XA9949686

# ANALYSIS OF THE MONITORING SYSTEM FOR THE SPALLATION NEUTRON SOURCE "SINQ"

E. BADREDDIN
Swiss Federal Institute of Technology (ETH)
Zurich, Switzerland

**Abstract:** Petri Net models (PN) and Fault-Tree Analysis (FTA) are employed for the purpose of reliability analysis of the spallation neutron source SINQ. The monitoring and shut-down system (SDS) structure is investigated using a Petri-Net model. The reliability data are processed using a Fault-Tree model of the dominant part. Finally, suggestions for the improvement of system availability are made.

**Keywords:** monitoring, Petri networks, neuron source, fault tree, reliability

## 1. INTRODUCTION

### 1.1 Brief functional description

Paul Scherrer Institute-Villigen-Switzerland, has built one of the largest spallation neutron sources (SINQ) for research purposes. For the following description please refer to Fig. 1. The proton beam from a low energy source is accelerated to approx. 600MeV by means of a ring-cyclotron. The beam current is approx. 1.5 mA. Different kinds of sensors monitor the vacuum, magnet current, beam profile and ionisation along the transportation path. A number of fast (and slower) acting shutter are activated by the beam shut down system. The main shut-down actuator, however, is the kicker-magnet assembly placed directly after the low energetic source. Finally, the proton beam hits a Zircaloy target in a tank of $D_2O$ for cooling and neutron moderation. The target window is also cooled by another $D_2O$ jacket.

### 1.2 Problem statement

The shut-down of SINQ is formulated as a Two-Time-Scale (TTS) problem as follows (see Fig.2):

a) Fast-Time Scale (FTS): Events which lead to a shut-down for a period of ≤1 month (e.g. short-term vacuum and/or cooling failure).
b) Slow-Time Scale (STS): Events which lead to a shut-down of >1 month (e.g. $D_2O$-contamination of the proton beam transport line or target defects.

Based on the time-scale classification made above, we consider the STS only. Further, we shall concentrate on the $D_2O$-contamination of the proton beam transport keeping target defect events out of the scope of this analysis.

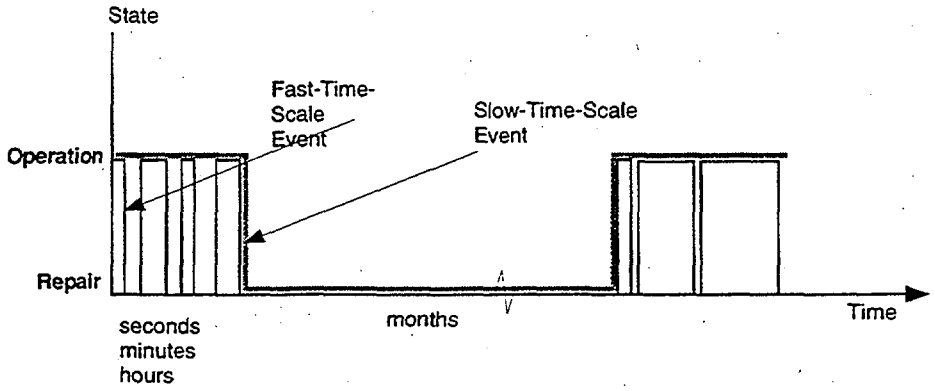
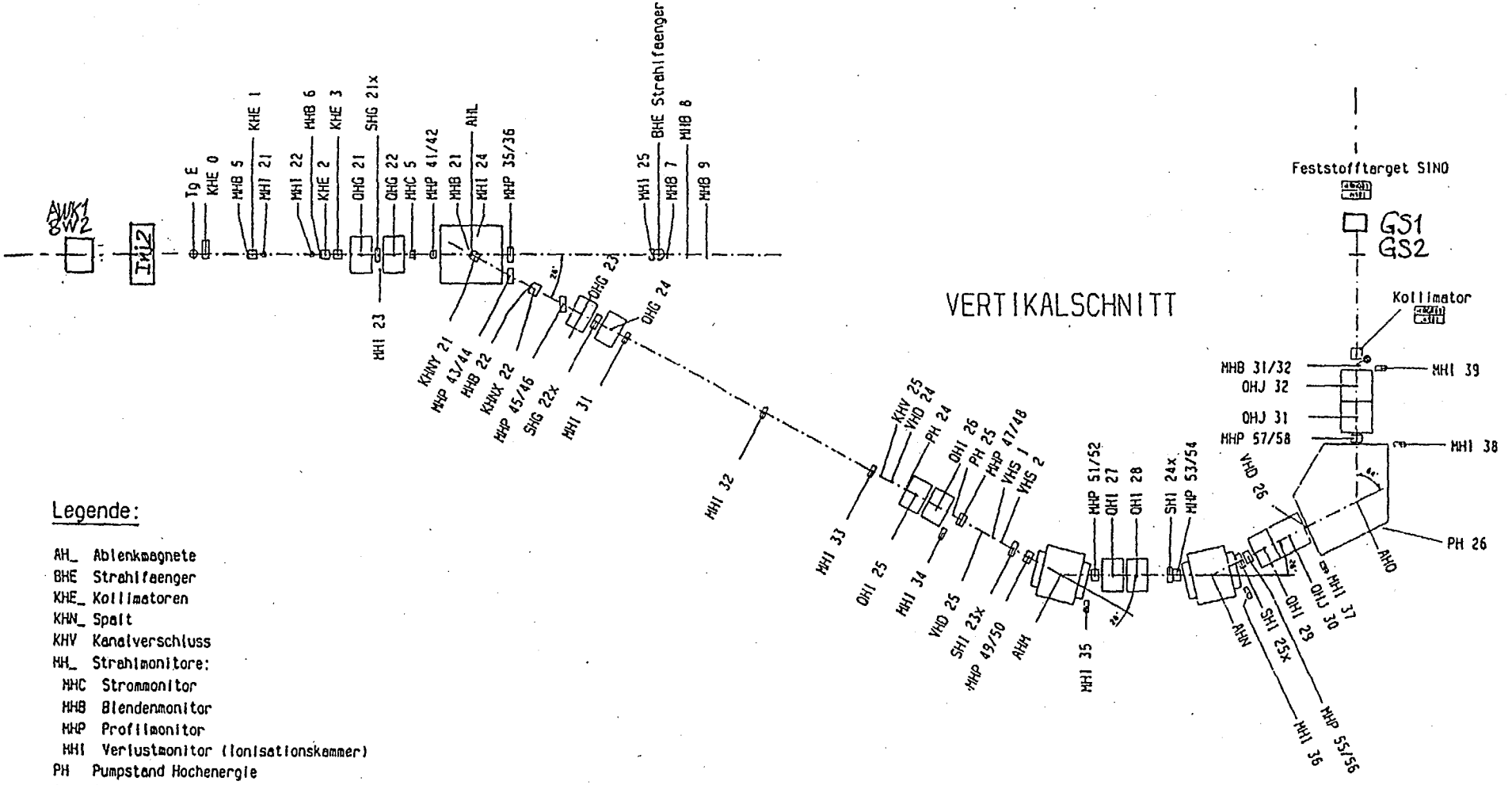



*Fig. 2 Two-time scale events*




## Legende:

AH_ Ablenkmagnete
BHE Strahlfaenger
KHE_ Kollimatoren
KHN_ Spalt
KHV Kanalverschluss
MH_ Strahlmonitore:
MHC Strommonitor
MHB Blendenmonitor
MHP Profilmonitor
MHI Verlustmonitor (Ionisationskammer)
PH Pumpstand Hochenergie
QH_ Quadrupole
SH_ Steuermagnete
TgE Target E
VHS Schnellschluss-Schieber
VHD Durchgangsventil Hochenergie

Fig. 1

| SINQ-Sicherheitsbericht |
| --- |
| SINQ-Strahlfuehrung |
| Strahlopt. relevante Komponenten |

## 2. SOLUTION APPROACH

In this study, we shall also adopt the following general procedure :
a) definition of the system under investigation
b) investigation of the monitoring system through a discrete-event model (Petri Net)
c) qualitative analysis based on the PN-model to suggest improvements
d) quantitative analysis by means of a Boolean model (FTA)

The system under investigation consists of:
• Injector: only as far as the shut-down mechanism is concerned
• Accelerator: only as far as its interlock is concerned.
• Proton beam transport line.
• Target-window: only as far as leakage is concerned
• Electronics and power supplies of the SDS

Based on the documents [1] and [2], a sensor-actuator "Book-keeping" has been made for the purpose of determining the most important pairs involved in the SDS.

### *2.1.1 Sensors*

1) Vacuum pressure sensors GS1&GS2 (redundant)
2) Vacuum pressure sensors GH25&GH26 (redundant)
3) Cooling medium pressure sensors "Eckhardt"
4) Cooling medium temperature sensors PT-100
5) Magnet current-monitors MHC
6) Tritium-monitors
7) Beam monitors (Ionisation MHI and Profile MHP)

### *2.1.2 Actuators*

1) Kicker-magnet (AWK1&BW2): Deflection magnet AWK1 will react in < 1 msec, (700µsec after loss of vacuum the deflection current in the magnet is 90% of its nominal value) when triggered by GS1&GS2.
2) Vacuum shutters VHS1&VHS2: These are fast shutters (< 25 msec, directly triggered by GS1&GS2). They will not withstand the proton-beam but for a short-time (burns-through) and are only partially tight. Therefore, they interrupt both vacuum and proton-transport process only for a limited period of time (~500 msec for a moving shutter; 36 msec for a stationary shutter).
3) Vacuum shutters VHD25&VHD26: These shutters are slower than VHS1&VHS2 (<200 msec until completely closed) and can interrupt the vacuum and proton-beam transport processes for a longer time period (~ 1.0 sec).
4) Accelerator-Interlock

## 3. CASCADE STRUCTURE

The cascade structure is a proven structure for building controllers and monitors. It has demonstrated its robustness through many industrial application. A typical cascade structure is shown in Fig.3. It consists of several **nested** monitoring loops each involving a sensor-actuator pair.

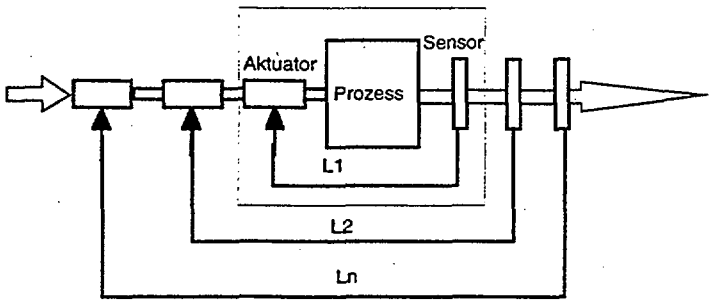



*Fig.3 Cascade structure*

### 3.1 Basic Properties of the Cascade Structure

#### *3.1.1 Time-delay*

The time-delay within a single loop is simply the sum of all individual delays of the process, the sensor and the actuator. For the i-th loop in general, the overall time delay can be computed recursively as:

$$\tau_{i+1} = \tau_i + \tau_{s_{i+1}} + \tau_{a_{i+1}} \quad , \quad i = 1,2,3,\cdots$$

where the suffices s and a stands for sensor and actuator respectively.
Therefore, sensors and actuators employed in the outer loops can be chosen slower than those employed in the inner loops.

#### *3.1.2 Reliability and failure probability*

- Since a loop (not the whole system) fails if either of its sensor or actuator fails, then the failure probability is an **OR**-conjunction of the sensor-actuator pair involved,

$$p_{as} = p_a + p_s - p_a \cdot p_s$$

In other words, a sensor-actuator pair represents two blocks in **series** with the reliabilities $R_s$ and $R_a$ respectively. Then the reliability of the loop can be written as,

$$R_{as} = R_a \cdot R_s$$

- For the nested loops, on the other-hand, an **AND**-conjunction applies since the system fails only if all its loops fail. Under the assumption of independent loop-failure, the overall failure probability can be written as,

$$p_n = p_{n-1} \cdot p_{n-2} \cdots p_2 \cdot p_1$$

In terms of reliability, one can think of the loops as **parallel** blocks. The overall reliability function for 1 out of 2 can be written as,

$$R = R_1 + R_2 - R_1 \cdot R_2$$

In general, the Reliability-function for n-loops can be written as,

$$R = 1 - \prod_{i=1}^{n} (1 - R_i)$$

This means that the reliability increases with the increase of the number of loops.

## 4. PETRI-NET MODELLING

Since the monitoring action takes place in a discrete-event state space, finite-state machines and Petri Nets (PN) are suitable for modelling the SDS. Useful readings on the principles and applications of Petri networks are found in [9], [10]. When ever possible, the processes are modelled using the synchronous-graph class of PN to avoid non-determinism and conflicts.
The PN-model serves several purposes:

a) understanding of the monitoring process (only then, a PN-model can be built) and analysis of the monitoring structure.
b) simulation of the logical discrete-event monitoring behaviour of the SINQ shut-down system (SDS).
c) examination of the monitoring reaction to specific failures (Scenario-generation). This one of the major advantages of using parameteric models.
d) determination of the dominant components and monitoring loops which reduces the effort in a subsequent quantitative analysis (FTA).

In the following, the operational space (in contrast to the failure space in FTA) will be modelled. The PN-model will be built for Type 1 and 2 failure only, i.e., the fast and slow shut-down systems (Schnelles-Abschalt-System SAS and Langsames-Abschalt-System LAS). The PN-model for the overall SINQ monitoring process is shown in Fig.4. The shaded blocks are by themselves processes (subnets).

### 4.1 Structure Analysis

Based on the investigation of PN-model for SINQ-SDS, the following is investigated:
1) Examination of the cascade structure: The monitoring loops are listed hereafter in an inside-to-outside order.
   - 1st-loop for the vacuum process: GS→VHS (+AWK1) : fast (≈ 25 msec)
   - 2nd-loop for the vacuum process: GS→VHD (BW2); slower (≈ 200 msec)
   - 3rd-loop for vacuum process: GH→VHD; slower (≈ 2 sec)
   - 4th-loop for the cooling process: PT100→VHD(+AWK1/BW2); slowest (≈ 90 sec)
   - 5th-loop for vacuum process: GS→AWK1; **fastest** (≈ 1 msec)

We **conclude** that the cascade structure does **not strictly** hold. Although loops 1-4 follow a cascade scheme, the fastest actuator (AWK1) is always activated. The **outer-most** fifth loop is the **fastest** which violates the cascade structure design rules.
In other words, since the fastest loop is the outer-most, all other inner loops do not contribute to the prevention of contamination of the proton-beam transport line.
2) There is no overall loop for the system output (Neutrons):
   This is to point-out that the monitoring is based on secondary processes and not on the main one which is the Neutron production process itself.
3) The proton-beam transport process is monitored using the MHx monitors as sensors and the accelerator interlock as an actuator.
4) The fastest monitoring loop is implemented for the vacuum process. This means that the action will follow **after** a leakage has occurred.
5) The monitoring of the cooling process is approximately three orders of magnitude slower than that of the vacuum process.
6) Importance Analysis:
   a) vacuum-pressure monitors GS1&GS2 build a **dominant** node in the monitoring topology, they are redundant but not diverse and are of the same type.
   b) fast shutters VHS1&VHS2 are mounted are of the same type and not fail-safe.
   c) the individual connections from GS1,GS2 to VHS1,VHS2 are not redundant.

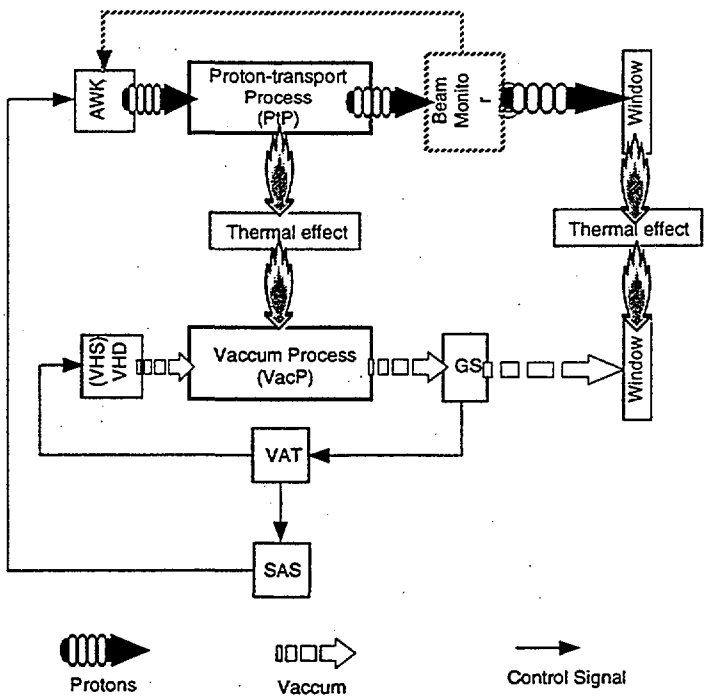
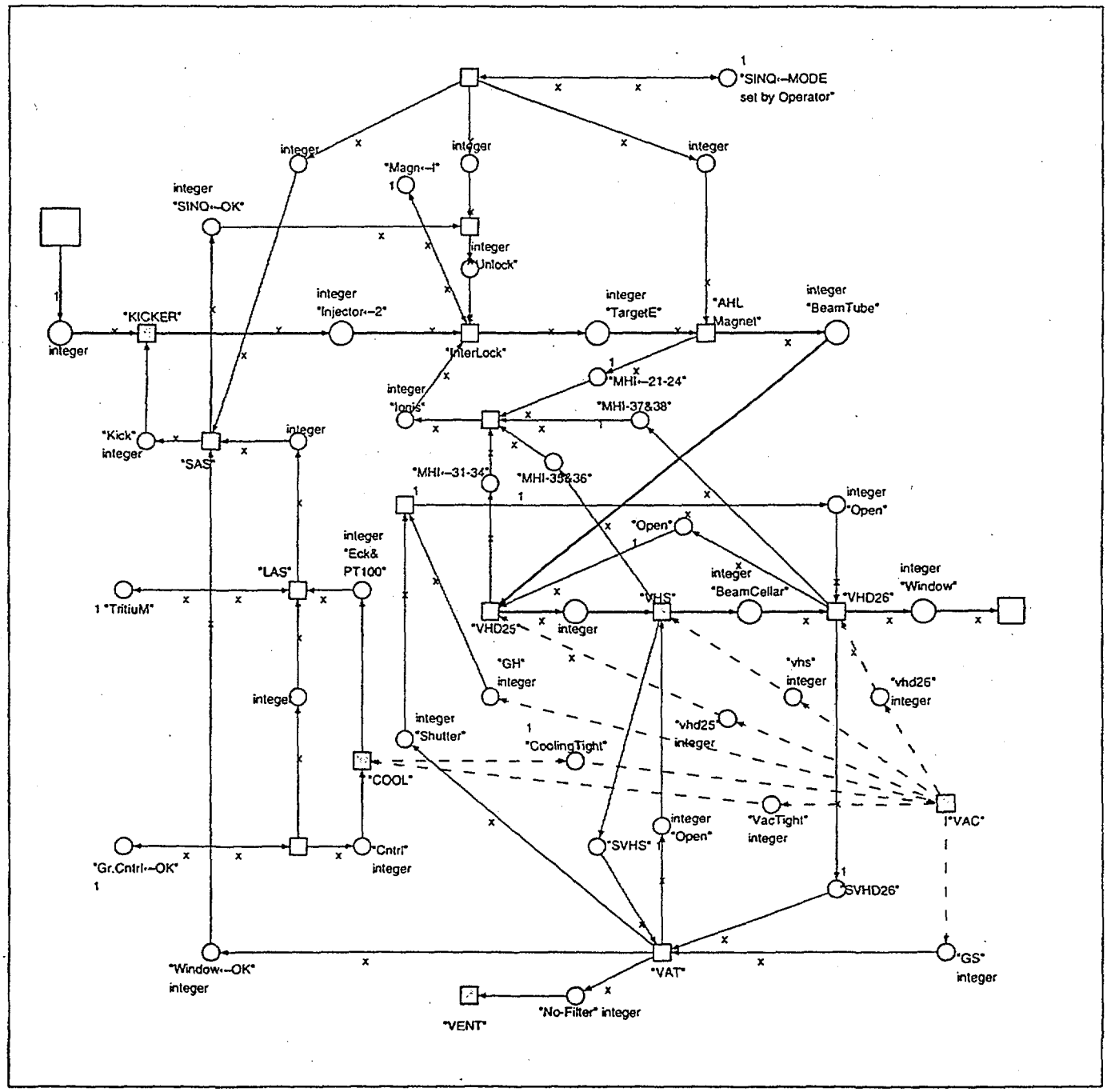



*Fig.5 Enhanced monitoring structure*

# SINQ-Shut-down system

Fig. 4

## ASystem-PP



### 4.2 Enhancement Suggestions

As a result of the system analysis using PN-models, we to monitor the proton-beam transport process itself as a part of the SINQ-SDS (not only the accelerator interlock). This can be done using additional (or the current) beam monitors (MHx) triggering the Kicker-magnet (AWK1). This provision brings-along two **benefits** (refer to Fig. 5):
a) adds a monitoring loop which acts **before** a damage to the target-window occurs
b) adds diversity to the fast monitoring loop of the vacuum process (GS→AWK1)

## 5. FAULT TREE ANALYSIS

For a (serious) $D_2O$ contamination to occur, two things must happen simultaneously:
a) the window must be damaged either due to some mechanical effects or fatigue and/or overheating through a collapsed proton beam and b) the SINQ-SDS must fail.
The two events a) and b) are represented by the two blocks of the Fault-Tree in Fig. 6.

Assuming a $\chi^2$-distribution for the failure, then the *upper bound* for the failure rate can be computed as [8]:

$$\lambda_o = \frac{\chi^2[\nu,(1+\gamma)/2]}{2\sum_{i=1}^{n}\tau_i}$$

where $\nu = 2^{m+1}$ is the degree of freedom with $m$ the number of failures, $\gamma$ is the confidence level, $\tau_i$ is the duration of operation of the $i$-th unit, and $n$ is the number of units.
We assume a confidence level of 0.95.

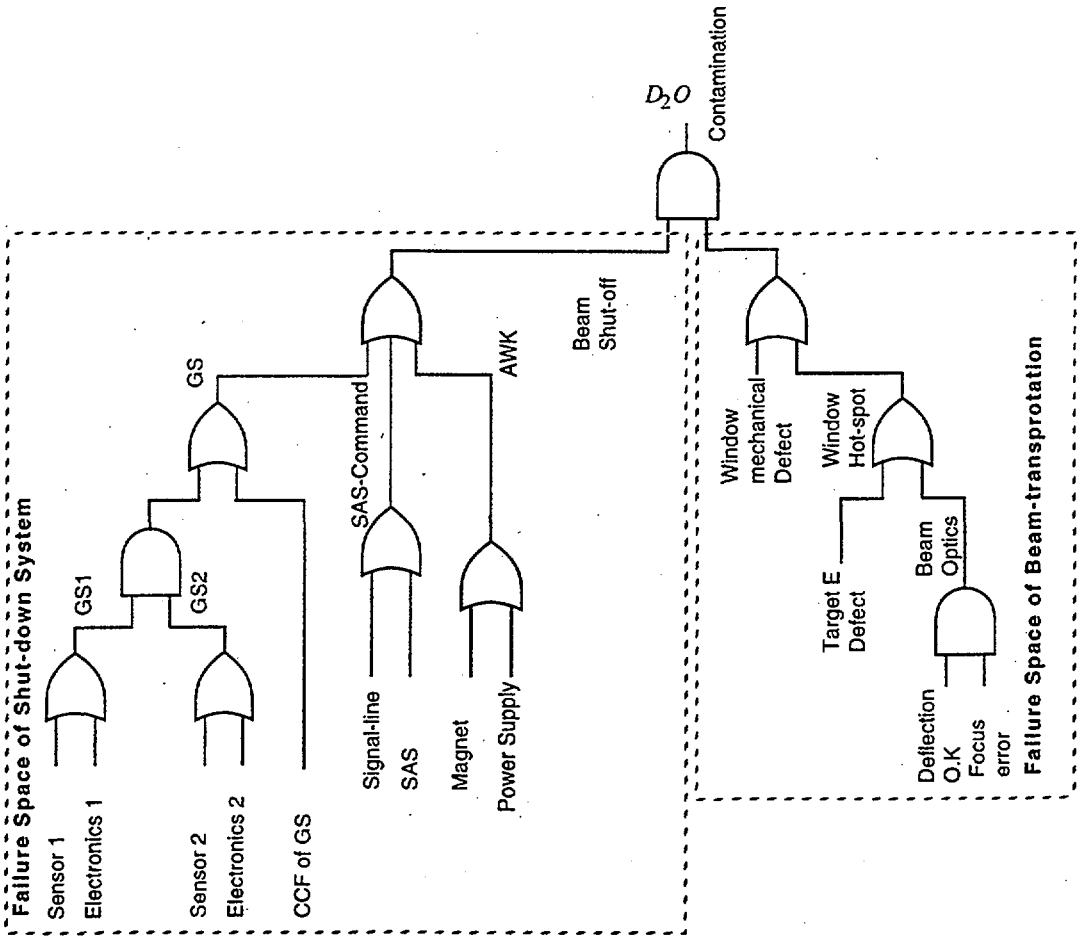



*Fig.6. Fault-Tree with $D_2O$ contamination as a Top-Event*

To use the failure rates obtained from the above formula in the fault tree, the failure probabilities within a time period are to be computed. Assuming a *constant failure* rate, i.e., exponential distribution, the probability that a failure occurs within the time $t$ given that the component is functional at $t$=0 is equal to, $P(\text{failure in time } t) = 1 - e^{\lambda t} \approx \lambda t$

For t = one hour (and 6000 hours per year), the **overall** failure probability of the **shut-down system** is computed as: $P_{sds} = 60.3 \cdot 10^{-6}$ per demand

## 6. CONCLUSIONS AND FINAL REMARKS

In the reliability analysis of SINQ, Petri-net models have been employed to investigate the monitoring structure and to run simulation for the fault propagation. Reduced fault tree models are then employed in the final evaluation of the failure probability.

On the basis of the previous analysis, our conclusions can be summarised as follows:

1) There is essentially a single dominant loop in the SDS, namely GS1&GS2→AWK1. This loop monitors the vacuum process and, therefore, reacts only after leakage had already occurred.
2) The fast sensors and shutters (GS1&2, VHS1&2) involved in this loop are built to meet the principle of redundancy but not diversity.
3) The overall failure probability of the SDS is $P_{sds} = 60.3 \cdot 10^{-6}$ per demand

4) Enhancement to the monitoring system can be made by monitoring the proton beam transportation process.

## REFERENCES


[1] Perret, Ch., "Sicherheitsbericht zur Spallations-Neutronenquelle SINQ am Paul Scherrer Institut (PSI)", Doku. Nr. 814/PC38-1011.A

[2] Heidenreich, G., "Abschaltzeit p-Strahl bei Schliessenden Ventilen VHS1, VHS2", Doku. Nr. 818/HG13-301.-, 8-Feb-93

[3] Braun, R., "Anschluss des Speisegerätes AHL an das Abschaltsystem", Doku.Nr. 837/BR81-301

[4] The Spallation Neutron Source SINQ, PSI, Oct. 1994

[5] Braun, R., "Konzept für SINQ-Abschaltsystem", Doku.Nr. 837/BR81-401

[6] Braun, R., "Vorführung Schnelles Abschaltsystem am 22.5.1996", Doku.Nr. 837/BR81-601

[7] SystemSpecs 2.1 Reference Manual, IvyTeam, July 1994

[8] Zuverlässigkeitskenngrössenermittlung im Kernkraftwerk Biblis - Abschlussberciht- Band2, 1984

[9] Baumgarten, B., Petri-Netze, Grundlagen und Anwendumgen, BI Wissenschaftsverlag, 1990.

[10] Jensen, K., Rozenberg, G., High-level Petri-Nets, Theory and Applications, Springer Verlag, 1991.