KfK 5192
Mai 1993

Proposal of a Concept and Reliability Analysis for a Fusion Plant Magnet Protection System

H. Schnauder, E. Pamfilie
Institut für Reaktorsicherheit
Association KfK-EURATOM
Projekt Kernfusion

Kernforschungszentrum Karlsruhe

Kernforschungszentrum Karlsruhe

Institut für Reaktorsicherheit
Association KfK-EURATOM
Projekt Kernfusion

KfK 5192

Proposal of a Concept and Reliability Analysis for a Fusion Plant Magnet Protection System

H. Schnauder, E. Pamfilie*

* Siemens/KWU Karlsruhe

Kernforschungszentrum Karlsruhe GmbH, Karlsruhe

Kernforschungszentrum Karlsruhe GmbH
Postfach 3640, 7500 Karlsruhe 1

ISSN 0303-4003

Proposal of a Concept and Reliability Analysis for a Fusion Plant Magnet Protection System

Abstract

The unavailability for the current switch down in case of a demand in the magnet coils of a fusion demonstration plant must be decreased by a few orders of magnitude as compared to the one of experimental facilities. The safety requirements to prevent initiation of event sequences which might lead to the release of radioactivity and energy by the plant must be fulfilled with the same standards as applied in a normally applicable plant. On the basis of this proven technology a general usable magnet protection system will be proposed, which achieves some considerable improvements in the failure detectability as compared to the conventional protection systems. It will be demonstrated by fault tree analysis that the principal demands on safety can be satisfied by that approach. The improvements are achieved by the use of an additional microprocessor supported system for failure detection without being used for initiation of any safety related actions. An influence on a safety action by the additional system therefore is excluded.

Konzeptvorschlag und Zuverlässigkeitsanalyse für ein Fusionsanlagen-Magnet-Schutzsystem

Kurzfassung

Die Nichtverfügbarkeit der Stromabschaltung in den Magnetspulen bei Anforderung in einer Demonstrations-Fusionsanalage muß, gegenüber den Experimentieranlagen, um mehrere Größenordnungen reduziert werden. Die Sicherheitsanforderungen zur Vermeidung der Auslösungen von Ereignisabläufen, die zur Freisetzung von Energie und Radioaktivität führen, sind mit den gleichen Maßstäben zu beurteilen wie bei den existierenden Anlagen. Auf der Basis dieser erprobten Technologie wird ein allgemein einsetzbares Magnet-Schutzsystem vorgeschlagen, das gegenüber den vorhandenen Schutzsystemen über eine wesentlich gesteigerte Fehlererkennungs-Fähigkeit verfügt. Anhand einer Fehlerbaum-Analyse wird der Nachweis erbracht, daß die grundsätzlichen Anforderungen erfüllt werden. Die Verbesserungen basieren hauptsächlich auf einem zusätzlichen, mikroprozessor gestützten System zur Fehlerdetektion, das aber selbst keine Sicherheitsaufgaben wahrnimmt. Eine Einflußnahme auf eine Sicherheitsaktion ist ausgeschlossen.

Content **Page**

Introduction

Reliability analysis of a current switch down in case of a demand in the magnet coils of the large experimental facilities results in unavailability values in the order of magnitude of 10^{-3} per demand. The safety relevant risk connected with non switch down is relatively low, and is mainly related to damage of the experimental facility. Radioactivity is not involved, so that a radioactivity release is excluded from the beginning.

This situation will change in case of e.g. ITER. On the one hand the possibility of an energy release is much higher, because of the high amount of energy handled and stored. On the other hand the possibility of a radioactivity release mainly by the Tritium (T) and contamination of highly loaded parts of the plant cannot be neglected. These risk factors require precautions according to the ones in conventional fission energy generation technology *(state of the art).* The values of unavailability for interruption of the energy production process in case of a demand in the worst case, are there in the order of magnitude of 10^{-6} to 10^{-7} per demand or even lower. A probability for damage of the plant and contamination of the neighbourhood is not to be neglected in case of fusion. The safety precautions for a fusion plant shall be similar to conventional nuclear plants, therefore, operational experience for fusion plants which forms the basis for actual safety evaluations is necessary.

Three levels of precautions contribute mainly to a high level of safety standards.

1. The plant protection system must be a fully independent autonomous system in relation to the operation system. The signal generation and signal processing of a plant protection system must not be influenced by other systems.

2. The design and the lay-out principle for achieving sufficiently low unavailability values are *redundancy* and *diversity.* This holds also in the safety equipment as well as in the working principles of the measuring and processing equipment and in the process variables itself. This is a very strict requirement and can only be achieved with a high amount of precautions.

3. An effective quality assurance (QA) system including administrative precautions need to be established.

System description

One can proceed from the working hypothesis, that a protection system in a fusion facility should follow the same safety demands and precautions that are valid in a conventional fission power plant. Therefore the regulations established by the Nuclear Safety Standards Commission *(Kerntechnischer Ausschuß (KTA))* in that field will be briefly described. Fig. 1 gives an example of the functional design of a protection system [1].

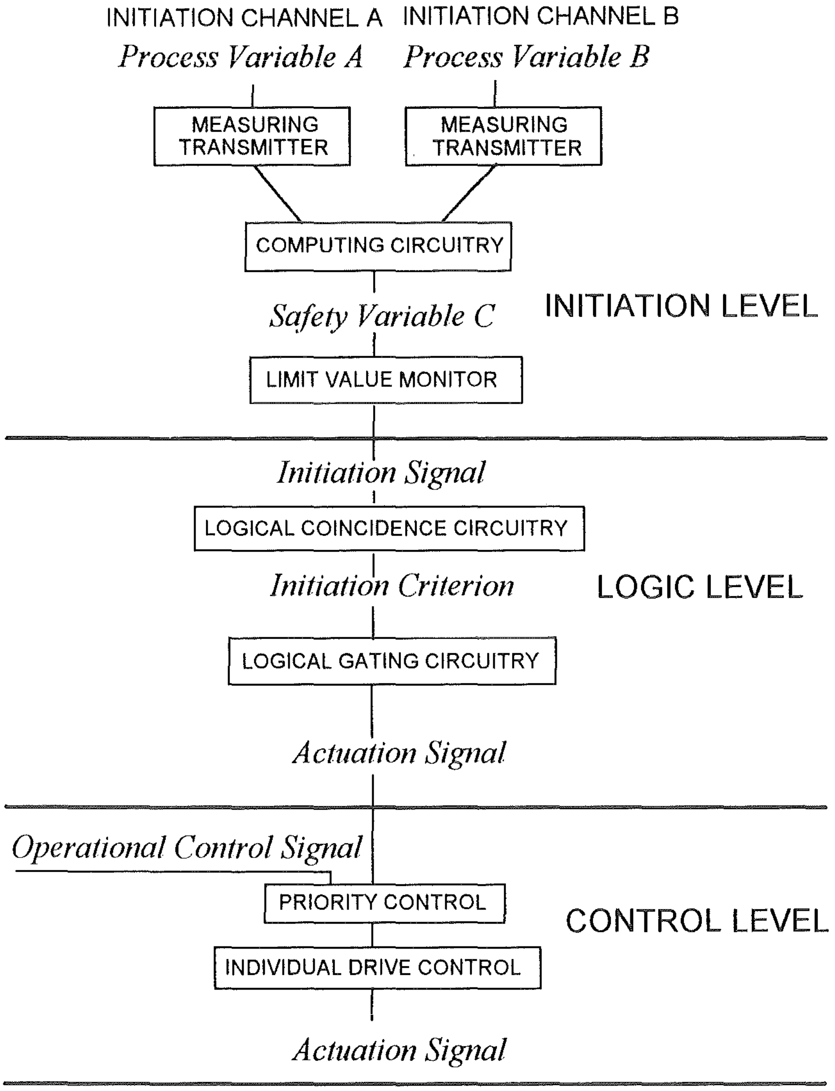


Fig. 1 Definitions in the protection system according to the Nuclear Safety Standards Commission (KTA) Regulation KTA-3501 [1]

The system can be divided into three functional levels.

1. The initiation level is responsible for the signal generation of the safety relevant process variables to process a safety variable. A limit value of that safety variable is a criterion for further actions and transmitted as initiation signal to the logic level. This process is always performed with a high degree of redundancy.

2. In the logic level these redundant initiation signals will be compared with initiation criteria (according to the 2 out of 3 or 2 out of 4 principle). If a particular criterion is fulfilled an actuating signal is given to the control level.

3. On the control level, the actuation signal can be overruled by an additional priority control. This is necessary because on demand of several safety actions a priority ranking must decide about the highest priority. The output will be an actuation of a safety action.

The reference [1] prescribes, that this signal generation and signal processing pertaining to the protection system has to be completely independent from other signals and other systems, e.g. the normal operation system.

A plant protection system according to these safety regulations *(as also used in the conventional fission reactor technology)*, but with additional capabilities will be recommended for fusion plants The principle of the design is given in Fig. 2.

The basic concept is, that the plant protection system is independent from the plant operation system as already pointed out. The plant protection system itself is part of a global safety system which also contains active and passive safety precautions. Active safety precautions are, e.g. safety valves or safety switches etc. Passive safety precautions are, e.g. layouts, limitation of power ratings and others. The active and passive precautions are dependent on the design in detail but in the present early design phase not part of the considerations.

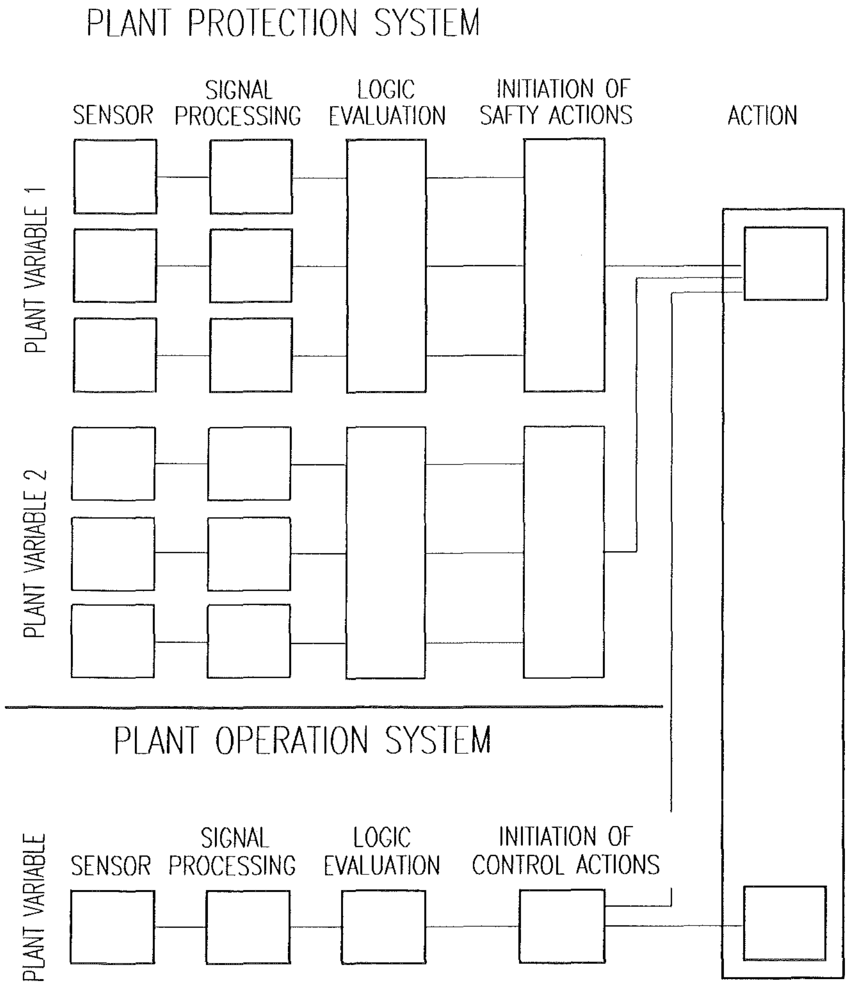
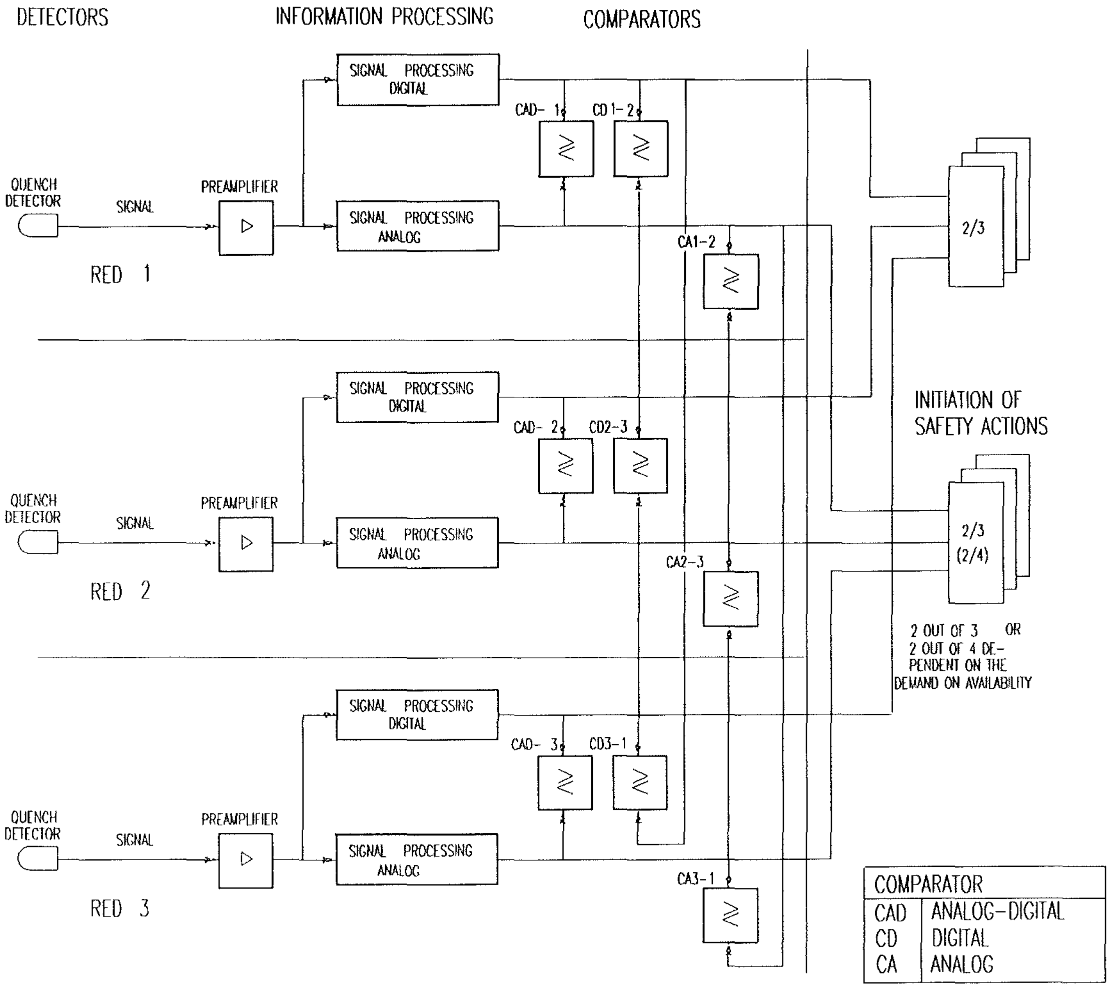


FIG. 2 PRINCIPLE OF THE PLANT PROTECTION SYSTEM

The principle of the protection system for a selected initiation criterion, e.g. a



COMPARATOR	
CAD	ANALOG-DIGITAL
CD	DIGITAL
CA	ANALOG

FIG.3 PROTECTION SYSTEM FOR A CERTAIN INITIATION CRITERIA (QUENCH)

quench, is given in Fig. 3. A quench is the transition from the super conducting state to the normal conducting state in a magnet coil. The quench as an initiation criterion is selected as a representative example. The system under consideration is of common interest for all of the safety relevant events in a fusion plant, e.g. switch down of the current in a neutral beam injector (NBI) etc.

Back to the reference example. One of the plant variables for quench detection in a super conducting magnet system is the current in the conductor coils. An abnormal change of the current is a measure for the quench. This current will be permanently monitored by detectors. The resulting analog signals will be amplified and processed in redundant analog processing units. Independent single failures in the measuring and in the processing channels will be supervised by comparators arranged between the redundant channels. In case of a signal difference of a few % an alarm signal is generated.

In this arrangement each channel is controlled by two comparators. The individual signal is also surveyed by limit values. In case of exceeding a limit value an initiation signal according to the description in Fig. 1 is transmitted to the logic part of the system. The analog part of the signal processing is identical to the conventional protection system according to [1]. The advantage is, that the essentially fix wired system possesses a very low unavailability in case of a demand. The disadvantage is, the system is only able to supervise minimum or maximum values, respectively. The values could also represent gradients or values dependent on other parameters, but it is always a single value. The necessary precautions against the Common Mode situation are very demanding and mainly based on administrative precautions and an extensive quality assurance.

One of the most serious Common Mode failures in the protection system, is the miscalibration of redundant measuring channels, because there is a large influence by the human activity involved which is very difficult to quantify. This Common Mode problem is discussed more in detail in the Appendix A. The problem of Common Modes caused by human actions was also a dominating part in the considerations of WASH-1400 [2] and the results are will be incorporated.

A new feature in the present concept is an additional microprocessor based signal processing in every redundant channel. The problem of using microprocessors in safety systems arises from the difficulty to guarantee the required level of reliability. If however the system is not used for initiation of a safety action but for error detection only, the reliability in view of the Common Mode problem may be improved in an acceptable manner. This is recommended in the case under consideration.

The system can be mainly used for:

- Detection of Common Modes
- Detection of plant conditions which show a tendency towards a fault or critical situation
- Detection of dependent failures
- Detection of sensor failures by on line failure tests

Especially the last point is a new feature in error detection. The basic idea is, that the signal behaviour is known in nearly every state of operation. Therefore it is possible to test whether or not the signal is in the range it should be according to the state of operation. Also during shut-down phases of the plant most of the sensors generate an output, e.g. noise or background, where the signal level is definitely known and can be used for error detection.

As shown in Fig. 3 there are comparators between the analog and the digital part of a measuring channel or redundancy. This precaution is especially intended for the detection of Common Mode failures between the diverse signal processing channels. According to the conventional analog system there are also comparators between the digital parts of the channels for detection of differences between the digital processing channels.

The output from the digital signal processing unit can be assessed according to the different logic principles. But as already pointed out, they can not be used for initiation of a safety action yet. At the present time it must be left open if this will also be the case in the future. There is a working group in the Nuclear Safety Standards Commission, to find an answer to the question, under which conditions the use of microprocessor sup-

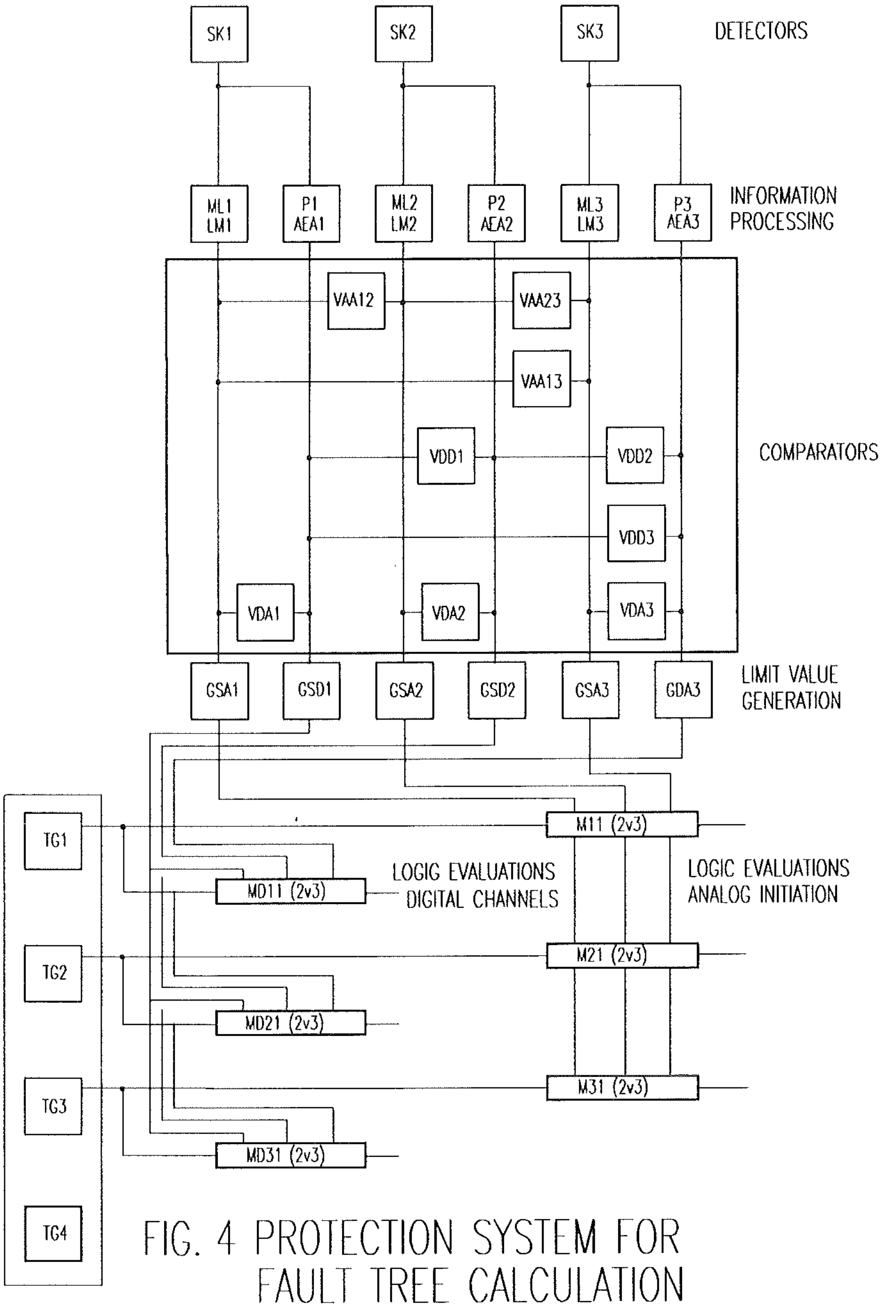


FIG. 4 PROTECTION SYSTEM FOR FAULT TREE CALCULATION

ported systems could be accepted for safety actions.

Fig. 3 shows the principle, how the system can be realised on the basis of the already proven technology, and being available in a 2 out of 3 lay-out. This configuration is also the standard example for the previous reliability analysis and can be seen as representative for the system in general. The system analysis is performed on the basis given in the Fig. 4. The basic or reference safety action is the detection of a quench and the subsequent initiation of a current switch down upon demand. In case of other safety actions the part of the measuring channels located prior to the comparators can slightly differ. In Tab. 1 the components and the failure modes are listed.

Tab. 1 Components and failure states

Component n=1,2,3	**States**	**Name of component**	**Failure description**
LM_n	1 2	Log. amplifier	Signal to low Signal = const
GSA_n GSD_n	1	Trip amplifier	no reaction
VG_n	1	Comparator	no reaction
M_n MD_n	1	Magnet core element	no reaction
AG_n	1	Terminating unit	no reaction
P_n	1 2	Processor unit	Hardware failure Software failure
ML_n	1	Cable, support	Interrupt
AEA_n	1	Analog input unit	no reaction
SK_n	1	Detector	Signal to low

Fault trees

For different TOP-events *(TOP is the top of the fault tree)* the unavailability values will be analysed in relation to the reference event, the quench.

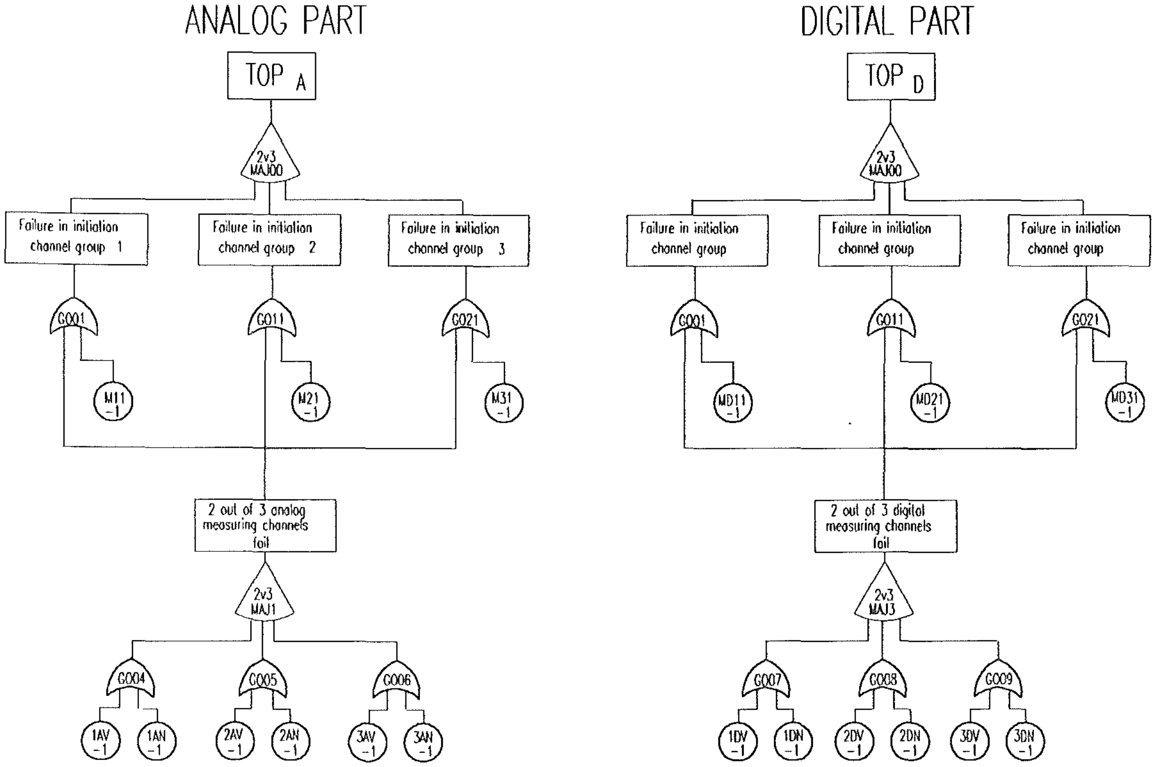

ANALOG PART
TOP A
2v3 MAJ00
Failure in initiation channel group 1
Failure in initiation channel group 2
Failure in initiation channel group 3
G001
G011
G021
M11 -1
M21 -1
M31 -1
2 out of 3 analog measuring channels fail
2v3 MAJ1
G004
G005
G006
1AV -1
1AN -1
2AV -1
2AN -1
3AV -1
3AN -1
DIGITAL PART
TOP D
2v3 MAJ00
Failure in initiation channel group
Failure in initiation channel group
Failure in initiation channel group
G001
G011
G021
MD11 -1
MD21 -1
MD31 -1
2 out of 3 digital measuring channels fail
2v3 MAJ3
G007
G008
G009
1DV -1
1DN -1
2DV -1
2DN -1
3DV -1
3DN -1

FIG. 5 FAULT TREE FOR THE SHUT DOWN ACTION INITIATED BY A QUENCH SIGNAL AS A TYPICAL INITIATION

TOP_A is the unavailability of the initiation of a current switch down upon demand for the classical analog part.

TOP_D is the unavailability calculation for only the digital part of the system. As already pointed out this part of the system cannot be used for the initiation of a safety action. Therefore the result has to be considered with caution, as will be discussed later on.

TOP_1 is the unavailability of the detection of one independent single failure in the alarm signal generation, analog and digital part included.

TOP_2 is the unavailability of the detection of an independent single failure in the alarm signal generation only for the digital part. This TOP event is also valid for the analog part because of the identical failure data.

TOP_3 is the unavailability for the case that an error in the alarm signal generation in either the digital or the analog part of one redundancy will not be discovered.

The components used in the fault tree calculation are listed in Tab. 2. For the signal generation and signal processing part the components from Tab. 1 are combined according to their location in reality in the portions, failures before and failures after the comparators. The comparators themselves can never prevent a demanded initiation signal. The comparators only play a role in error detection. The concentration of the number of single components to component groups allows a very high degree of simplification of the fault trees. Fig 5 shows the fault trees for the two TOP-events TOP_A and TOP_D. The shape of both of the fault trees is identical. The difference is in the basic events, which in the one case only contains the analog part, in the other case only the digital part of the system.

In the analysis only those undetected components or component failures are included which can prevent, in case of a demand, an initiation of a safety action. It is assumed, that all other component failures will be detected by the system and can be repaired in a few hours. The comparator failure do not play any role in view on the TOP-events TOP_A and TOP_D.

The fault trees for the TOP-events TOP_1 and TOP_2 for non detection of a failure in the alarm system are given in the Figs. 6 and 7. In this case the comparator failures are the dominating events.

In case of Fig. 6 each channel, analog as well as digital in one redundancy, is controlled by 3 comparators, e.g. analog channel one by VDA_1, $VAA_{1,2}$ and $VAA_{1,3}$ and digital channel one by VDA_1, VDD_1 and VDD_3 etc. That means, *each redundancy* will be controlled by 5 comparators. Comparator VDA_1 is active in both channels, analog as well as digital, of a channel group. This is a configuration which should lead to a high availability concerning error detection.

Fig. 7 shows the fault tree for the case *(TOP_2)* in which only the digital part of the system without assistance from the analog part is responsible for error detection. The same fault tree is also valid for the conventional part of the analog system, based on the assumption that the same version of comparators is used in the analog and in the digital part. That means no diversity of the comparators, which possibly should be avoided in the final design. But this question must be left open until a detailed analysis at a later state of the project is performed.

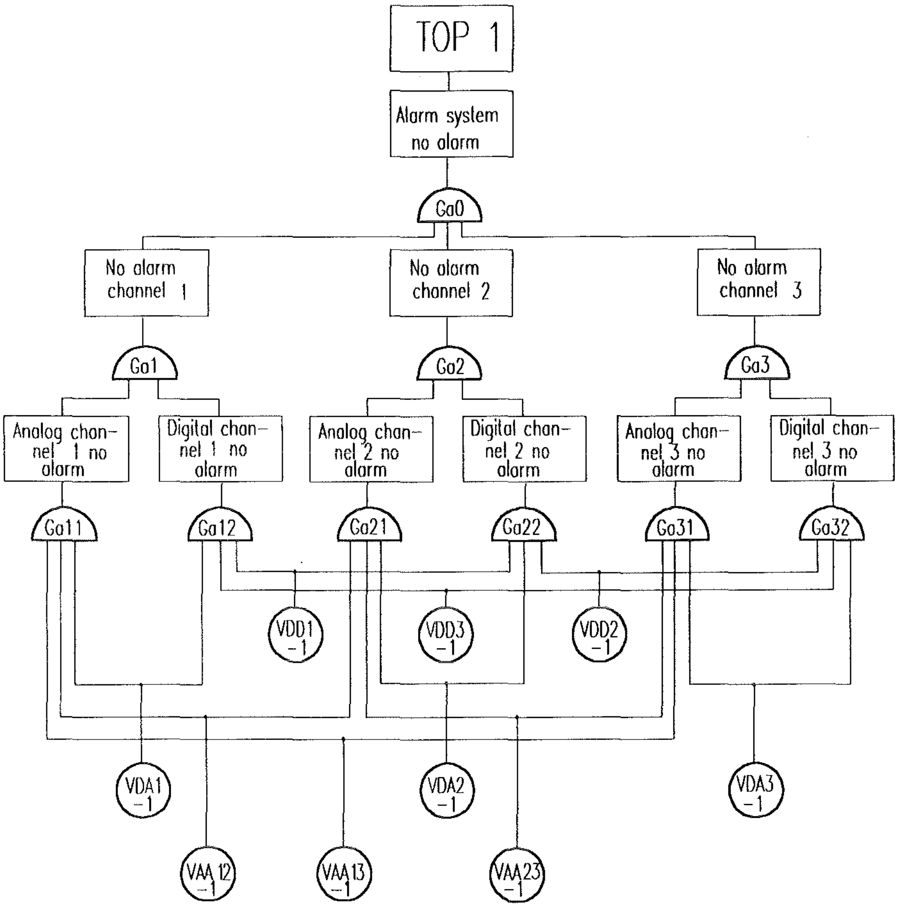


FIG. 6 FAULT TREE FOR ERROR DETECTION IN ALARM SIGNAL GENERATION (DIGITAL AND ANALOG)

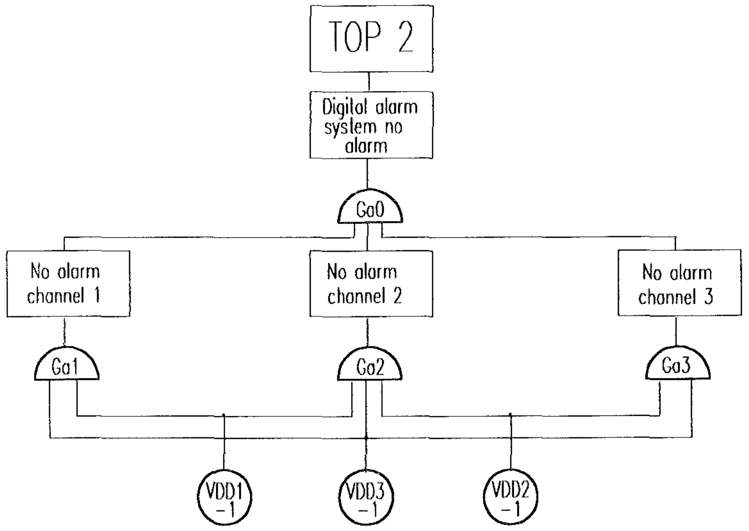


FIG. 7 FAULT TREE FOR ERROR DETECTION IN ALARM SIGNAL GENERATION IN THE DIGITAL PART OF THE SYSTEM

Tab. 2 Failure rates and failure states for the components

Component
n=1,2,3
j=1,2,3
	State	Failure rate [$\cdot 10^{-6}$/h]	Repair time [h]	Description of failure state

AV_n	1	10	5	Analog initiation channel before comparator failure
AN_n	1	0.017	8760	Analog initiation channel after comparator failure
DV_n	1	7.33	8760	Digital initiation channel before comparator failure
DN_n	1	0.017	8760	Digital initiation channel after comparator failure
$M_{n,j}$ $MD_{n,j}$	1 1	0.003 0.003	8760 8760	Magnet core element failure
VAA_n	1	0.004	8760	Comparator A-A failure
$VDA_{n,j}$	1	0.004	8760	Comparator D-A failure
VDD_n	1	0.004	8760	Comparator D-D failure

The TOP-event TOP_3 is defined by:

$$TOP_3 = \{VDD_n\} \wedge \{VDA_n \vee VAA_n\}$$

and is valid only for one redundancy. That means it occurs three times in a system. The index *n* represents the respective redundancy, according to the three independent redundant channels of a channel group.

Results of the analysis

The results of the analysis are given in Tab. 3. The unavailability for the TOP_A, of the protection system, the classical analog system, is evaluated as $1.2 \cdot 10^{-7}$. This value is also the probability that the initiation of a signal for a safety action upon demand is not generated. The initiation signal is not available due to failures in the protection system. This is the order of magnitude expected and accepted for the layout. Here one has to keep in mind, that all other events, the events not influenced by the protection system, are of no interest in view of the analysis.

Tab. 3 Results of the fault tree calculation

Event	**Unavailability values [per demand]**
TOP_A	$1.2 \cdot 10^{-7}$
TOP_D	$1.1 \cdot 10^{-2}$
TOP_1	$7.0 \cdot 10^{-36}$
TOP_2	$3.7 \cdot 10^{-9}$
TOP_3	$2.4 \cdot 10^{-9}$

Fig. 8 shows the block diagram for the analysis. In the upper part of the diagram the combinations of the *expected unavailability values* of the different components are given. Each horizontal combination represents a failure of the whole system in case of a demanded safety action.

The lower part of the diagram contains the *failure probabilities*. Values in the horizontal lines, are multiplied, since they represent AND combinations, while the results of the lines will be added, which represent OR combinations.

The diagram shows where the influences of the individual components to the overall unavailability comes from. The minor influence comes from the combinations of the magnet logic elements, e.g. $M_{n,j}$ and $MD_{n,j}$. These are the elements responsible for the logic evaluation on the logic level. The combinations are in the lower part of the diagram, marked by a separate dashed box. Their unavailability value of $2 \cdot 10^{-9}$ is only 1.7 % of the overall unavailability.

The combinations of the analog part prior to the comparators AV_n contribute about 6 %, the combinations between AV_n and AN_n, the combinations prior to and after the comparators, about 37 % and the combinations of AN_n alone after the comparators, have the largest impact on the result, i.e. they contribute with about 55 %. As the failure rate of the components AN_n is very low, the detectability of failures is also low. It is assumed that a detection of a failure occurs only during the service inspection, which normally takes place once a year. During the normal test, that type of failure can not be detected because it simulates a faultless system.

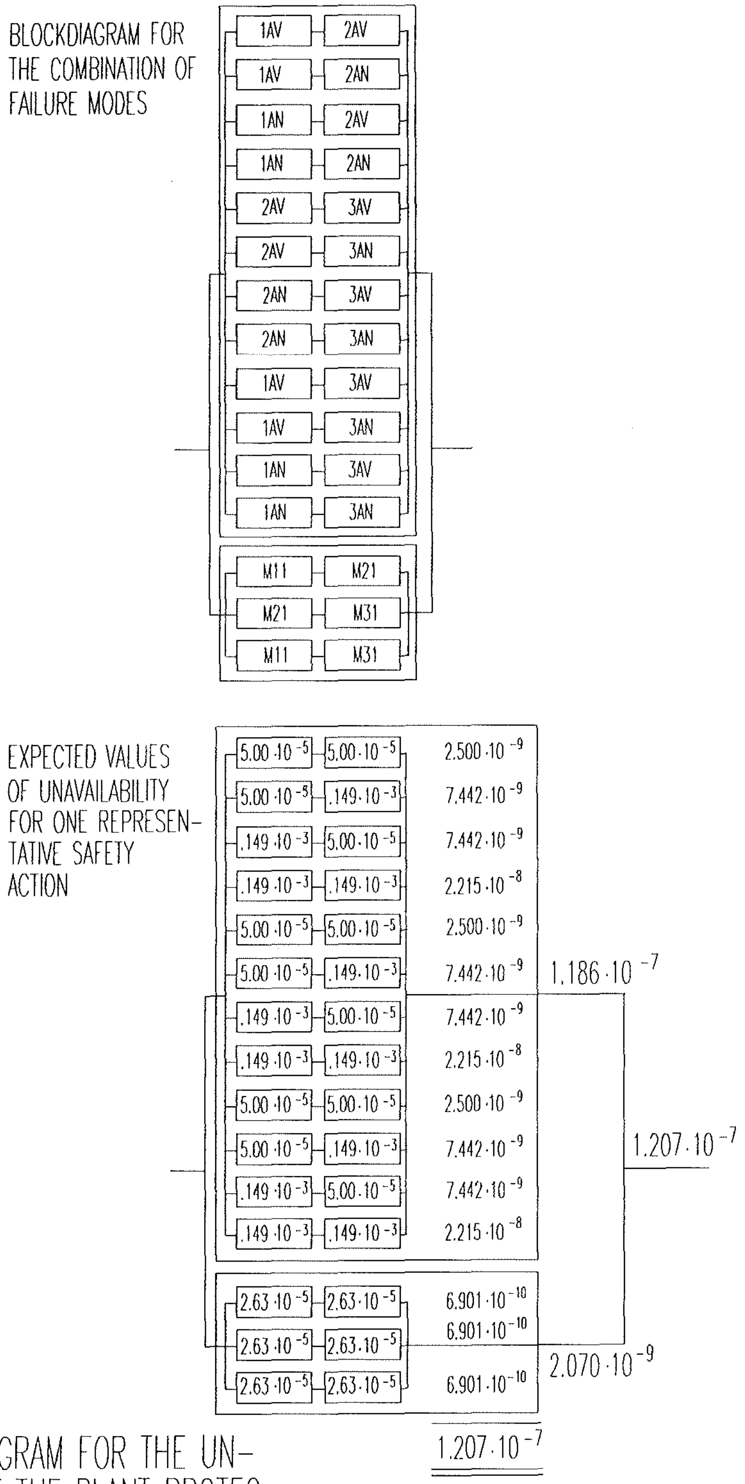


FIG. 8
MAIN BLOCKDIAGRAM FOR THE UNAVAILABILITY OF THE PLANT PROTECTION SYSTEM IN CASE OF A REPRESENTATIVE SHUT DOWN INITIATION

The unavailability of the digital part of TOP_D is, as expected, a few orders of magnitude higher namely $1.1 \cdot 10^{-2}$. This value is dominated by the result of the failure probability of the microprocessor system. The block diagram is given in Fig. 9. It has the same structure as Fig. 8.

The difficulty arises from the fact, that there are a few errors, which are not detectable by systematic tests. As already pointed out, the unavailability will be influenced by the failure detectability, expressed by the mean time to repair (MTTR), remember the product repair rate times MTTR is the expected unavailability value. The high value of the unavailability for the components nDV determines the result of the overall unavailability of $1.1 \cdot 10^{-2}$ per demand.

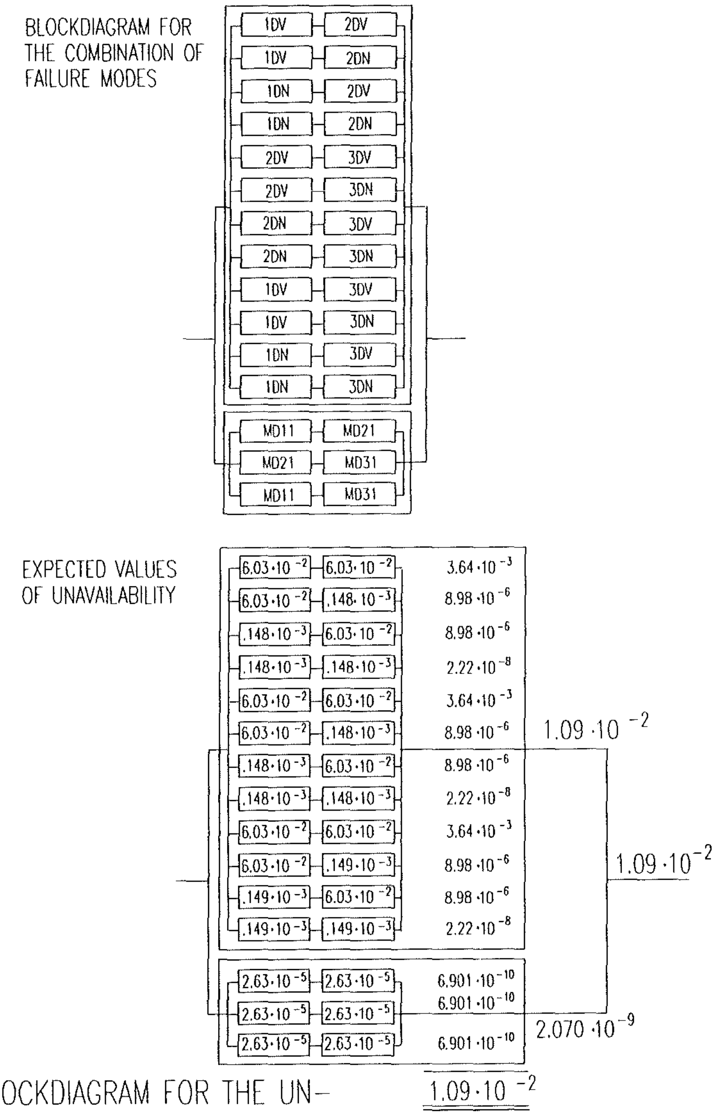
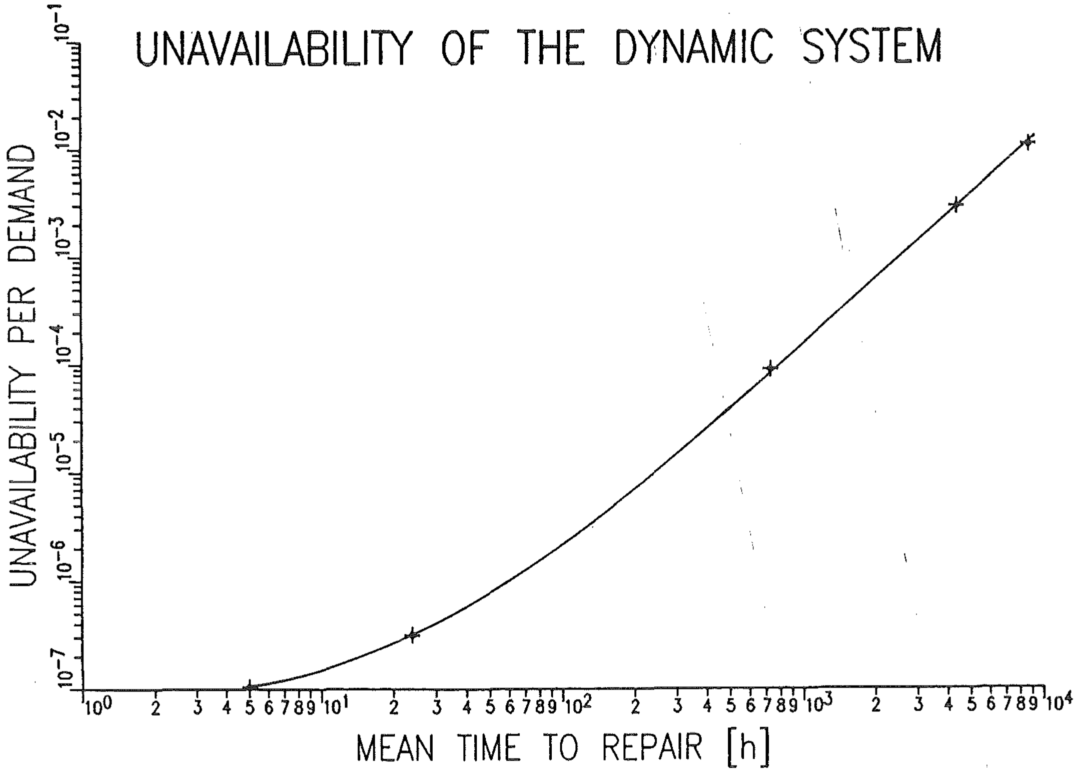


FIG.9 MAIN BLOCKDIAGRAM FOR THE UN-AVAILABILITY OF THE DIGITAL PART SYSTEM

Fig. 10 shows the influence of the MTTR on the unavailability upon demand. A reduction of the MTTR from 1 year to 1 month will result in a reduction of the overall unavailability by the factor $1.2 \cdot 10^{2}$. This shows evidently the influence of the failure detectability. A reduction of the MTTR to 1 week brings the unavailability even down to about $5 \cdot 10^{-6}$. That means by adequate precautions, there is still a potential for improvements in the system reliability.

It is evident that a reduction of the failure rate of the microprocessor system will lead to the same improvements. A combination of both effects would probably be the most desirable solution.



As already pointed out, the comparators are without any influence on the initiation of a safety action. They will be used for error detection in the analog as well as in the digital part of the measuring channels and in the signal processing in the part of the system before the limit value control. According to Fig. 1 that is the initiation level.

The unavailability values for non detectability of an error, in the case of an error, is also given in Tab. 3. The value which results for $TOP_1 = 7 \cdot 10^{-36}$ for independent single failure is very low and is more of academic nature. It shows however, that there is sufficient margin for uncertainties.

TOP_2 represents the unavailability of error detection in the analog as well as the digital part independent of each other. The value is calculated to be $3.7 \cdot 10^{-9}$.

The unavailability for the TOP_3 is calculated to be $2.4 \cdot 10^{-9}$. This is the unavailability for the individual channels in one redundancy, i.e., either the analog or the digital part. Based on the assumption, that the two different measuring and processing channels are diverse in the lay-out, the TOP-event can be set equal to the result of TOP_3 for the Common Mode risk.

Conclusions

The advantage of the protection system under consideration compared to the conventional systems is the improvement in the failure detectability. New in the present system is the on-line testability of the measuring chains including the sensors and the high safety against Common Modes. The on-line test is based on the assumption that the sensor signal level is known and can be tested during each shut-down and during the operating phase. The high reliability for the initiation of a safety action is based on the proven classical technology. Further improvements in the failure detectability will be achieved by combination with a microprocessor supported new digital system. The transfer of safety functions to the digital microprocessor system is not considered here. According to the current safety regulations this would not be accepted due to problems in the proof of digital systems reliability. This might change, however, in the future.

The protection system was designed to cope with the reference event, the quench. But it is quite obvious, that the basic concept of the system is also applicable for initiations of safety actions in general in a fusion power plant.

References:

[1] KTA 3501, Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen, Sicherheitstechnische Regel des KTA, Fassung 10/80, Carl Hanser Verlag KG, Köln

[2] WASH-1400, Reactor safety study; An assessment of accident risk in U.S. commercial power plants, (NUREG 75/014), Appendix 2: Fault trees, PB-248-203 (Oct. 75), Appendix 3 and 4 : Failure data, PB-248-204 (Oct. 75)

[3] A.D. Swain, H.E. Guttmann; Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278, Oct. 80

[4] A.D. Swain; Effects on human performance on nuclear power plant operations, Seminar, Garching 28 to 30 Nov. 1980

Appendix A

The Common Mode problem

Common Modes in the analog or in the digital part of the system will be detected by the comparators in between the two systems. One open point is a Common Mode in the comparators (*VDA according to Fig. 4*). If that cannot be prevented from the beginning, for their diversification might become necessary. But this is not a major problem. At present this question will be left open.

Keeping the risk acceptably low in this domain is still very important and is a dominating part of safety discussions, in relation to power stations in general.

In the handbook of the human reliability [3], which is one of the references for the present considerations, the problem of dependencies of different degrees in view of human actions is the most important part of [3].

The occurrence probability for Common Modes in the protection system, as it was postulated in WASH-1400 is, as we believe, not transferable to the procedures used in the German reactor plants. The reason is, there are differences in the lay-out, in the service and maintenance strategy and in the administrative precautions.

It is written in [3] concerning the calibration procedure:

..... *In this situation, a technician is checking the calibration of a series of set points consisting of the tree comparators. To do this, he must first set up some test equipment, and he could make an error in this initial set-up. For example, he could select the wrong decade resistance, set up the wrong scale on the decade, or make some other errors in the test set-up. Unless corrected, such an error will result in miscalibration of all three comparators.*

The problem was evaluated in WASH-1400, p II-101. Fig. 7-3 presents the event tree diagram for this task. In this evaluation, a probability of 10^{-2} was estimated for the common cause failure of a miscalibration due to faulty set-up. This estimate was modified by recovery factors as follows: it was reasoned that when the technician discovered that the calibration of the first setpoint had to be changed, he would change it. It was further reasoned that when he found that the second setpoint also had to be changed, 90 % of the time he would be suspicious, would recheck his test set-up and discover his error. Ten percent of the time he would not be suspicious, and, give that he had this unsuspicious nature, it was judged that the conditional probability of the third error (i.e., failing to be become suspicious when he has to recalibrate the *third set-point) was 1.0. This is, CD was assumed between the last two tasks. Thus, the joint probability of error in calibrating the three setpoints was .01 x 1.0 x .1 x 1.0 =* 10^{-3} *.....*

In the fault tree analysis in [2] p. II-101 (but also p. IV-19) for a failure of the reactor protection system a value of $3 \cdot 10^{-5}$ is reported. This is based on the assumption that for missing the reactor protection function at least two independent groups of initiation channels have to be miscalibrated. In this case it is supposed that for the upper limit there exist a *complete dependency* (CD) between the two groups, for the lower limit it is supposed a *complete independence* (*zero dependence* (ZO)) between the two groups. The upper limit P_U becomes:

$$P_U = P_1 \wedge P_2' = 1.0 \cdot 10^{-3} \cdot 1.0 = 1.0 \cdot 10^{-3}$$

the lower limit P_L:

$$P_L = P_1 \wedge P_2'' = 1.0 \cdot 10^{-3} \cdot 1.0 \cdot 10^{-3} = 1.0 \cdot 10^{-6}$$

P_1 is the probability for miscalibration of the first channel.

P_2' is the probability for miscalibration of the second channel in case of complete *dependency.*

P_2'' is the probability for miscalibration of the second channel in case of complete *independence.*

Because of the assumption of a log normal distribution the median P_m becomes:

$$P_m = \sqrt{P_U \wedge P_L} = \sqrt{1.0 \cdot 10^{-3} \cdot 1.0 \cdot 10^{-6}} \approx 1.0 \cdot 10^{-5}$$

In [2] p. III-66 it is explained, that because of personnel redundancy a sizeable reduction of the failure probability could be reached.

For calibration work one can achieve values of 10^{-5} for the probability of a miscalibration [*A. D. Swain takes the view, that probabilities in connection with human actions never could reach values lower than* 10^{-5} *(?)*]. Values of 10^{-5} are possible if the calibration procedure is carried out by a two person team. One person reads and writes the check-list, while the second person does the calibration work. After that, the procedure becomes reversed, the second person reads and writes while the first calibrates. By the assumptions, supposed in [2,3], one can suppose, that this procedure was not being used at the time of WASH-1400 in general in US power stations.

Concerning the calibration, service and maintenance procedures in German power stations, one must distinguish between the first calibration and later or periodical tests of the once set values (*here the reference is Biblis)*. The first calibration is necessary when the set-point is set for the first time, e. g. before the first start up of a new plant, after a replacement, and after a demanded change of a set-point. All set-points are rechecked systematically every three months and after each shut down period exceeding two days. For first calibrations as well as for periodical tests the calibration procedure is performed by two persons using two different calibration meters, calibrated by an independent calibration service. Partly there is also an independent expert from the TÜV *(Technischer Überwachungsverein)* with them, authorised from the licensing authorities, before the first start up and once a year during the annual general inspection *(normally during refuelling)*. For the first calibration as well as for the periodical inspections the identical calibration procedure and the calibration meters are prescribed.

Normally during the first calibration, the first person reads the calibration instructions. The second person sets the set-point. The first person writes the setted value down in the instructions beside the prescribed value. After that, the procedure is reversed. The whole calibration procedure is observed by a representative of the TÜV.

The procedure during the periodical inspection is the same. The measured values are written beside the nominal value in the instructions. If there is a difference between the instruction and the two measured values *(from the two persons)*, larger than *10 mV* to *20 mV (0.1 to 0.2%)*, then the calibration team is authorised to make a correction, but the new value has to be documented as the third value in the instruction sheet *(Änderungsvermerk)*. The TÜV must always be informed of such corrections.

If the differences are larger than *20 mV*, then the case is put into the class of repair procedures. The calibration team is not authorised to make correction. From a repair team an independent check is made and if the result is equal to the result of the calibration team, the calibration procedure is equal to the first setting. In this case the licensing authorities must be informed.

According to [3] Tab. 14-2 and 11-3 the probability *(for human errors)*, that a miscalibration is not discovered or a calibration instruction not correctly used is, approximately equal to $A \cong 10^{-3}$, with a lower limit $X_L = 0.5 \cdot 10^{-3}$, and an upper limit $X_U = 5.0 \cdot 10^{-3}$. In each case, there is a check of the actual calibration value by a second person and by a second calibration meter, where it is supposed, that this second person is very experienced. The check procedure of the first step can not be seen independently from the first calibration step, because both steps are followed by each other and the calibration instructions are the same.

The probability of B, that a miscalibration is not discovered therefore has to lie in between the limits of *complete dependence* and *complete independence.* If a lognormal distribution is assumed, the lower limit becomes $X_L = (A)^2 = 10^{-6}$ and the upper limit $X_U = A \cdot 1.0 = 10^{-3}$. The probability, that the set-point is miscalibrated becomes :

$$P_m = A \wedge B = \sqrt{X_U \wedge X_L} \approx 3.0 \cdot 10^{-5}$$

According to [3] Tab. 15-1 the probability for B could be taken as 10^{-2}. In this case one gets:

$$P_m = A \wedge B = 1.0 \cdot 10^{-5}.$$

This value should be adopted, because it seems to be more realistic. This consideration is valid for the setting of the first value in general. For the checking or setting of the second set-point, in the two or more redundant channels of a channel group, one has to distinguish between the three cases;

Case 1: An initial *(first)* or new setting of all of the set-points of a group.

Case 2: A *(first)* setting of one or more set-points after a repair or exchange of a channel. The criterion here is, that in the channel group under consideration one or more channels remain as previously set.

Case 3: Check of the setting, e. g. in the frame of periodical inspection. In this case normally a re calibration is not necessary.

In **Case 1**, the probability for a miscalibration is the largest. Because if miscalibration of the first set-point occurs also the following set-points will be miscalibrated with high a probability.

Case 2 lies in between one and three. But probably it will tend more to case three, because in case two there is still a reference available. If a difference is discovered, with a high probability, the whole group will be checked once more and the probability is also high, that the miscalibration will be discovered and corrected, in a way as described previously.

In **Case 3** the probability is lowest. If the first technician discovers a discrepancy relative to the nominal set-point, the second technician will cross-check the set-point. There is a certain probability that they will become suspicious and recheck the tested value once more. Remember that the technicians may only make corrections in the range 0.1 to 0.2 % of the nominal set-point. Otherwise they must report this disagreement and a repair or an exchange procedure is started.

Therefore, in **Case 1**, the probability that the second or further channels of a group will be miscalibrated, given that the first channel already is miscalibrated could be set equal 1. In this case it is very difficult to imagine any facts which could motivate the technician to become doubtful after the first setting and recheck this setting once more, because the second and higher chains are also new to calibrate, and the in other cases 2 and 3 existing reference, is not available.

In **Case 2** is a lower probability than in the American study [3] seem likely (C = 0.1) because of the personnel redundancy and the restriction, that a correction of the setting outside the limits defined previously is not permitted. The probability for discovering the miscalibration will be set equal to the upper limit for miscalibration of the first value according to the assumption of *complete dependency* with C = 0.001.

In **Case 3** the same probability as already pointed out is assumed with C = 0.001. The second as well as the third case seem to be pessimistic, because of the administrative difficulty of re calibration of a once set value. There is a cross-check by a third independent person before the recalibration procedure can take place.

One can agree with the opinion, that the third miscalibrated set-point will not be discovered, when the miscalibration was also not discovered in the former two. That means D = 1.0. Calculating the overall probability one gets:

$$P\{CMA\} = P\{A \wedge B \wedge C \wedge D\}$$

the probability for the case, that all of the three *(from three)* channels of a channel group will be miscalibrated.

For the postulated three cases one can calculate the probabilities $P\{CMA\}_n$ substituting the value for B = 0.1 from [3], Index n according to the cases:

Case 1 $P\{CMA\}_1 = 1.0 \cdot 10^{-5} \cdot 1.0 \cdot 10^{-0} \cdot 1.0 = 1.0 \cdot 10^{-5}$

Case 2 $P\{CMA\}_2 = 1.0 \cdot 10^{-5} \cdot 1.0 \cdot 10^{-3} \cdot 1.0 = 1.0 \cdot 10^{-8}$

Case 3 $P\{CMA\}_3 = 1.0 \cdot 10^{-5} \cdot 1.0 \cdot 10^{-3} \cdot 1.0 = 1.0 \cdot 10^{-8}$

Case 3 is the normal case and here the probability should be lower than in **Case 2**, because it is limited to measuring and documenting but a correction of the setting is a new procedure. Considering the first case, which is the critical one, more in detail, the following question comes up: *"Under which conditions is a miscalibration possible?"* The answer is: *"Miscalibrations are possible if both calibration meters are incorrectly set, if the calibration instructions are incorrect or if the channel group to calibrate is not the correct one, e.g. if the labels to identify the group are not correct."*

For this type of errors one can assume a complete dependency between occurrence of an error and the occurrence of a miscalibration, that means, the higher value of both probabilities each, gives the value. The probability for a wrong reference value in the calibration instruction is very low to classify due to the extended administrative procedure. First a set-point is chosen and justified. Than multiple tests are performed by different persons and organisations and at the end by the independent expert, the TÜV on behave of the licensing authority. In addition the operating experience from other plants and from the manufacturer are also incorporated. Nevertheless, only a three level process for estimating the failure probability should be supposed. But data about that, can only be generated by transfer from other procedures. According to [3] p. 14-7 the probability for the first miscalibration is set equal to $3.0 \cdot 10^{-3}$. The first documented value will be checked and according to the first setting one can assume that the probability ($B = 1.0 \cdot 10^{-2}$) has a certain dependence, e. g. the same working team, the identical sources etc., therefore the same value is assumed. The check by the independent expert (TÜV) can be assumed as completely independent from the other two events and therefore one can take the same probability value than in step 1. From this a probability for a wrong calibration instruction results according to the relation:

$$P\{CMA\} = 3.0 \cdot 10^{-3} \cdot 1.0 \cdot 10^{-2} \cdot 3.0 \cdot 10^{-3} \approx 1.0 \cdot 10^{-7}$$

By the assumptions made there is a tendency to the safe side, which means that the value is pessimistic.

A miscalibration of the two calibration meters at the same time seems to be still more unprobable than the probability of wrong calibration instructions. The calibration meters are subjected to a certain quality assurance and only permitted for use of calibration in the reactor protection area. All of the meters are checked annually according to special standards by an independent calibration service outside the plant.

Approximately the same order of magnitude may be assumed for wrong or misleading labelling of a channel group. Here it is also the personnel redundancy, two technicians and an independent expert, which makes the occurrence probability very low.

The considerations until now are only valid for the first calibration. But before the first start up, there will be an additional check of the set-points. In this way with a high probability existing errors will be discovered. A recognition of larger differences, as pointed out earlier, results not in recalibration, but in a repair procedure, which starts with an analysis of the origin for the necessary repair. At the exchange of one channel in a group, the correct calibrated ones remain in the group. A difference in the signal level in the different channels of a group is observed and will be discovered by comparison of the signals.

The previous consideration allows one to conclude that the probability of a miscalibration of all channels of an initiation channel group in the reactor protection system is very low. That means, that the risk due to the Common Mode problem, could be kept so low, that it loses its dominating character.

References according to the reference list on page 18.