag K. Thiemig, München, 1968. p.191.
- [6] Reactor Safety Study, Appendix III, Failure Data.
- [7] H. Böck: Sicherheitsbezogene Störfälle in amerikanischen Leichtwasserreaktoren im Zeitraum 1967 bis 1974 und Vergleich von Fehlerraten Spezieller Reaktorkomponenten. Atomkernenergie 26, /4/, 242, 1975.
- [8] D. Nielsen: Reliability Analysis of Proposed Instrument Air System. RISØ - M - 1903, 1977.
- [9] S.G. Ireson: Reliability Handbook, New York, McGraw Hill, 1966, Table 12.10.

APPENDIX 1

ZR-6M CRITICAL ASSEMBLY

1.1 General Description

The core of the reactor is formed by WWER-type fuel elements arranged in a hexagonal lattice of 12.7 mm pitch. The core is situated in the core tank /CT, see Fig. 7/ which, in turn, is inside the pressure vessel /PV/. The moderator is distilled or borated water. Water is heated in PV to operating temperature and is then pumped into CT. PV is filled from the storage tank /ST/.

The reactor is regulated by changing the water height. There is a wide range of critical water heights depending on core configuration and boron concentration. Three groups of safety rods, with three rods each, serve for fast shutdown of the reactor in case of a scram. The safety rods, made from borated stainless steel, have a three-pointed asteriod section and enter the lattice in the space between three fuel rods. Should the safety rods fail to shut down the reactor, six fast-drain valves open and dump the water from CT into PV. Water from PV can be drained into ST through a dump valve. PV is situated in the reactor shaft which is in the middle of the reactor hall. ST is in the technological shaft. The two shafts are connected by a tunnel.

Technical characteristics:

Critical water heights:	600 ... 1000 mm
Reactivity worth of water level change:	0.3 ... 8.0 ϕ mm ⁻¹
Number of fuel rods:	600 ... 2000
Enrichment:	1.6; 3.6; 4.4 %
Operating temperature:	20 ... 130°C
Overpressure:	0 ... 3,5 bar
Boric acid concentration:	0 ... 7 g/l

1.2 Reactor protection system

A simplified schematic diagram of the reactor protection system is shown in Fig. 8. Neutron flux in the core is measured by six detectors, two of them operating in pulse and four in current regime. Any of these six neutron channels is capable of tripping th reactor if the flux exceeds a preset value. There are also trip settings for low doubling time.

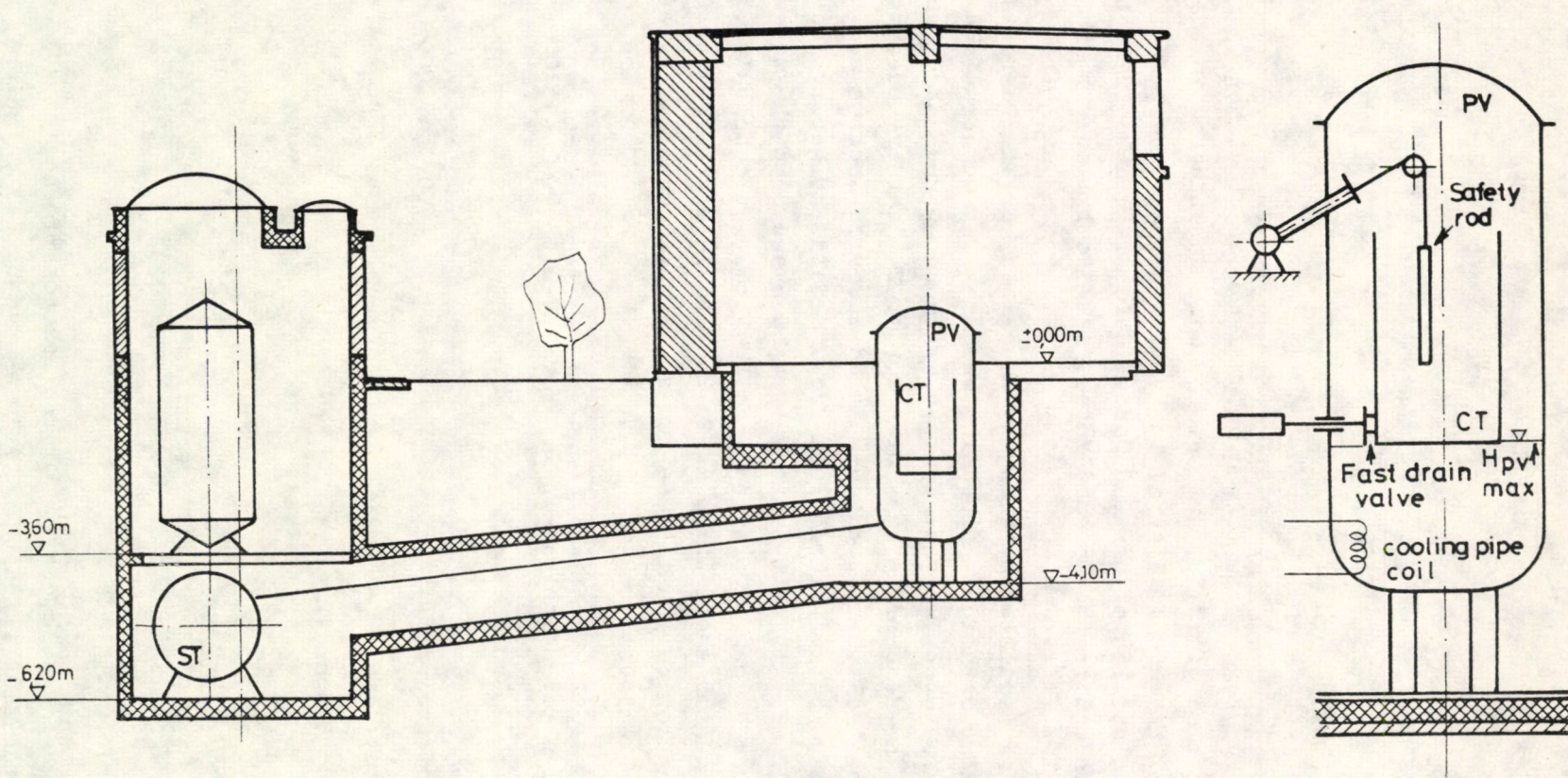


Fig 7. Elevation of the facility

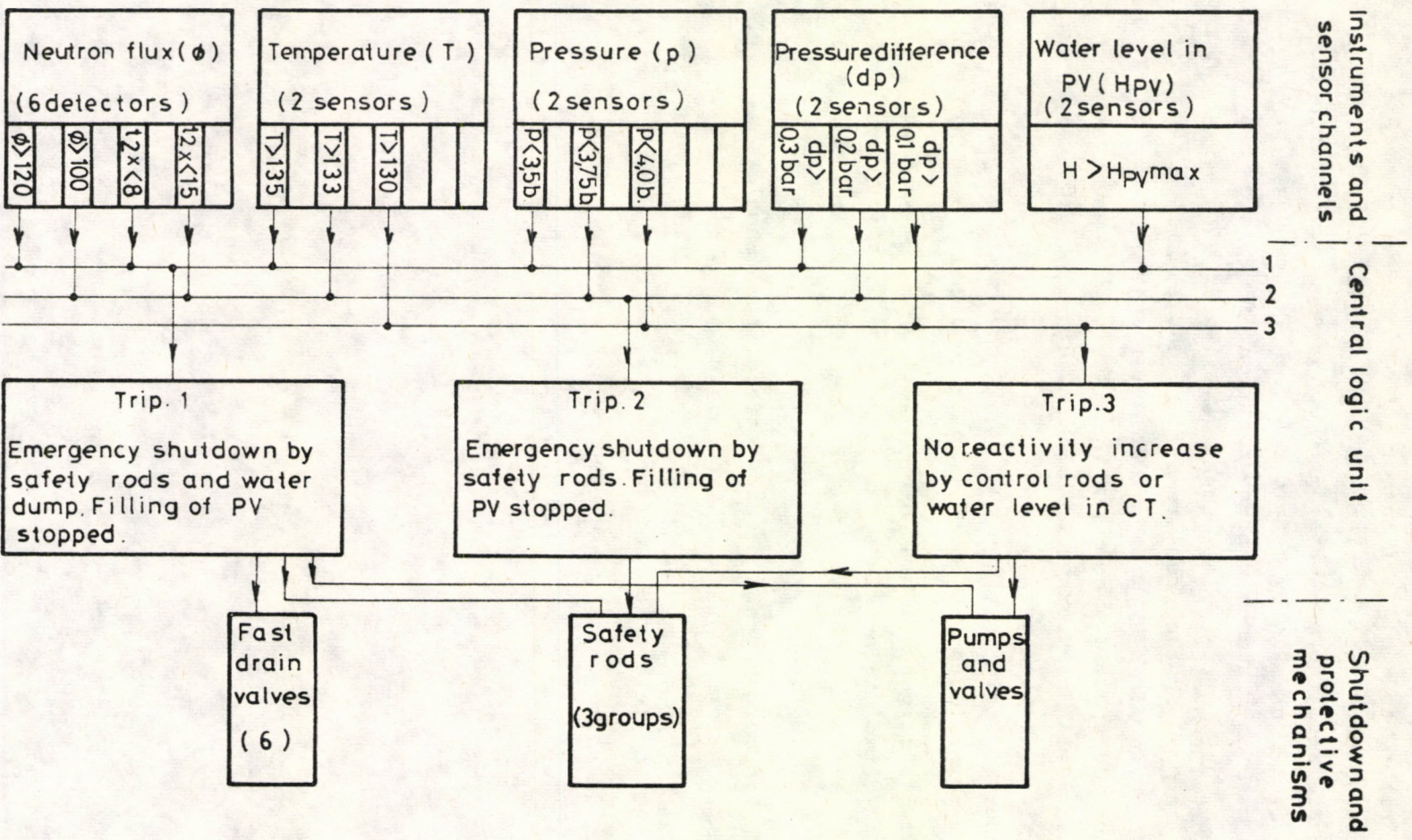


Fig. 8 Simplified diagram of RPS.

Pressure in PV must always be higher than the saturation value at the given temperature to avoid boiling of the water. Two temperature and two pressure transducers trip the reactor before this unstable regime is reached.

There are also two pressure-difference transducers connected between PV and a puffer tank which communicates with PV through a pipe of small diameter. In case of a sudden depressurization of PV /e.g. due to a tube rupture/ pressure in the puffer tank changes with considerable delay and the reactor is tripped by the pressure-difference signal.

The water level in PV must not be higher than the bottom of CT /in order to provide space for dumping the water/. The pump filling PV is stopped if the water level in PV exceeds the permissible maximum value. At the same time there is a reactor trip.

The central logic unit, which is self-checking, compares actual parameter values with trip limits and initiates the required protective action:


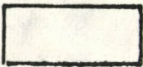
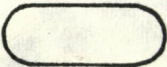
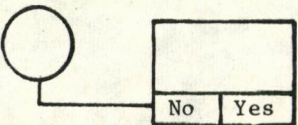
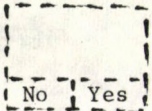



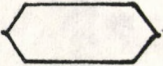
Trip 1: Emergency shutdown by safety rods and water dump. Should two drain-valves fail, the remaining four are sufficient to dump the water in the required short time. Trip 1 also stops the pump filling PV.

Trip 2: Emergency shutdown by safety rods. Should one group of safety rods fail, the remaining two are sufficient to shut down the reactor. The pump filling PV is stopped by this trip function, too.

Trip 3: No reactivity increase by control rods or water level in CT.

APPENDIX 2.

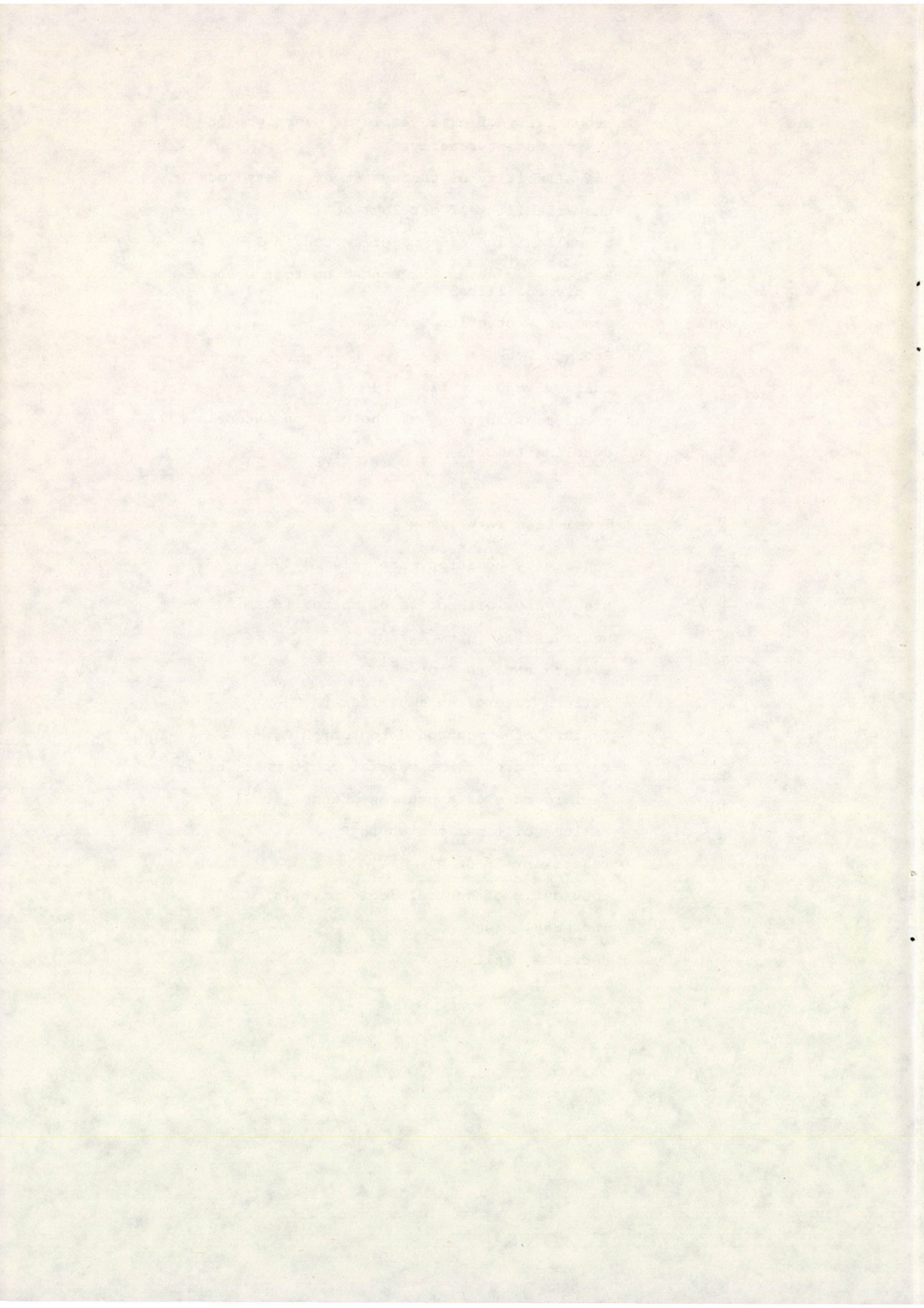
CCC SYMBOLS

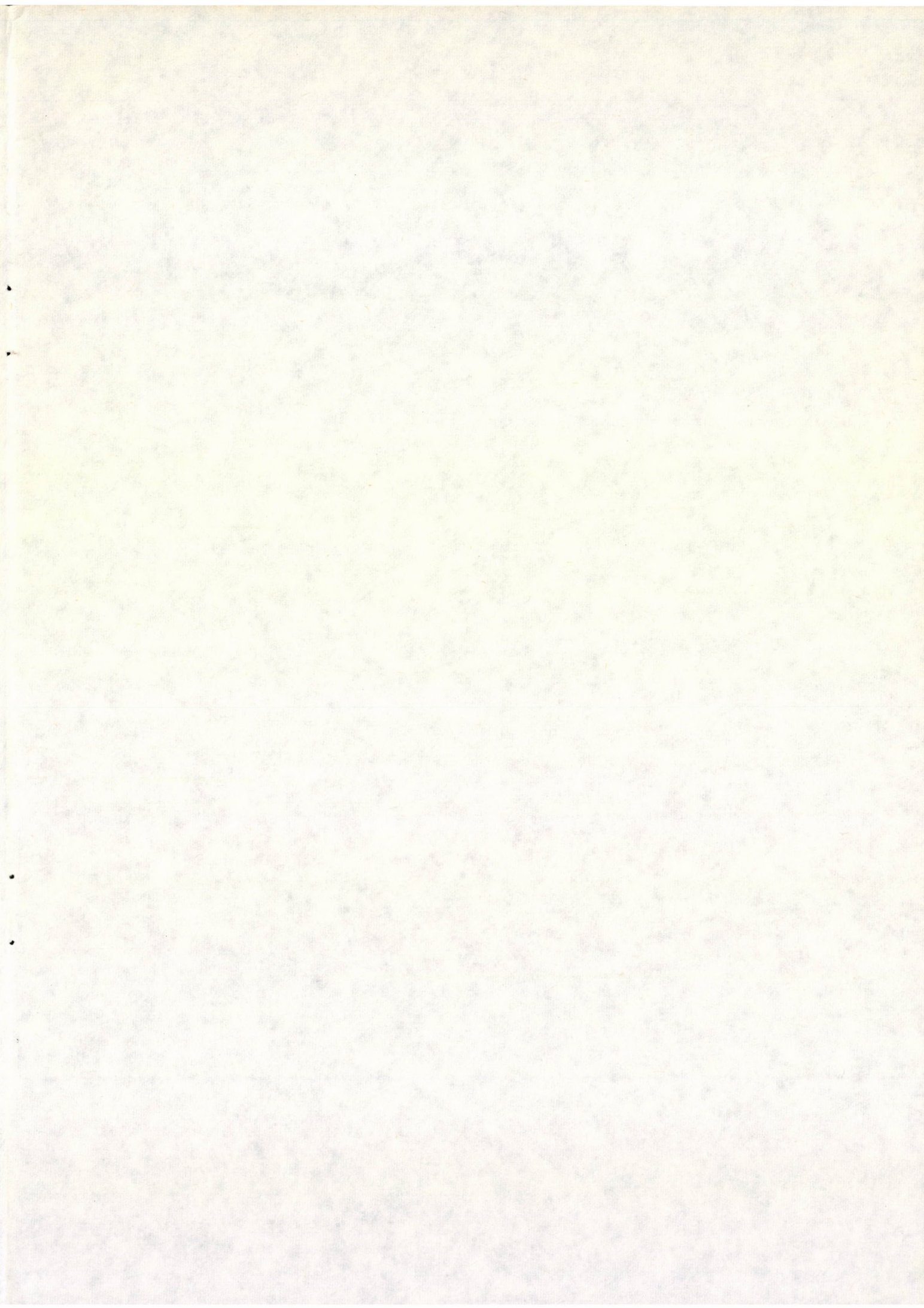
		Basic condition
		Event
		Comment
failure condition		Either/or vertex /Designed safety action/
		Condition vertex
		Delay /minutes/
		AND - gate
		OR - gate
		Consequence

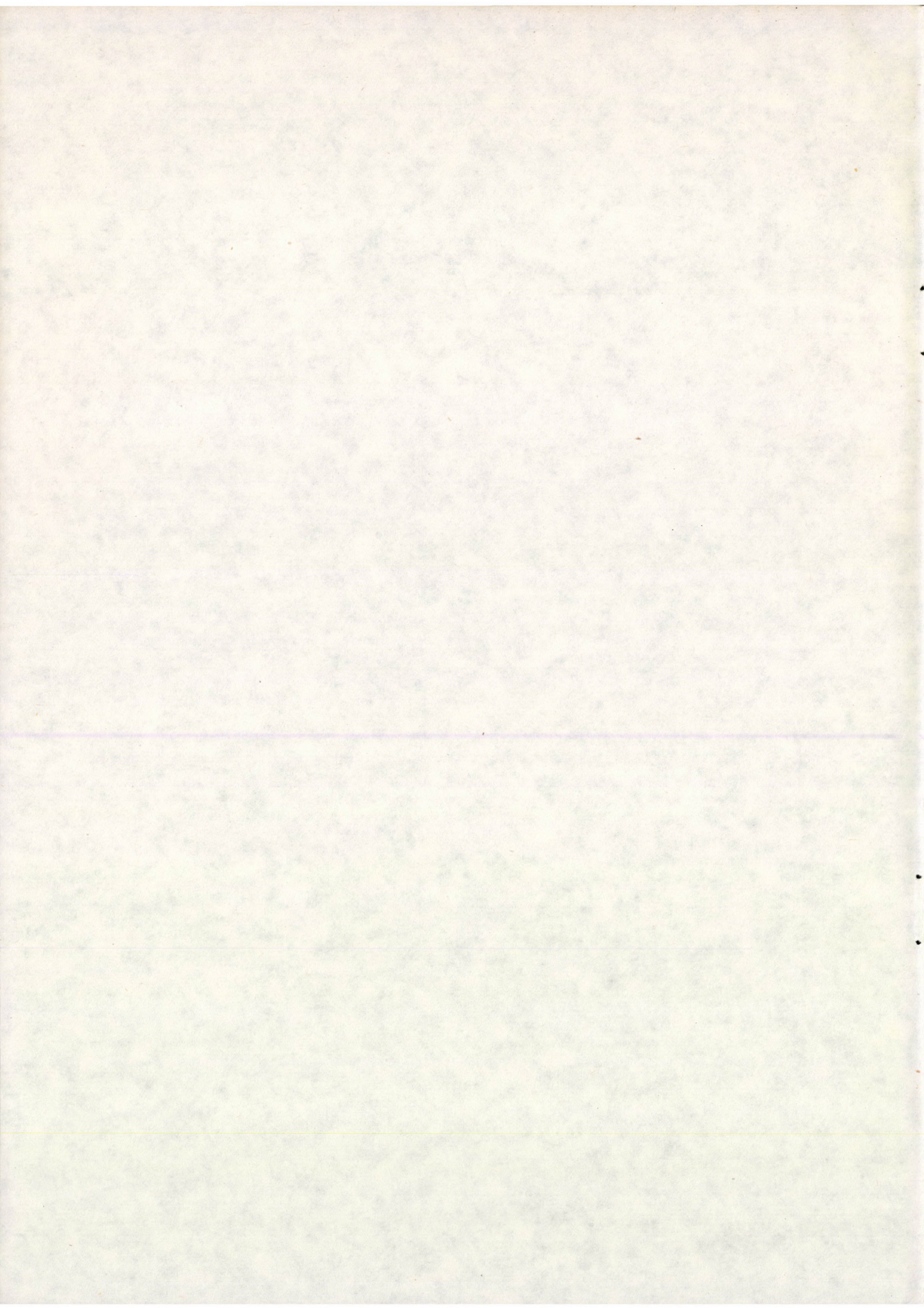
NOTATIONS, ABBREVIATIONS

A	reactivity addition rate [ϕ s ⁻¹]
CCC	Cause - consequence chart
CT	Core Tank
d ⁻¹	per demand
D _{fl}	probability /per week/ of unsafe final state in CCC - f/l
d _{fl}	corresponding Boolean variable
H	water height [cm]
H _{cr}	critical water height in CT [cm]
H _{PV max}	permissible maximum water height in PV [cm]
p	pressure in PV [bar]
dp	pressure difference between PV and puffer tank
PV	pressure vessel
Q	unavailability, failure probability /per week/
Q ₁	unavailability of the central logic unit during a test cycle
Q ₂	failure probability of the reactor during a test cycle
Q _{fl}	probability of emergency situation f/l /per week/
Q _H	unavailability of the system of two level gauges [d ⁻¹]
Q _{HP}	probability of failure of stopping the pump filling PV if water level exceeds H _{PV max} [d ⁻¹]
Q _L	unavailability of central logic unit [d ⁻¹]
Q _N	unavailability of the system of neutron channels [d ⁻¹]
Q _{N1}	unavailability of a neutron channel [d ⁻¹]
Q _{NR}	failure probability of emergency shutdown by safety rods if neutron flux exceeds 100% [d ⁻¹]
Q _{NP}	probability of failure of stopping the pump filling PV if neutron flux exceeds 100% [d ⁻¹]
Q _{op2}	probability of human failure: omission of response to acoustic scram signals [d ⁻¹]

Q_{Op4}	probability of human failure: oversight of instrument readings [d^{-1}]
Q_R	unavailability of the system of safety rods [d^{-1}]
Q_{rel}	unavailability of a relay [d^{-1}]
Q_{ts}	unavailability of a timer switch [d^{-1}]
q_1 etc.	Boolean variables corresponding to the above probabilities
RPS	Reactor Protection System
ST	Storage Tank
t_{fe}	failure exposure time [h]
t_m	proof test interval of the neutron channels [h]
t_{2x}	doubling-time [s]
T	temperature [$^{\circ}C$]
$\frac{\partial H}{\partial t}$	level rise rate [$mm\ s^{-1}$]
$\frac{\partial \rho}{\partial t}$	reactivity addition rate [$\phi\ s^{-1}$]
$\frac{\partial \rho}{\partial H}$	reactivity worth of level change [$\phi\ mm^{-1}$]
ϕ	neutron flux [$n\ cm^{-2}\ s^{-1}$]
λ	failure rate [h^{-1} or d^{-1}]
λ_A	failure rate of an amplifier [h^{-1}]
λ_D	failure of a neutron detector [h^{-1}]
λ_L	failure rate of the central logic unit [h^{-1}]
λ_{N1}	failure rate of a neutron channel [h^{-1}]
λ_{ts}	failure of timer switch [h^{-1}]
ρ	reactivity [$\$$ or ϕ]
τ	test cycle of central logic unit [s or h]
\uparrow	increase, rise
\downarrow	decrease, fall







63.141



Kiadja a Központi Fizikai Kutató Intézet
Felelős kiadó: Gyimesi Zoltán
Szakmai lektor: Bürger Gáborné
Nyelvi lektor: Harvey Shenker
Gépelte: Beron Péterné
Példányszám: 335 Törzsszám: 81-240
Készült a KFKI sokszorosító üzemében
Felelős vezető: Nagy Károly
Budapest, 1981. május hó