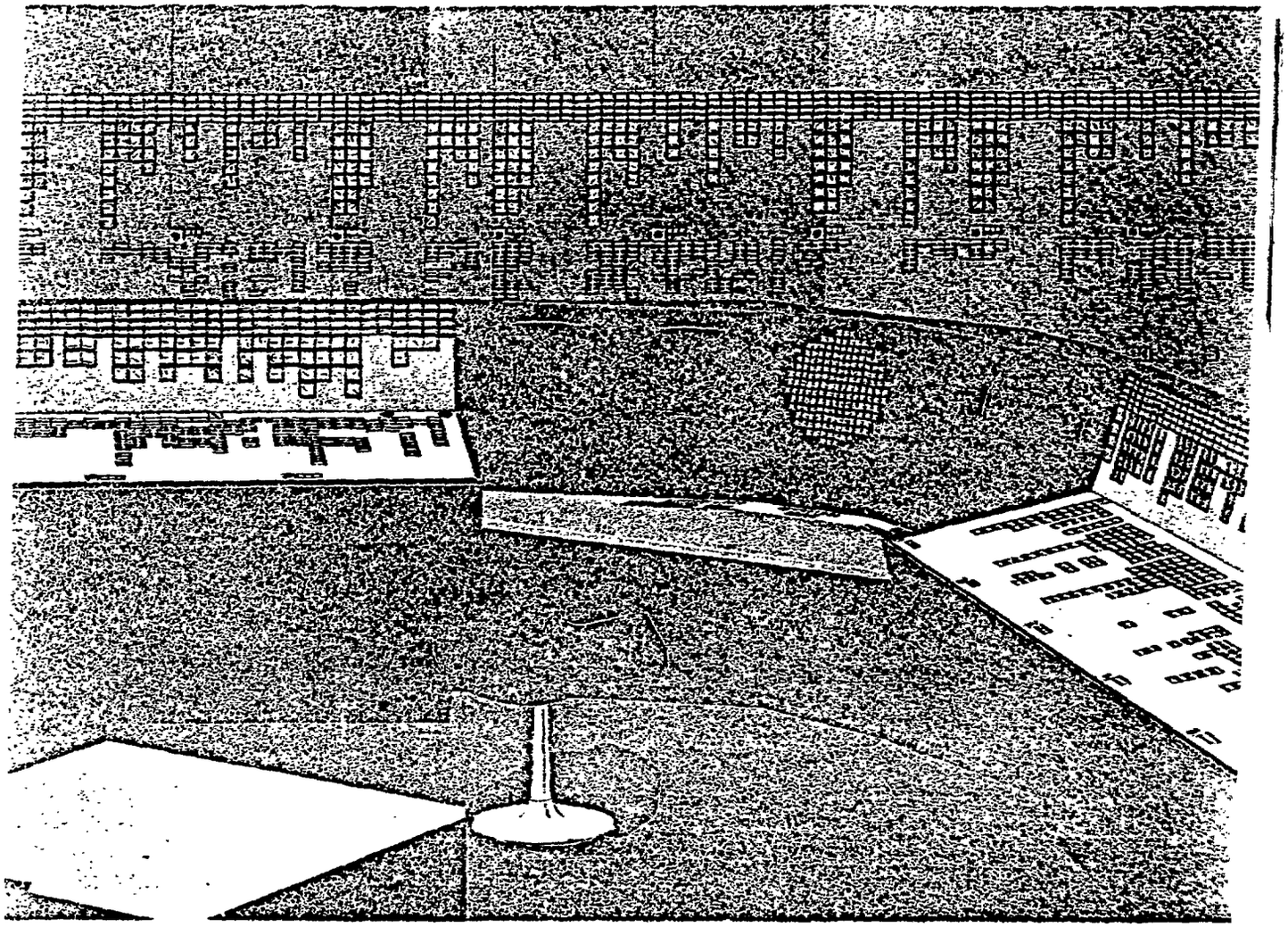
INIS-mf--4246 ES7800186

SAFETY ASPECTS ON CONTROL ROOM DESIGN



ASEA-ATOM

Tr. 1994 c 77-09 200.000 Västra Aros Tryckeri AB

ASEA-ATOM

ES 7800186

SAFETY ASPECTS ON THE ASEA-ATOM BWR 75 CONTROL ROOM DESIGN

by

Paul van Gemst,
Tor Pedersen

AB ASEA-ATOM
S-72104 VÄSTERÅS, SWEDEN

Presented at the
IAEA Specialist Meeting on

"The Effect of Regulatory Requirements on Nuclear Power Plant Control and Instrumentation Systems"

in Madrid, October 4-6, 1977

1804 c 77-09 300.000 Västra Aros Tryckeri AB

SUMMARY

BWR 75 designates the most recent design of the ASEA-ATOM boiling water reactor on which the basic design was carried out during 1974 and 1975. The first plants of this new design were ordered by Swedish customers in 1975 and 1976.

In fact, the BWR 75 is far more than a reactor plant. The goal for the design work was a complete power generating plant where reactor, turbine and BoP (Balance of Plant) systems were technically and economically integrated.

The control room is an integrated part of the total plant layout and is located in a special building, known as the control building.

This paper is dealing with the problems of designing a control room meeting all safety requirements and at the same time allowing for modifications to meet special customer specifications.

The analysis comprises:

- Control room system design
- Location and physical separation
- Design of the display and manual control systems
- Operator's role
- Ventilation and lighting systems
- Crashing aircraft
- Sabotage
- Shut down facilities outside control room.

Furthermore a classic conflict situation between established safety criteria and man/machine requirements is pointed out.

4 c 77-09 300.000 Västra Aros Tryckeri AB

CONTENTS:

Bl. 1604 c 77-09 300.000 Västra Aros Tryckeri AB

Bl. 1604 c 77-09 300.000 Västra Aros Tryckeri AB

ATTACHED FIGURES:

1. BWR 75 - Main Communication routes, Level ± 0.0
2. BWR 75 - Control building, Level ± 0.0
3. BWR 75 - Control room layout
4. BWR 75 - Control building, Level - 4.0
5. BWR 75 - Buildings, Physical separation
6. BWR 75 - Control room ventilation, Normal ventilation and control room isolation
7. BWR 75 - Control room ventilation, Smoke removal and cooling with outdoor air.
8. BWR 75 - Buildings, Protection against crashing aircraft.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

INTRODUTION

In a power plant, conventional as well as nuclear, the control room is partly a center for the supervision, monitoring and control of the plant operation and partly a center for the communication with the surrounding world.

The operators are responsible for the start-up and shut-down procedures of the power plant and for the supervision of the plant and of its various processes during normal operation. The operators shall also decide whether the demands on power output can be met with regard to the prevailing plant conditions, whether expected power changes can be accomplished, whether and how disturbances or limitations shall be remedied, etc.

To give the operators the best possible overall view of the situation in the power plant, all information that is of importance for the plant operation, is collected from the process and brought together in the control room. Great care must be taken, though, to make the presentation to the operator as clear and distinct as possible to ensure rapid recognition of the situation.

In a nuclear power plant, special considerations must be taken to the aspects of nuclear safety and the requirements from the authorities. These requirements are partly site-dependent requirements specified in detail, and partly general requirements given as references to U.S. NRC General Design Criteria, Regulatory Guides, Standards, etc., of which those applicable to the design of the control room and control equipment are listed below.

Bl. 1004 c 77-09 300.000 Västra Aros Tryckeri AB

NRC General Design Criterion 19	Radiation protection of operators. Shut down possibility outside the control room.
NRC Regulatory Guide 1.78	Habitability of control room during chemical releases.
NRC Regulatory Guide 1.95	As RG 1.78.
NRC Regulatory Guide 1.114	Being operator.
IEEE 420	Control switchboard.
IEEE 566 (Draft)	Design of display and control facilities.
SEN 36 90 03 (Draft Swedish Standard)	Reactor shutdown without access to the control room.
NRC General Design Criterion 2	Protection against natural phenomena.
NRC General Design Criterion 3	Fire protection.
NRC General Design Criterion 13	Instrumentation and control.
NRC Regulatory Guide 1.17	Protection against sabotage
NRC Regulatory Guide 1.22	Periodic testing.
NRC Regulatory Guide 1.47	Bypass indication.
NRC Regulatory Guide 1.62	Manual indication.
NRC Regulatory Guide 1.75	Physical independence.
NRC Regulatory Guide 1.97	Post accident monitoring.
NRC Regulatory Guide 1.120	Fire protection.
SEN 36 90 01 (Swedish Standard)	Protection systems.

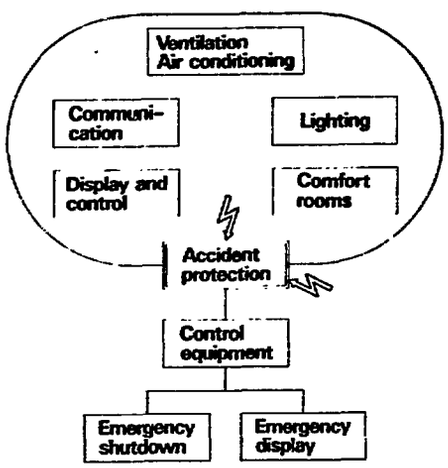
Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

This paper will discuss the effects of safety requirements on the design of the control room system. The discussion will mainly deal with the control equipment as an integrated part of the total system complex, i.e. taking into consideration equipment and systems which are normally beyond the responsability of the control engineer.

Bl. 1804 0 77-09 300.000 Västra Aros Tryckeri AB

THE CONTROL ROOM SYSTEM

The control room including the control equipment inside it, the auxiliary systems like ventilation and air-conditioning, lighting, etc., and comfort rooms, is a system complex that is a key element in the total control system concept of the power plant.



One of the characteristics of the control system concept of the ASEA-ATOM BWR power plants is that the control equipment inside the control room only comprises displays and manual control units. All process interface and electronic signal conditioning and process control equipment are located in special apparatus rooms outside the control room.

As required by the NRC General Design Criterion 19, and also the draft Swedish Standard SEN 369003, facilities are also provided for emergency manual shutdown of the reactor outside the control room.

Bl. 1204 c 77-09 300.000 Västra Aros Tryckeri AB

To be very strict, the control room system is confined to the equipment and the environment inside the control room and to the surrounding building structures, but could in a wider meaning be extended to comprising also the control equipment outside the control room and the interface towards the control room and the plant processes.

The most important functions of the control room system and the operating staff can be summarized in the following way:

- The control room system shall provide

  acceptable working conditions for the operators with regard to presentation of information, comfort, light intensity level, etc.,

  protection of operators and control room equipment against accidents occurring outside the control room.

- The control room shall also enable

  protection of plant equipment outside the control room against accidents occurring inside this room to safeguard the safe shutdown of the plant without access to the control room,

  prevention of incidents by rapid manual actions when alarms are initiated or simply by avoiding operator errors during manual control actions,

  monitoring and following up of important parameters when an accident occurs in the plant even if a single failure occurs in the control equipment.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

In the following, the discussion will concentrate on the three first functions, since the two last ones are well covered by previous papers and other available literature and will also be regulated by a new *IEEE Standard* that is in progress.

Bl. 180:4 c 77-09 300,000 Västra Aros Tryckeri AB

THE CONTROL ROOM LOCATION AND LAYOUT
(See attached figures 1, 2 and 3).

In the ASEA-ATOM BWR power plant design, one control room is provided for each reactor unit, even if two identical units are being built on the same site.

The control room is located in a separate building, known as the control building. This building is sited adjacent to the reactor building and has good personnel communication with the entrance building with its offices and with the other plant buildings via the main communication routes on both controlled (possibly radioactive) and uncontrolled area.

Rooms are provided in the control building and around the control room for the electronic and computer equipment, battery systems, ventilation and air-conditioning. Rooms are also provided to ensure the comfort of the operator, such as office, mess room, documentation room and toilets.

The building normally has two floors, the cable floor being below ground level. Cables between equipment inside and outside the control building are run in this area.

Various types of control desks, boards and panels are located inside the control room. The control units for safety-related equipment (including the auxiliary systems such as for power supply, cooling and ventilation) are placed together, so that the operator will have a clear overall view of these systems. Other typical areas in the control room are

- desk for internal and external communications, etc,
- desk for normal operation (power operation, hot startup and shutdown procedures),

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

- panels for service systems and for cold startup and shutdown procedures.

Note that the desk and panels in the control room only contain displays and manual control equipment. The process interface and the signal conditioning electronics are located in the special apparatus rooms.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

PHYSICAL SEPARATION
(See attached figures 2, 4 and 5)

For the newer nuclear power plants in Sweden the authorities require that safety-related equipment be separated into four subdivisions with regard to the single failure criterion. These requirements are applicable to mechanical as well as electrical systems.

Operation of two subdivisions is sufficient for safe shutdown of the plant in the case of a LOCA. During normal operation this makes it possible for the plant owner to repair equipment and still accept the single failure criteria during the repair work.

Components belonging to different subdivisions must be located in different rooms. Exceptions are only allowed inside the reactor containment and in the control room. The walls and, of course, the penetrations through the walls (e.g. for cables, ventilation, doors) must withstand different types of accidents, such as fires, flooding, missiles and, in newer plants, also sabotage.

The control panels for the four safety-related subdivisions are located in the control room. These panels incorporate indicators, annunciator lamps, push-buttons and lamps for status indication. Following an accident, the plant will be shut-down automatically and no manual control action is required.

The operator's task is mainly to follow up the course of the accident. It is possible, especially if minor component faults have occurred, that he may want to take manual action. In accordance with Swedish design requirements, it is not necessary to make these corrections before 30 minutes after the accident.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

At ASEA-ATOM, we have discussed the safety classification of these control panels in much detail, and we decided tc classify them as safety-related equipment and separation criteria must thus be applied.

Equipment for each subdivision is installed in totally-enclosed, sheet steel cubicles. Furthermore, cubicles belonging to different subdivisions have an air gap of about 15 cm between them.

Cables are run downwards through the floor to the cable area beneath.

As you can see from the layout sketches, there are four cable areas, separated by heavy concrete walls. In each cable area, there are cables for connection between the control room and the signal conditioning equipment and between the latter and the plant.

You will note that the physical separation in our plant differs widely from the minimum requirements in the Regulatory Guide 1.75 or IEEE Standard 384. In these documents separation by distance is normally acceptable. The Regulatory Guide and IEEE 384 also specify separation between safety-related and non-safety-related equipment.

In order to make the life easier for our QA (Quality Assurance) people, we do not mix these two types of equipment. We install them in separate cubicles and run cables on individual cable trays. However, we do not use the distance separations as required in the Regulatory Guide 1.75 and IEEE 384. We do not understand the reasons behind these requirements.

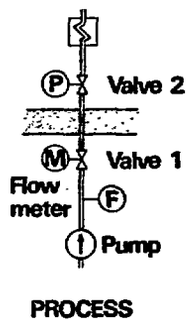
Bl. 1604 o 77-09 300.000 Västra Aros Tryckeri AB

THE CONTROL ROOM AND CONTROL PANEL DESIGN

Over many years, a practice has been established for the design of the control room and control panels. Most of these conventional guidelines have been developed in order to improve the interface between the process and the operator.

The new safety requirements which have been primarily established for technical reasons, such as single failure accidents and physical separation, can decrease the operator's ability to monitor the plant.

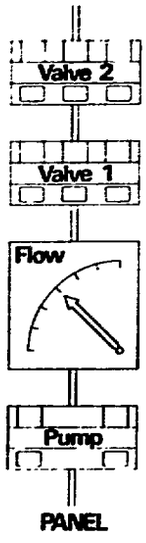
We can illustrate this with the following example:



Safety	
Yes	No
Subdiv	
A	B	
	x	
x		
		x
		x

In a typical plant, there is a cooling system which supplies water to components inside the reactor containment. Many of these systems are classified as non-safety-related systems. However, every pipe passing through the containment wall must be provided with isolation valves. These valves are safety-related components.

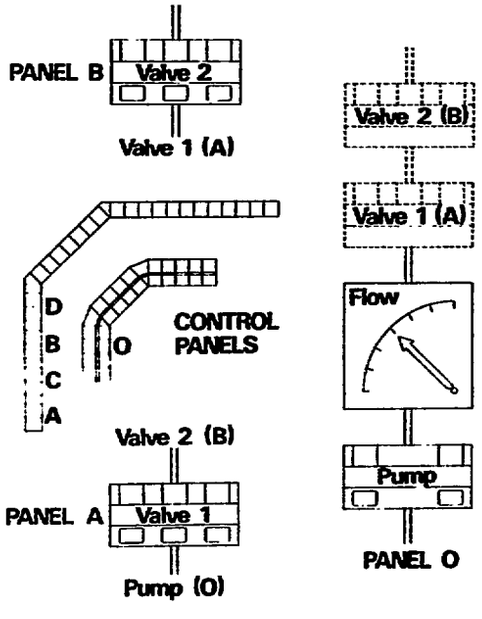
Bl. 1804 o 77-09 300.000 Västra Aros Tryckeri AB



In a conventional plant, all displays and other control units are located in the same control panel and have been grouped together in a functional way. So it is easy to check that, for instance, valves are open before the pump is started. Damage to pumps due to improper manual starting procedures therefore occurs very seldom.

However, this design cannot be used in nuclear power plants, where there are requirements on separation for components belonging to safety-related and non-safety-related equipment and for components belonging to the four safety-related subdivisions.

In our example, there are two safety-related subdivisions (the inner and outer isolation valves) plus non-safety-related components (the pump and flow indicator), so the display and control systems in the control room must be separated into three parts. As a result, they are very often located on three different panels, and the operator has lost the overall view of the system.



Bl. 1804 c 77-09 300.000 Västra Ärca Tryckeri AB

(In this way, the electronic signal conditioning equipment belonging to this special cooling system is also located in three different rooms. This makes service and commissioning more difficult than in the conventional design.)

The control of all containment isolation valves as well as other safety-related components must take place from the appropriate sections of the safety-related control panels, so that following an accident the operator shall be able to check that necessary automatic functions (closing valves, etc) have been carried out.

The inconvenience of the strict application of the separation criteria could, however, to some extent be mitigated by adding status indications for the safety-related components in the non-safety-related control panel (as indicated by dashed lines on the figure).

This practical compromise improves the overall view of the system, but implies additional isolating devices in the safety-related electronic equipment and an increased signal exchange between safety-related and non-safety-related equipment. In our opinion, such compromises should therefore not be applied generally.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

VENTILATION AND AIR-CONDITIONING
(See attached figures 6 and 7)

Parts of the ventilation system for the control room have been classified as safety-related equipment. The control room ventilation is separated from the four systems which ventilate the other safety-related areas inside the control building.

Since it is considered acceptable for the control room ventilation to be out of service for some time, it consists of only two redundant parts. There are different operation modes, of which we can mention the following important ones:

- comfort ventilation during normal operation
- emergency ventilation during accidents outside the control room
- emergency ventilation for smoke removal from the control room.

Several alternatives are available for the different operation modes such as with or without filters, air recirculation, etc.

During normal operation, the ventilation together with the air-conditioning units, supply the control room with the specified quantity and quality of air. Note that the air-conditioning unit is not part of the safety-related system.

Regardless of the weather conditions, there will be a comfortable working environment in the control room.

Bl. 1604 c 77-09 300.000 Västra Ärva Tryckeri AB

In the event of an accident outside the control room, radioactivity or toxic gases like chlorine or smoke may be drawn into the control room. The Regulatory Guide 1.78 requires instrumentation to detect such gases and to switch the ventilation over to the emergency mode.

In our design, the normal and emergency modes of operation are the same, so we do not need this additional instrumentation. The necessary filtering equipment is continuously connected to the system. Other possibilities for keeping toxic gases outside the control room are provided, such as closing the ventilation isolating valve, which is to be done manually. During both normal and emergency modes, most of the air will be recirculated through the air-conditioning unit. Recirculation through the filters is also possible.

In the event of a fire inside the control room, the valves at the inlets must be closed manually from the outside. The smoke can be removed by the exhaust fans and ducts which are designed for the higher air temperatures.

Bl. 1804 e 77-09 300.000 Västra Aros Tryckeri AB

LIGHTING

After an accident and simultaneous loss of electric power, the plant is automatically safely shut-down and operator action is not immediately necessary. However, we are of the opinion that even during such situations, good lighting must be available in the control room, in order to reduce human stress and avoid panic. A certain part of the control room lighting system is therefore supplied with power from battery-backed a.c. systems. Furthermore, the lighting power supply is redundant and a single failure is acceptable. The remaining part of the lights are connected to two stand-by diesel-generator systems, so the interruption time will be of the order of 10 s.

It is very difficult to design the light intensity level in the proper way. There are many conflicting requirements. The level must be high, to allow conventional indicators to be read and to make it possible for the operator to write and read. The intensity level must also be sufficiently low to allow for the discernment of the lamp indications and the computer displays (CRTs). Furthermore, there are requirements concerning the minimizing of reflections from instruments.

These requirements are normally satisfied by having different lighting areas. Each area has its own thyristor-controlled light intensity level adjustments. The lamps are often adjustable, with provisions for direct or indirect lighting. So it is easy for the staff to make adjustments after the plant has been taken into operation.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

PROTECTION AGAINST CRASHING AIRCRAFT
(See attached figures 2 and 8)

During the past few years and depending on the site locations demands are made on aircraft crash protection for power plants. The type of aircraft, the speed and crash angle are specified by the authorities.

In order to guarantee safe shutdown, the control building is in the same way as the reactor building and parts of other buildings protected in the following way.

Roofs and walls which are exposed to the risk of a crash are made out of very thick reinforced concrete.

If possible, the civil engineers add another floor on top of the building or place other buildings around the control building. This additional floor or buildings must not contain safety-related equipment.

To increase the protection, of the control room and the control equipment a corridor is provided around and just inside the outer concrete wall of the control building. From the control engineer point of view this corridor is very advantageous, since it also reduces the magnetic fields and induced interference under thunderstorm conditions.

These measures provide very good protection, so that equipment cannot be destroyed. However, the walls and roofs are penetrated by ventilation ducts. In order to reduce the risk that a crash will make ventilation of the control building impossible, the air outlets and inlets for the various subdivisions are located at the greatest distance from each other and very often at opposite walls. The minimum distance of about 20 m has been considered to provide very good protection.

81. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

Other measures must be adopted, so that burning fuel cannot flow directly into the building. Furthermore, equipment inside the building must be capable of withstanding the vibrations caused by the crash.

Bl. 1804 c 77-08 300.000 Västra Aros Tryckeri AB

PROTECTION AGAINST SABOTAGE
(See attached figure 2)

Two types of measures can be adopted to protect the plant against sabotage, vandalism, etc.

The first set of counter-measures is what is known in the USA as "Industrial Security Program". This program is very well described in the ANSI N 17.7-1973 standard and its main purpose is to prevent sabotage in the plant. The application of this standard to the control room will be discussed here.

The other sets of measures presume that, in spite of the above counter-measures, sabotage has been carried out in the plant. In such a situation, this type of sabotage inside the control room must be confined to the control room, so that safe shutdown by equipment outside the control room will be possible.

Requirements necessary to safeguard against this type of sabotage have been described in the draft Swedish Standard SEN 369003.

In earlier plants, before they were modified, it was relatively easy to enter the control room. Special facilities were provided for visitors inside the room to demonstrate operation of the plant. Furthermore, people employed in the plant, but not belonging to the control room staff, received their instructions in the control room.

So the first thing we did for the new plants was to limit the number of people entering the control room. It is basically forbidden for visitors to enter the room. This applies in practice to the whole control building.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

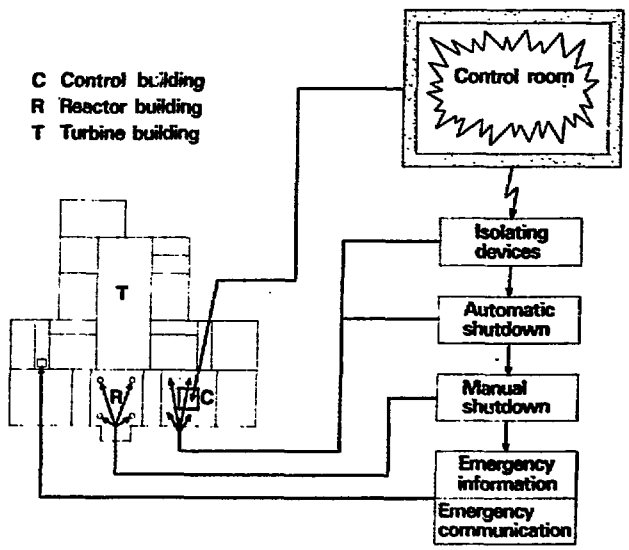
Working instructions for personnel not belonging to the control room staff, are given at a special counter, so that it is not necessary to open the control room door. Good personnel communication is provided between this counter and the control room.

Only one entrance into the control room is available. There are obviously several emergency exits, but they cannot be opened from the outside.

This entrance is provided with a double-door arrangement, and the space between the doors can be inspected from the control room side.

All these measures can delay sabotage, but cannot prevent it, so we assume in Sweden that the control room can be destroyed, but that the staff has been warned and can shut down the plant in time. After this manual shutdown, the automatic sequence equipment, which is located outside the control room, will take over and no additional manual action is required for several hours after the control room has been destroyed. The sabotage is not combined with a LOCA (Loss of Coolant Accident), so the task of the sequence equipment is very easy

Reactor shutdown outside the control room



Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

The plant must be designed so that the destruction will be limited to the control room and cannot spread to other rooms or equipment outside the control room. For this reason, the control room is confined within heavy concrete walls, which are designed to suit the above requirement. No direct penetrations are permissible between the control room and rooms with safety-related electronic equipment. The penetrations which are necessary to other rooms, such as for ventilation, cables and doors, are sufficiently strong to withstand an explosion or are designed so that it is acceptable to have them blown out.

Conceivable damage to electronic equipment is not merely mechanical, but also electrical, e.g. by short circuits, earth faults or by excessive voltages applied to the inputs and outputs. For this reason, isolating devices have been included in the safety-related signal cables to the control room. These isolating devices are of a type we have used before for physical separation and include relays, opto-couplers, resistors or isolating amplifiers. In the future, we plan to use fiber optics, thus eliminating electrical connections.

After postulated sabotage, the sequence equipment will be in operation for several hours until manual control action is required. This can be carried out from outside the control room, at different locations in the plant in the vicinity of the process equipment.

Process control is transferred from the automatic sequence equipment to push-buttons by means of individual switches for every process component. Status indication of these switches is provided in the control room.

Bl. 1604 e 77-09 300.000 Västra Aros Tryckeri AB

The circuits for manual control are independent of those for automatic shutdown and have their own control power supplies. The shutdown procedure can be supervised from a small room, where a few important indicators are installed.

In this room equipment for communication with personnel inside the plant and with authorities outside is also provided.

Bl. 1804 c 77-09 300,000 Västra Aros Tryckeri AB

CONCLUSIONS

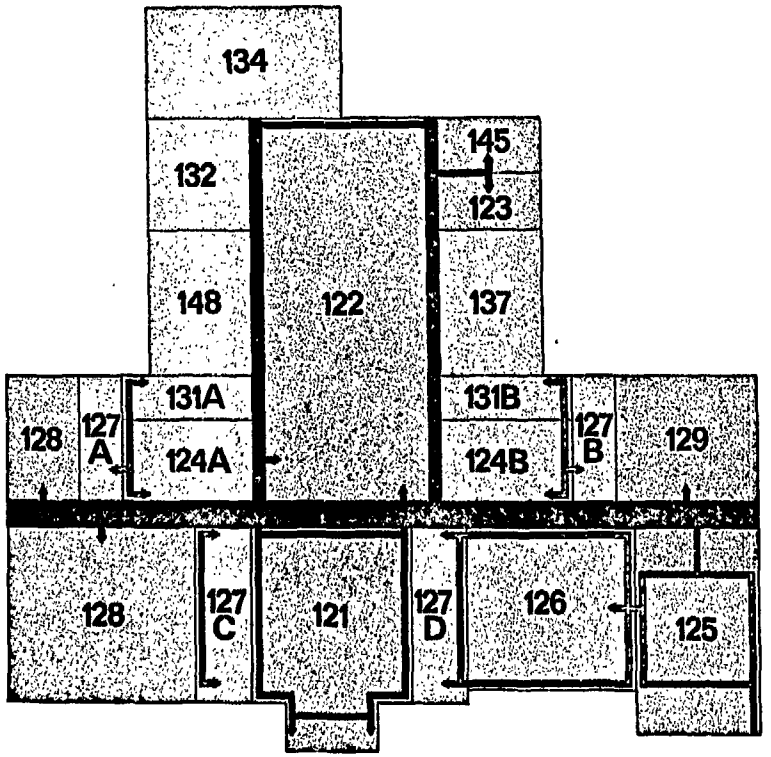
This paper has described some design requirements for the control room system. As this system incorporates both electrical and mechanical equipment as well as building structures the following conclusions can be drawn.

The control room designer is normally very familiar with the requirements for both human comfort and control equipment function. Thus it is natural that he should take the initiative to specify the other, non-electrical parts which can influence the working conditions inside the control room.

It is also evident that the application of individual safety requirements does not a priori lead to a safer plant, an advantage from one point of view often turns out to be disadvantageous from an other. The control room system is technically and human very complex and if new safety requirements shall be applied, the evaluation must be based on the total control room design and not on individual safety aspect bases.

Bl. 1804 c 77-09 300.000 Västra Aros Tryckeri AB

BWR 75 – MAIN COMMUNICATION ROUTES, LEVEL ±0.0



121 Reactor building
122 Turbine building
123 Condensate cleanup system building
124 Auxiliary systems buildings A, B

125 Entrance building
126 Control building
127 Diesel buildings A, B, C, D
128 Waste building

129 Active workshop building
131 Auxiliary cooling water buildings A, B
132 High voltage switchgear building
134 Transformer building

137 Turbine cooling water systems building
145 Offgas building
148 Storage building

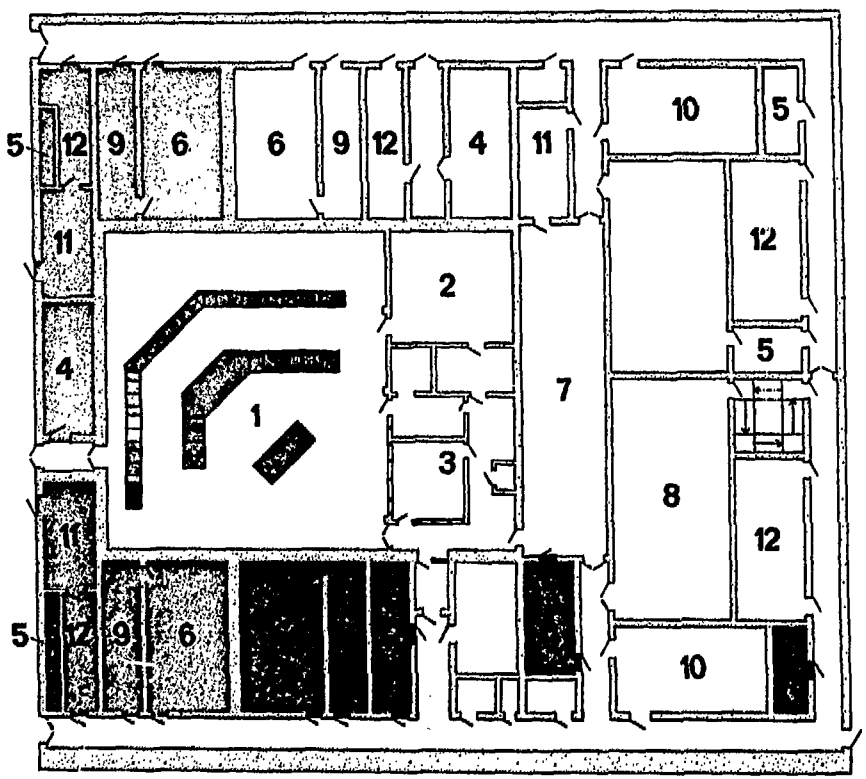
Controlled area
Uncontrolled area

Figure 1

TR 100-11, 2.1976

ASEA-ATOM

BWR 75 – CONTROL BUILDING, LEVEL ±0.0



Scale: 0 5 10 m

1 Central control room
2 Computer room
3 Office area

4 Control room ventilation
5 Other ventilation

6 Safety-related control equipment (IKM, etc.)
7 Operational control equipment, reactor plant (IKM, etc.)
8 Operational control equipment, turbine plant

9 Safety-related control voltage supply
10 Operational control voltage supply
1 Lighting and general power distribution
12 Batteries, ± 24 V

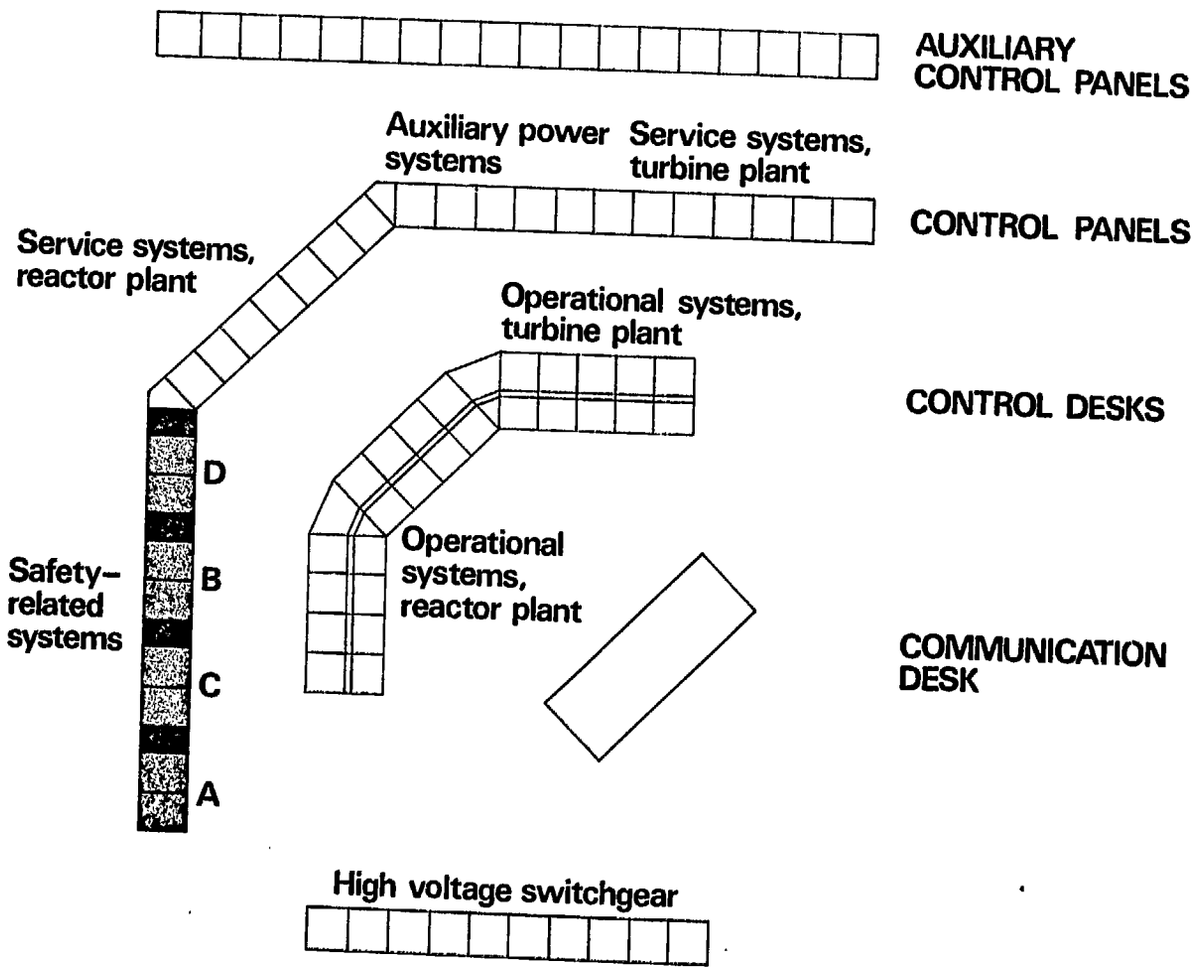
■ Subdivision A
□ Subdivision B
▣ Subdivision C
◘ Subdivision D

Figure 2

TR 126-1, 10.1975

ASEA-ATOM

BWR 75 – CONTROL ROOM LAYOUT

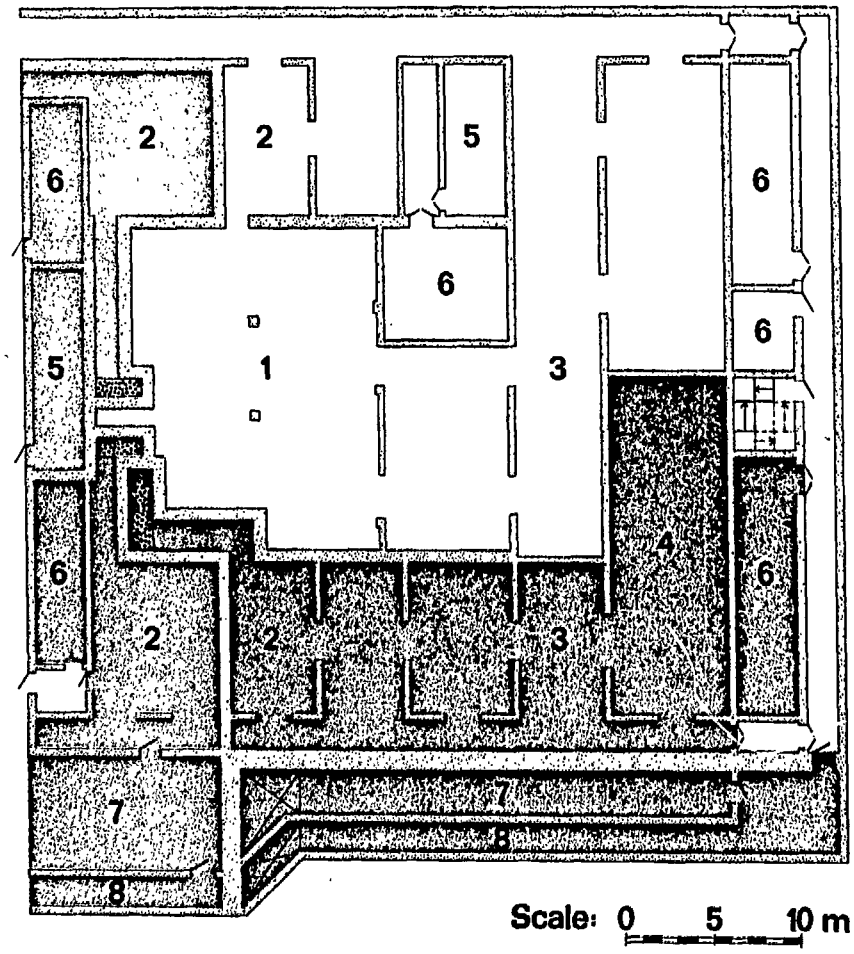


TR 511-1, 12.1975

ASEA-ATOM

Figure 3

BWR 75 – CONTROL BUILDING, LEVEL –4.0



Scale: 0 5 10 m

Cable spreading areas:

1 Control room equipment
2 Safety-related equipment
3 Operational equipment, reactor plant
4 Operational equipment, turbine plant

5 Control room ventilation
6 Other ventilation

7 Cable culvert
8 Service culvert

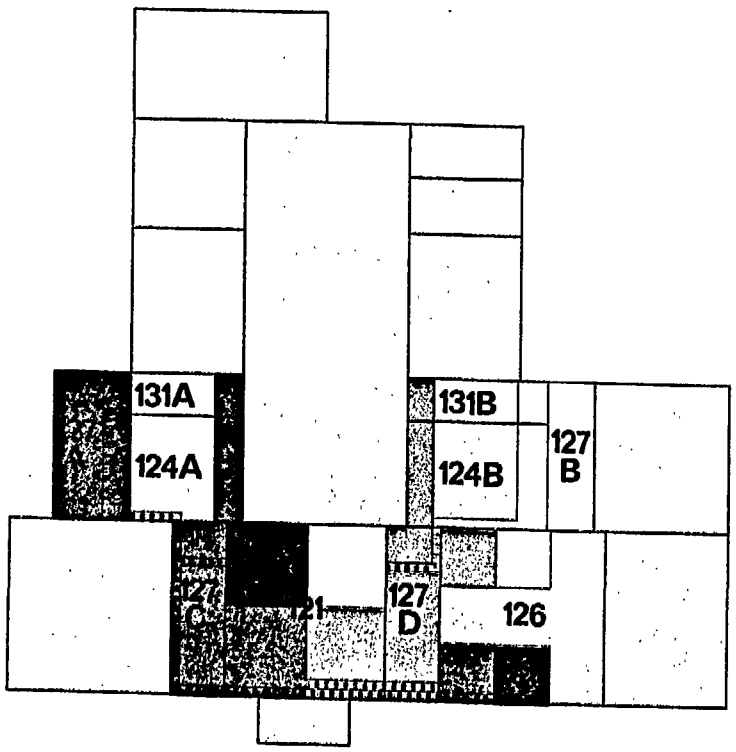
■ Subdivision A
□ Subdivision B
▩ Subdivision C
▨ Subdivision D

Figure 4

TR 126-2, 10.1975

ASEA-ATOM

BWR 75 – BUILDINGS, PHYSICAL SEPARATION



- Subdivision A
- Subdivision B
- Subdivision C
- Subdivision D

121 Reactor building
124 Auxiliary systems buildings A, B
126 Control building
127 Diesel buildings A, B, C, D
131 Auxiliary cooling water buildings A, B

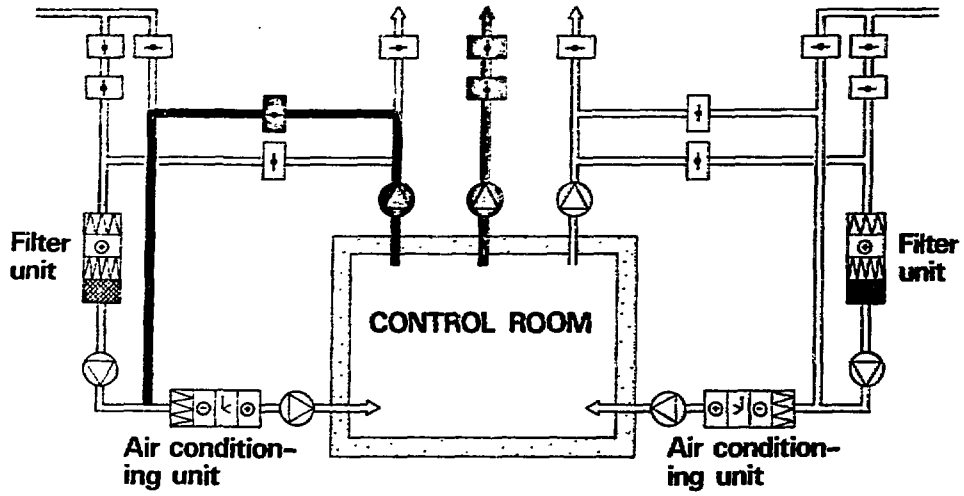
TK 120-4, 6.1977

ASEA-ATOM

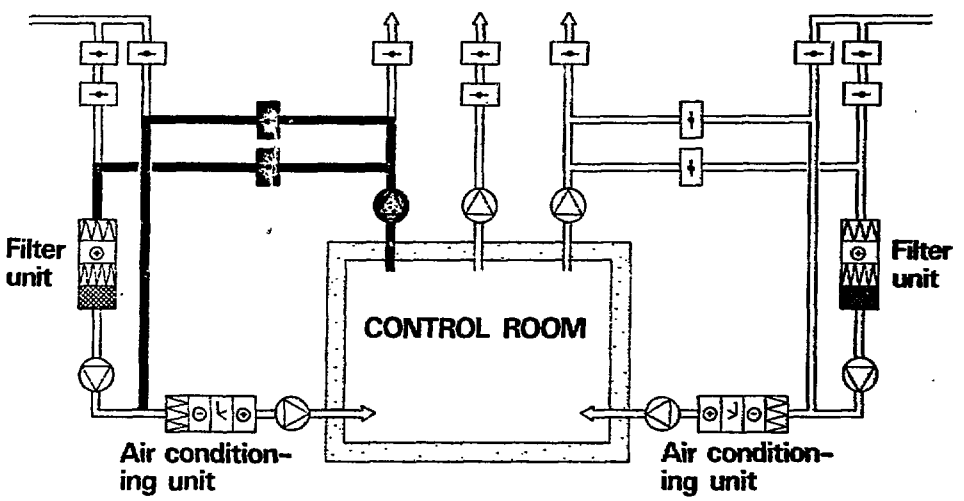
Figure 5

BWR 75 - CONTROL ROOM VENTILATION

Normal ventilation



Control room isolation

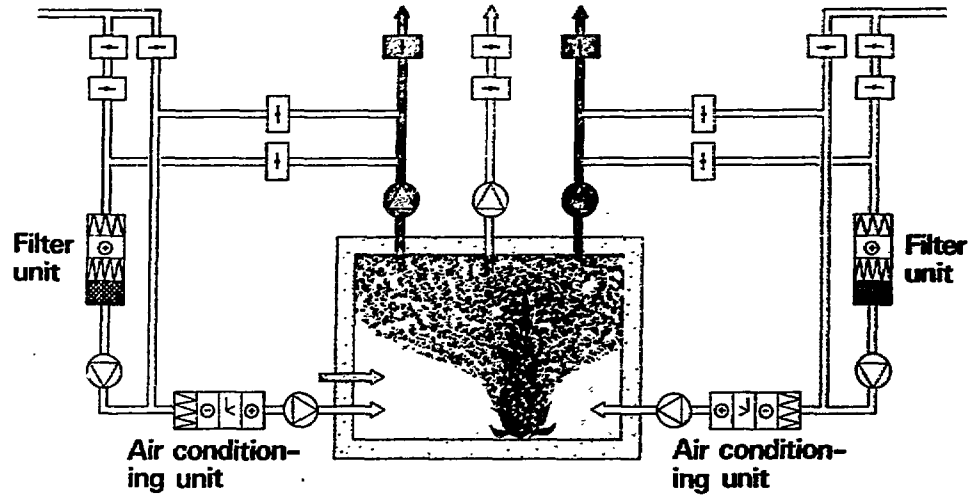


☐ Outdoor air ■ Recirculated air ☐ Not in operation
☐ Treated air ■ Exhaust air

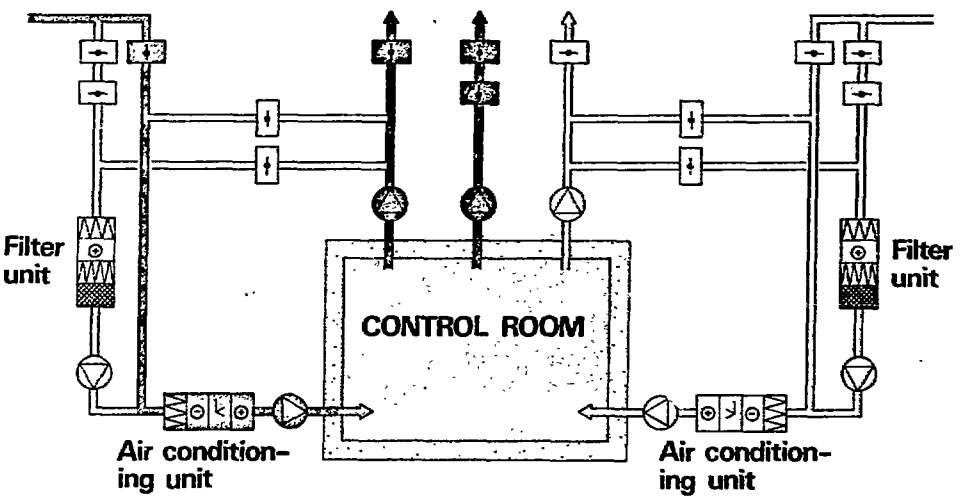
ASEA-ATOM

BWR 75 – CONTROL ROOM VENTILATION

Smoke removal



Cooling with outdoor air



□ Outdoor air ■ Smoke □ Not in operation
▣ Exhaust air

ASEA-ATOM