The contribution to safety of a diverse backup system for digital safety I&C systems in Nuclear Power Plants, a probabilistic approach

W. Postma[a*], J.L. Brinkman[a]
[a] NRG, Arnhem, the Netherlands

Abstract: NRG performed a research project on the influence on safety of diverse backup systems next to the existing digital I&C safety systems in Nuclear Power Plants (NPPs). As part of this research project a probabilistic approach has been used to evaluate the basic options to connect a diverse backup system logically to the existing digital I&C systems.

One can distinguish four different basic design options: (1) no backup system is used; (2) the backup system is used only if the digital system has failed, the switch-over to the backup system is automatic; (3) the backup system is used only if the digital system has failed, the switch-over to the backup system is manual; (4) the backup system is in continuous operation, with an equal vote as the digital system.

Design (2) and (4) have been modeled and compared with the situation without backup system (design 1). This paper will discuss the model and the results, including the sensitivity analyses, in order to reflect on the probabilistic impact of a diverse backup system.

Keywords: Digital I&C, Backup system, PRA, CCF

1. INTRODUCTION

NRG performed a research project on the influence on safety of diverse backup systems next to the existing digital I&C safety systems in Nuclear Power Plants (NPPs). As part of this research project a probabilistic approach has been used to evaluate the basic options to connect a diverse backup system logically to the existing digital I&C systems. The probabilistic evaluation and its results will be discussed in this paper.

Digital I&C systems, compared with analogue I&C systems, provide many important technical benefits. They are basically drift-free and system performance has been improved in terms of accuracy and computational capabilities. Since digital I&C systems have outstanding capabilities of data handling and storage, the plant operating conditions can be effectively measured and displayed.

However, digital systems are vulnerable to common cause failure (CCF) that may cause redundant safety systems to fail in their functions. Avoiding CCF is of vital importance for a safe and reliable operation of digital safety systems.

With this background most regulators require a diverse backup system to complement the digital safety systems in NPPs. The main goal of the diverse backup system is to enhance the safety further. The system has to bring the plant in a safe state if all digital systems have failed due to a CCF.

One can distinguish four different basic design options: (1) no backup system is used; (2) the backup system is used only if the digital system has failed, the switch-over to the backup system is automatic; (3) the backup system is used only if the digital system has failed, the switch-over to the backup system is manual; (4) the backup system is in continuous operation, with an equal vote as the digital system.

Design (2) and (4) have been modeled and compared with the situation without backup system (design 1). Design 3 is very similar to design 1 and mainly limits the number of functions suitable for backup, because of the time frame that is needed to carry out the manual action to switch to the backup system.

*w.postma@nrg.eu

2. MAIN DESIGN OPTIONS IN BACKUP SYSTEM LOGIC

An important aspect in assessing the impact of the diversity strategy on safety is how the backup/diverse system "knows" when to operate. In this section the three main design options to incorporate the backup system in the architecture are discussed:

- **Automatic switchover (design 2)**: The system is actuated when failures in the other systems are detected by the monitoring system;
- **Manual switchover (design 3)**: The system is actuated manually if the operators notice a loss of the computerized systems;
- **Continuous operation with an equal vote to the digital system (design 4)**: The system functions completely in parallel to the other systems, but incorporates a limited number of functions.

The manual switchover and the automatic switchover are very similar. In both cases the backup system will only be used if failures in the normal systems are detected. As it is of course impossible to react on undetected failures of the normal systems, the fraction of undetected failures will have a large impact on the effectiveness of the backup system. To make a best estimate of the reliability of a system it is therefore important to know the fraction of undetected failures as compared to the detected failures.

Every option has its advantages:

- The automatic switchover and the manual switchover will not likely contribute to the unavailability and the back-up-system is only used when really necessary, consequently the reliability requirements can be less stringent than for the digital system. Also, the automatic switchover is fast and reliable.
- The manual switchover does not need additional computerized elements to carry out the switchover, so it will be more robust against a complete loss of the computerized I&C.
- Continuous operation with an equal vote to the digital system always contributes to the safety.

The disadvantage of the back-up in continuous operation is that the backup system should be classified in the same safety category as the standard systems, as it carries out the same, although limited number of safety functions. Another disadvantage is that the reliability requirements for spurious actuations should also be equal to those of the standard digital systems in order to prevent an increase in spurious trips and actuations.

In digital I&C systems there are numerous possibilities to mitigate the effects of failures. One of the mitigative measures is to switch the outputs of the failed module to a predefined status or notifying the operators, if possible. If it is possible to define a failsafe status of a module the additional effect on safety of a backup system might be small, as will be shown in this paper.

In all cases it is necessary to ensure the independence of the computer based systems and the backup system in order to prevent that failures in the computer based systems can affect the operation of the backup and vice versa. Additionally the diversity between the digital I&C system and the backup system is needed to eliminate potential CCF.

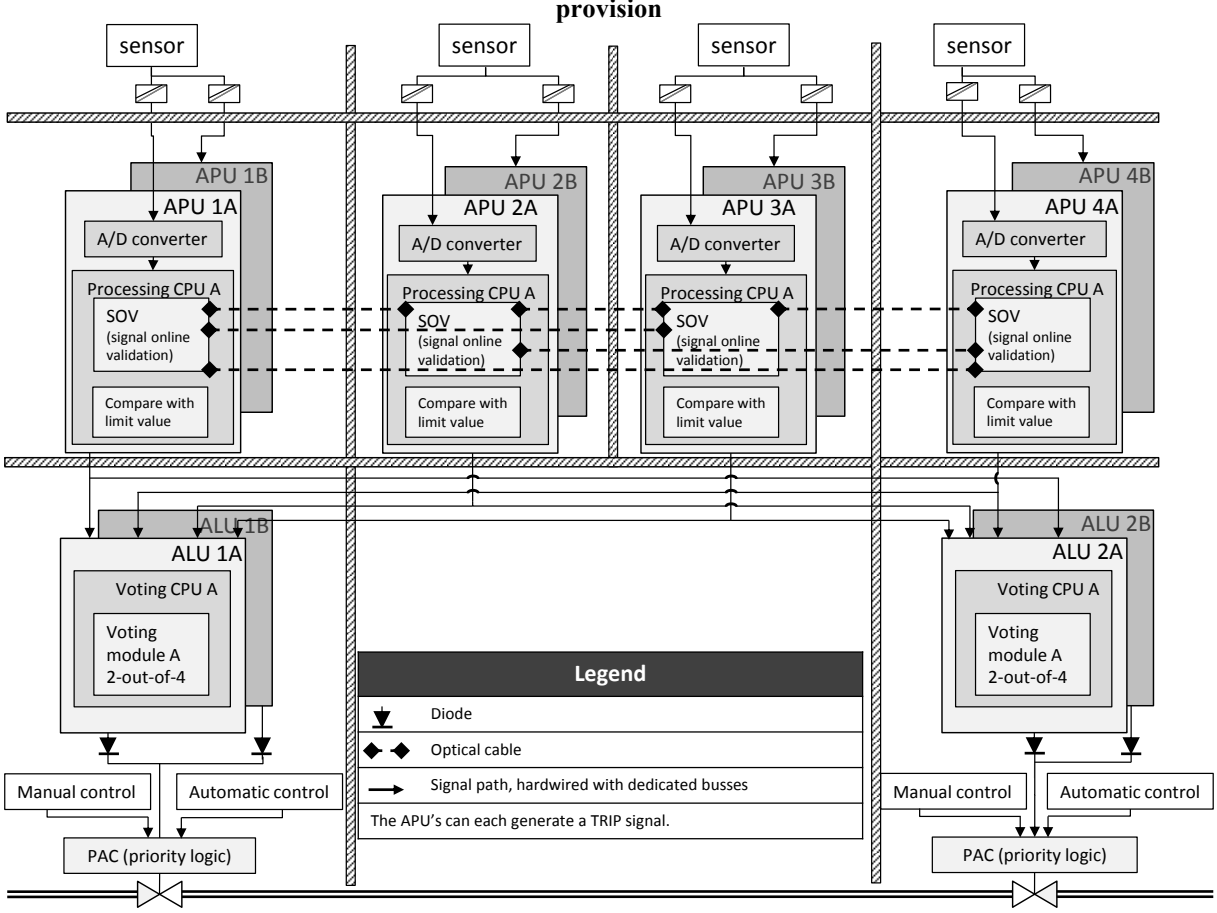
3. SYSTEM ARCHITECTURE

The architecture that is used for the present study is an example system that is based on information in publically available literature on digital I&C for Nuclear Power Plants. The schematic of the architecture is shown in Figure 1.

The input of the system is carried out 4-fold redundant, the output is 2-fold redundant. Every redundant channel has two diversities, named diversity A and B. There is no communication between the two diversities.

The data acquisition is done by four sensors. The signal of a sensor is – per sensor - divided over diversity A and B. A/D converters convert the signal into a digital signal.

Figure 1: I&C structure that is the basis for the model. The architecture is shown without backup provision



In the acquisition and processing units (APUs) the sensor values are processed and validated. The digitized input is computed to get the corresponding physical value of the measurement that is processed.

The digitized values from all four channels are distributed to all the redundant channels for validation purposes. Each input is compared to the measuring range limits. The digitized inputs of the other channels are used for comparison.

The Actuation Logic Units (ALUs) receive the result of the validation process of every APU of the corresponding diversity. In the ALU a 2 out of 4 voting process takes place to decide whether or not to send an actuation signal to the Priority Actuation and Control (PAC).

The PAC sends an actuation command to the actuator (for example a valve). Also, the PAC ensures that safety commands will always get priority over non-safety commands. The PACs in both trains are assumed to be identical.

For all communication optical cables are used to ensure independency, using dedicated buses.

Three designs are modeled:

- Design 1: No backup provision
    - The architecture of design one corresponds to the architecture presented in Figure 1.

- Design 2: Switchover
    - In this case the backup system is used when the normal system has failed detectably. An automatic switchover is modeled (design 2). The architecture of design two is shown in Figure 2. The backup system is coupled to the standard system by using an inverse AND-gate (hardwired). If the backup system sends activation signal AND the monitoring of ALU A AND B gives an error message (sending 0, fail safe), the inverse AND-gate gives an activation signal. In normal operation the monitoring of ALU A and B gives an active high signal and the output of the backup systems is blocked.
- Design 4: Continuous operation with an equal vote to the digital system (design 4)
    - The architecture of design 4 is shown in Figure 3. The backup system is connected logically to the standard system via an OR-gate. This means that either subsystem A, subsystem B or the backup can initiate an actuation signal.

Figure 2: Backup system logic configuration in case of an automatic switchover to the backup system, when the normal system has failed detectably (design 2)

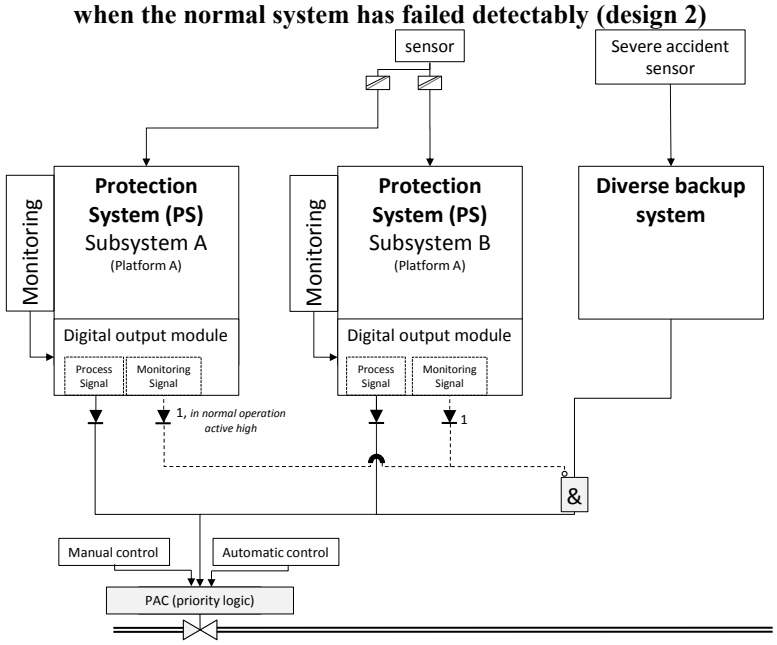
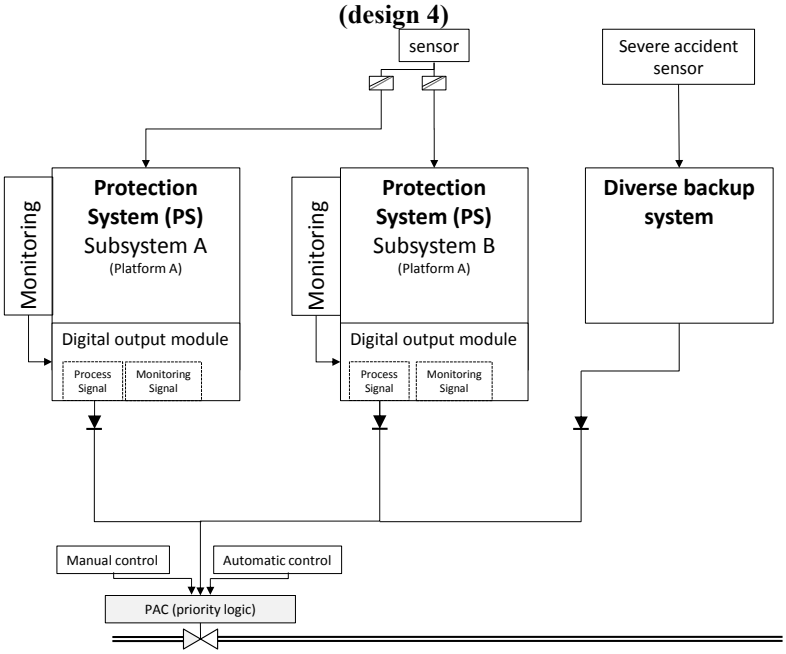


Figure 3: Backup system logic configuration in case of equal and continuous operation of the backup (design 4)



4. FAULT TREE MODEL

4.1. General description of the model and the approach

Given the available information in publically available literature the most appropriate level of abstraction is the I&C unit level. An I&C unit has a specific task in the process of executing the function. An example of an I&C unit is the ALU, which has the specific task of sending an actuation signal after carrying out a voting process. If more details are available, the I&C units can be further decomposed in CPU, I/O-modules, racks etc. (module level). In order to make the I&C unit level an accurate description of the module level, appropriate assumptions have to be made on for example diagnostic coverage, common cause failures and predefined outputs.

Three top-events are considered:

1. Failure to actuate without backup system which corresponds to design 1;
2. Failure to actuate with a backup system that is used only when the normal system has failed detectably which corresponds to design 2;
3. Failure to actuate with a backup system in continuous operation with an equal vote to the digital system which corresponds to design 4.

Design 3 is not modeled separately, because it is very similar to design 2 (see section 1).

The model considers only one automatic protection function, carried out by the protection system of a plant. The model reflects the system up to and including the actuation signal and does not include failure of the actuator itself. Additionally, the model does not include manual actions and support systems. The power supply is not modeled assuming a high redundancy of power supply systems. Based on experience, the impact of loss of power on the failure to actuate is negligible for highly redundant power supply systems.

The standard top-down ("upstream") approach has been used to make the model. Starting with the top-event, failure to send an actuation signal, to the valve and then upstream to the sensors. To take into account all relevant failures for all components, all flow paths are followed consistently, starting with the priority logic and ending at the sensors.

In case of design 2, automatic switchover to the backup after the standard system has failed detectably, the backup is built into the system in way that it reacts differently to different types of faults. If the standard system fails detectably the backup will be used, if the standard system fails undetectably the backup cannot be used. This defeats the "good practices" way of making fault trees, because it forces one to think in combinations of failures, which is very error prone.

In this model it is assumed that the backup is used only if both ALUs have failed detectably. If there are detectable failures in an ALU, the output of the ALU is marked as invalid and the output goes to the predefined value (=0, no actuation signal) and the control signal goes from 1 (active high) to 0. If there is a combination of a detected failure and an undetected failure of the ALUs, the backup system is not coupled in. Therefore, the event that the priority logic receives a faulty input signal from the ALUs is split into four options:

1. A detected failure in both ALUs → the backup is used;
2. A detected failure in ALU A and an undetected failure in ALU B → backup is not used;
3. An undetected failure in ALU A and a detected failure in ALU B → backup is not used;
4. An undetected failure in both ALUs → backup is not used.

The ALUs can get a faulty input from the APUs. A detected failure of an APU will lead to a "high" signal (= partial trigger) due to the defined fail safe position. The voting logic will now see at least one high signal and will need only one additional high signal to send an actuation signal to the priority logic. The result is that the voting logic, by definition, changes from 2 out of 4 (2oo4) to 1 out of 3 (1oo3) in the corresponding diversity. If yet another APU fails detectably, the output is again set to 1 (=partial trigger). The voting module (ALU) will now see 2oo4 signals high and will send an actuation

signal to the PAC. So, detected failures of the APUs will not contribute to a failure to actuate. Only the undetected failures of the APUs will contribute to a failure to actuate. If three or more APUs in a diversity fail undetected, the ALUs in that diversity will not be able to send an actuation signal.

It is assumed that the backup system is completely independent and diverse from the digital I&C systems. For the backup system different sensors are used than for the digital I&C system. The backup system cannot be set to a predefined value. No CCF has been assumed between the backup system and the standard systems in order to determine the maximum impact of the backup system.

3.2. Failure modes

Five failure modes are included in the model:

1. **Detected failures (DF0) programmable logic (APU/ALU/PAC)**: In case of detected failures, the I&C units will go to the predefined outputs, which are as follows:
    - APU = 1 (partial trigger)
    - ALU = 0 (no actuation)
    - PAC = 0 (no actuation)
    - The failure of a module can be detected by internal means and by external means. For example, if an APU fails, this can be detected by the APU itself (internal means). Another possibility is the detection of a failure at the next I&C unit in the processing line, as it is the case for the sensors. If there is a failure of a sensor, the sensor itself will not detect that, but the APU is capable of validating the signal. If the signal is lost or corrupted and the APU can detect that (external means), the output of the APU is set to 1.
    - Examples: loss of power supply, loss of input, crash of a microprocessor, etc.
2. **Undetected failures (UFB) programmable logic (APU/ALU/PAC)**: under the undetected failures, the failure mode "undetected-blocking" is considered, because this is a fail to danger. In case of undetected blocking the output of an I&C unit does not generate a (partial) trigger, although a partial trigger is should be generated. Because the failure mode is not detectable, the output cannot be set to the predefined output value. Examples: saturation of a system network, progressive saturation of a memory block, etc.
3. **Detected (DF) and undetected (UF) failures backup system**: In both cases, the backup system fails to send an actuation signal. It is assumed that it is not possible to set the output of the backup system to a predefined state. In case of a detected failure, repair can be started. In case of an undetected failure, the failure will be discovered after testing.
4. **Out of range (OOR) sensor**: A sensor can indicate a value that is outside a 5% bound of the value read by the other sensors. In this case an error message is sent to the control room. However, because this type of validation is dependent on communication with other sensors, it is conservatively assumed that this type of error does not set the APU to the predefined output value.
5. **In range but low (IRL) sensor**: This failure mode is a calibration error. All sensors lie within a 5% bound of each other, but all sensors indicate a too low value. This failure mode is undetected.

3.2. Data

Failure rates

The data that is used, is obtained from publically available sources and is shown in Table 1. Table 1 shows the total failure rate. Based on the diagnostic coverage the failure rate is split into a detected and undetected fraction. The failure rates for the hardware modules APU, ALU and the backup system are the sum of the theoretical failure rates of the power supply, backplane, CPU, memory, carrier board, digital input piggyback, digital output piggyback and serial I/O piggyback (MIL-HDBK-217F [1]). For the backup system similar reliability data is assumed as for the digital I&C system. Also for the sensors are similar data used as for the sensors of the digital I&C system.

Table 1: Data used for the fault tree model

Component	Failure rate [h^{-1}]	Remarks	Data source
Sensor out of range	$1.0 \cdot 10^{-6}$		[2]
Sensor in range but low	$1.0 \cdot 10^{-6}$	CCF all sensors: 5.0E-9 [h^{-1}]	-
APU/ALU/ Backup system	$1.6 \cdot 10^{-5}$	It is assumed that all these modules consist of the same hardware, but have different software modules with the same reliability.	[3]
PAC	$4.4 \cdot 10^{-5}$	This value corresponds to the failure rate of the AV42, which is a priority and actuation control module.	[4]

Diagnostic coverage
The ratio between detected and undetected failures is largely determined by the coverage of the monitoring. In other words, what percentage of failures will be recognized by monitoring? The diagnostic coverage used in the model is 99%. This is the highest diagnostic coverage that is claimed in the IEC 61508 standard for requirements for electrical/electronic/programmable electronic safety-related systems [5].

Test intervals
Test intervals are an important measure to limit the impact of undetected failures on the system failure probability. At this point it is not known what the test intervals are. Therefore the test intervals are assumed to be the same for all modules and are set to 1 year (8760h), which corresponds to the yearly outage of most nuclear power plants.

Repair times
Repair times depend on the kind of failure, accessibility and availability of spares. For example, an I/O module can be replaced with power on the backplane bus, but if processing units have to be replaced, the power of the backplane bus has to be shut down.

For the repair times a realistic assumption has been made, namely 8h. Assuming that repair can be carried out in one shift. The replacement time reflects the repair time from detection until the notification that the system is repaired.

Common cause failure (CCF)
CCF is the failure of two or more identical or similar components as the result of a common cause which has not been explicitly modeled, for example design errors or errors during maintenance. In redundant systems, common cause failure (CCF) can lead to loss of more than one channel or train. Modeling CCF is important, because CCF can be a dominant contribution to system unavailability.

The following groups have been considered for CCF analysis:

1. Sensors;
2. APUs (Acquisition and Processing Units);
3. ALUs (Actuation Logic Units);
4. PACs (Priority and Actuation and Control).

The Binomial Failure Rate model (BFR model) has been used for the quantification of the CCF. In the BFR model both dependent and independent failures are considered. For the modeling of CCF one is interested in the dependent failures. For this study the generic data from the report “European Utilities requirements for LWR Nuclear Power Plants” [6] have been used. Which leads to a percentage of common cause failure of 14% (=common cause failure probability/total failure probability). This does not mean that 14% of the failure on demand is caused by CCF. For example 3 out of 4 APUs have to fail to contribute to the failure on demand. The undetected common cause failure of 3 out of 4 APUs is

in the order of 10^{-8}, while a combination of three APUs failing independently is in the order of 10^{-21}, which is much less than the failure rate for common cause failure. Therefore common cause failure is a dominant contribution to the total failure on demand.

For the CCF of sensors other CCF values have been chosen, based on the values known from analog systems. The parameters of the BFR model are chosen such that the probability of a CCF of the sensors (for example due to calibration errors) is 0.6% of the total failure rate of one sensor.

4. RESULTS

4.1. Dominant cutsets

The dominant cutsets provide valuable information on the model. In Table 2 the dominant cutsets are shown. The first 10 cutsets represent in each case more than 95% of the total failure rate. The first order cutsets, which are all common cause failures, provide the largest contribution to the PFD. In all three models, the dominating cutset is an undetected common cause failure of the priority modules (PAC), representing more than 60% of the total probability of failure on demand (PFD).

Compared to design 1 (without backup system) the following is observed for design 2 and 4:

- Design 2, automatic switchover, addresses only one failure mode: a detected CCF of 4oo4 ALUs (0.8% of PFD), because in case of a detected failure of all ALUs the system will switch over to the backup system. The other cutsets of design 2 are the same as the cutsets of design 1.
- Design 4, continuous backup, also addresses calibration errors of the sensors (14% of PFD), because two independent sensors are available for the backup system, and undetected CCF of the ALUs (4.6% of PFD). The new dominant cutsets compared to design 1 represent combinations of CCF in the backup-system together with CCF in the digital systems.

Table 2: Dominant cutsets. Cutsets that show up in every model are marked grey.

	no backup (design 1)	backup that is coupled in, in case of failure of the normal system (design 2)	backup in equal and continuous operation (design 4)
1	Undetected CCF of 2oo2 PACs	Undetected CCF of 2oo2 PACs	Undetected CCF of 2oo2 PACs
2	Calibration error of 4 out of 4 sensors	Calibration error of 4 out of 4 sensors	Detected CCF of 2oo2 PACs
3	Detected CCF of 2oo2 PACs	Detected CCF of 2oo2 PACs	Combination of independent undetected failures of 2oo2 PACs
4	Undetected CCF of 4oo4 ALUs	Undetected CCF of 4oo4 ALUs	Combination of undetected failure of PAC1 and detected failure of PAC2
5	Combination of independent undetected failure of 2oo2 PACs	Combination of independent undetected failures of 2oo2 PACs	Combination of undetected failure of PAC2 and detected failure of PAC1
6	Undetected CCF of 6oo8 APUs	Undetected CCF of 6oo8 APUs	Combination of detected independent failure of 2oo2 PACs
7	Detected CCF of 4oo4 ALUs	Undetected failure of 7oo8 APUs	Calibration error of the sensors of the backup system in combination with calibration error of the sensors of the standard system
8	Undetected failure of 7oo8 APUs	Combination of undetected failure of PAC1 and detected failure of PAC2	Calibration error of the sensors of the backup system in combination with undetected CCF of 4oo4 ALUs
9	Combination of undetected failure of PAC1 and detected failure of PAC2	Combination of undetected failure of PAC2 and detected failure of PAC1	Undetected CCF of 2oo2 backup systems and a calibration error of the sensors of the standard systems
10	Combination of undetected failure of PAC2 and detected failure of PAC1	Combination of detected independent failure of 2oo2 PACs	Undetected CCF of 2 oo2 backup systems and an undetected CCF of 4oo4 ALUs

4.1. Failure to actuate on demand

The quantification results (PFD) of the three models are summarized in Table 3. The results show that the impact of a switchover backup system (design 2) on safety is very small from a probabilistic point of view (1% lower PFD). This can be reasoned from the cutsets, since the dominant cutset represent failures that are not addressed by the backup system, in particular, undetected failures and failures of the priority logic.

The backup that is in continuous operation with an equal vote as the digital system does have a significant effect on the PFD, because also the undetected failures of the ALUs and APUs, and the calibration errors are addressed by this configuration.

Table 3: Summary of the quantification results of the three models

	no backup (design 1)	backup that is coupled in, in case of failure of the normal system (design 2)	backup in equal and continuous operation (design 4)
1st order	$1.5 \cdot 10^{-4}$	$1.5 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$
2nd order	$6.9 \cdot 10^{-6}$	$6.8 \cdot 10^{-6}$	$6.6 \cdot 10^{-6}$
3rd order	$7.9 \cdot 10^{-9}$	$7.9 \cdot 10^{-9}$	$6.5 \cdot 10^{-10}$
Higher order	-	-	-
Total	$1.6 \cdot 10^{-4}$	$1.6 \cdot 10^{-4}$	$1.2 \cdot 10^{-4}$

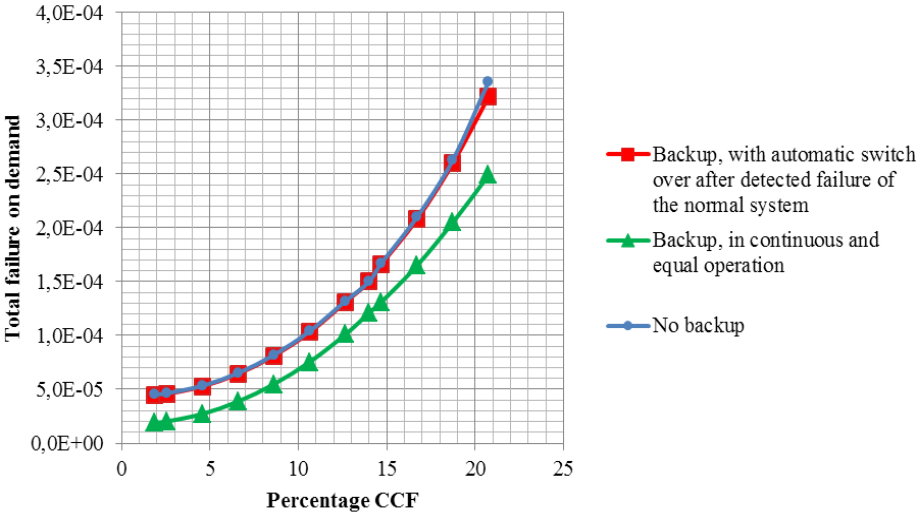
4.2. Sensitivity analysis common cause failure

The impact of the percentage of CCF on the PFD has been analyzed by adjusting the ratio between the common cause failure rate and the total failure rate of a component. The results are shown in Figure 4. The response to the percentage of CCF is the same for all three architectures. The higher the percentage of CCF the larger the difference is between the PFD of the model with and without backup.

The difference between design 2 (switch-over backup) and design 1 (no backup) remains very small: 4% lower PFD for a CCF of 20%. As the percentage of CCF increases the contribution of CCF to the PFD also increases. Consequently the impact of detected CCF of the ALUs increases, which is addressed by the backup system. However this effect is masked by the increased contribution of cutsets that are not addressed by the backup system, for example CCF of the priority logic.

The system with a backup in continuous operation (design 4) performs better for all values. The difference increases as the percentage of CCF increases.

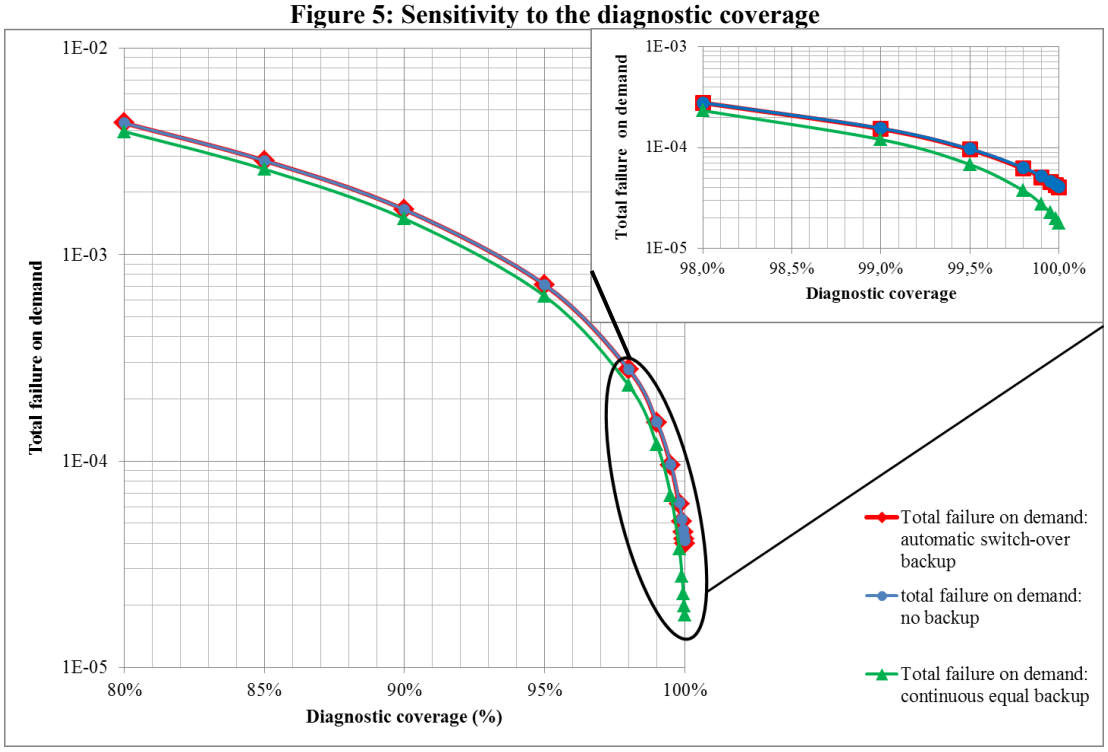
Figure 4: Sensitivity to the percentage of CCF



4.4. Sensitivity to the diagnostic coverage

The value of the diagnostic coverage is uncertain. Additionally it is known that more detailed models (lower level of abstraction) show a higher importance of detected failures, i.e. the diagnostic coverage is higher than could be expected from the model with a high level of abstraction. Therefore it is important to know the sensitivity of the results to the value of the diagnostic coverage. The diagnostic coverage has been varied from 80% to 100%; the effect on the PFD of the three models is shown in Figure 5.

Figure 5: Sensitivity to the diagnostic coverage



The results show that the PFD is very sensitive to the diagnostic coverage. The PFD changes almost two orders of magnitude between 90% detected failures and 100% detected failures. Also, the higher the diagnostic coverage, the more sensitive to the diagnostic coverage the model will be.

However the differences between the models are very small as the diagnostic coverage is changed. In the limit of 100% diagnostic coverage the dominating cutsets of design 1 (no backup) are from CCF of the sensors and CCF of the PAC, neither are addressed by a switchover backup. The failure that is addressed by the switchover backup, detected CCF of the ALUs, presents only 3% of the total PFD. Therefore the system with an automatic switchover backup system will only perform 3% better than the system without backup. In the limit of 100% diagnostic coverage a continuous backup will perform 57% better than the system without backup, because also the CCF of the sensors is addressed.

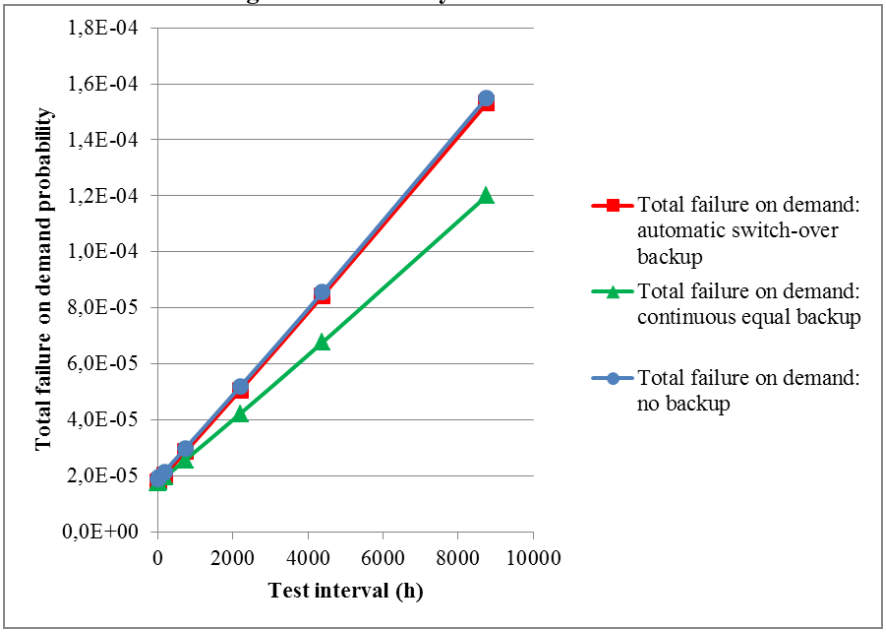
Note that if all detected failures that are addressed by the backup system would lead to a predefined failsafe value, the models would give the same result. However in the present study it is assumed that the detected failures of the ALUs and the sensors will not lead to a failsafe output.

4.5. Impact of the test interval

The test interval has a high impact on the PFD. As the test interval is decreased, the PFD also decreases. This can be explained by the fact that the undetected failures have a less pronounced impact on the PFD in this case. The results are shown in Figure 6. The dominating cutsets of design 1 (no backup) for a chosen limit value for the test interval of 1h are: 1) detected CCF of the PAC (91% of the PFD), 2) detected CCF of the ALU (7% of the PFD). From these failures only the detected CCF of the ALUs is addressed by a backup system (both design 2 and 4) because a backup system cannot address CCF of the priority logic (PAC). Therefore, for both designs, switchover backup and

continuous backup, a decrease in the total PFD of ~7% results when a test interval of 1h is chosen (PFD without backup ≈ $1.8 \cdot 10^{-5}$).

Figure 6: Sensitivity to the test interval



4.6. Impact of the failure rate of the priority logic

Since common cause failure of the priority logic has the highest contribution to the PFD, the model is very sensitive to changes of common cause failure probability of the priority logic. For all three models, the common cause failure probability has been changed in order to observe whether the backup systems have a more pronounced effect on the PFD in case of a lower common cause failure probability of the PAC. As is shown in Table 4 the effect of the backup systems is more pronounced if no CCF between the PACs is assumed (for example, because the PACs are diverse). Especially the backup in continuous operation shows significantly better results than the system without backup. The switch-over backup shows slightly better results (~3%) than the system without backup.

Table 4: Impact of the CCF probability of the PACs on the PFD

CCF of 2oo2 PACs	no backup	switch over backup	continuous backup
• Detected: $4 \cdot 10^{-4}$ • Undetected: $4 \cdot 10^{-6}$	$5.6 \cdot 10^{-04}$	$5.6 \cdot 10^{-04}$	$5.3 \cdot 10^{-04}$
• Detected CCF: $4 \cdot 10^{-5}$ • Undetected CCF: $4 \cdot 10^{-7}$	$1.6 \cdot 10^{-04}$	$1.6 \cdot 10^{-04}$	$1.2 \cdot 10^{-04}$
no CCF	$4.1 \cdot 10^{-05}$	$4.0 \cdot 10^{-05}$	$6.6 \cdot 10^{-05}$

5. CONCLUSION

How the backup is implemented does have an influence on the impact of the backup system on the probability of failure on demand (PFD). In general a backup system in continuous operation and with an equal vote as the digital system has a more pronounced effect than a backup system that is used when the standard systems have failed detectably.

Several parameters have been changed to determine the influence on the model: the percentage of common cause failure, the diagnostic coverage, the test interval and the common cause failure rate of the PAC. The results are summarized in Table 5.

Table 5: Summary of the results in terms of % lower PFD with backup compared to the system without backup

	No backup PFD	Switch-over backup (design 2) (% lower PFD)	Continuous backup (design 4) (% lower PFD)
Values as described in section 3.2	$1.6 \cdot 10^{-4}$	1%	23%
20% of CCF	$3.4 \cdot 10^{-4}$	4%	26%
2% of CCF	$4.5 \cdot 10^{-5}$	2%	58%
Diagnostic coverage of 100%	$4.1 \cdot 10^{-5}$	3%	57%
Diagnostic coverage of 80%	$4.3 \cdot 10^{-3}$	0%	9%
Test interval of 1h	$1.9 \cdot 10^{-5}$	7%	8%
No CCF between PACs	$4.1 \cdot 10^{-5}$	3%	84%

If the backup system is only used when the other systems have failed detected, the impact on the PFD is very small. The dominating cutsets are: 1) failure of 2 out of 2 priority logic modules (PAC), either CCF or independent, either detected or undetected, 2) CCF of 4 out of 4 sensors, 3) undetected CCF of the ALUs, 4) detected failure of the ALUs (0.8% of the total PFD). A switchover backup can only address the detected failure of the ALUs, therefore the maximum decrease of the PFD with a switchover backup is 0.8%. The continuous backup can also address CCF of the sensors (if other, independent sensors are used) and undetected failure of the ALUs, which leads to a decrease of the PDF of 23%.

Furthermore it is shown that if the percentage of CCF, diagnostic coverage, the test interval or the failure rate of the priority logic is changed, the decrease of the PFD of a switch-over backup system is relatively small (maximum 7%). The relatively small gain needs to be balanced to the increased complexity and possibilities for spurious failures. Additionally, another possibility to mitigate detected failures is to set the failed module to its predefined output value, and if possible to a failsafe value. In this study a failsafe value is only assumed for the APUs and not for the ALUs and PACs. In the limit that all failures are detected and lead to a failsafe status, the backup system will not have any impact.

If the backup system is used in continuous operations with an equal vote to the digital system the performance is significantly better than for the system without backup. The calculated impact is for one function, not for the complete digital I&C system. The impact on the complete system will be less, since the standard I&C systems are already diverse and implement diverse functions.

Other possibilities to improve the safety of a digital protection function are: 1) increasing the diagnostic coverage; 2) investing in timely detection for example by periodic testing; and 3) diversifying the priority logic.

Acknowledgements
This research has been carried out under contract with the Dutch Ministry of Economic Affairs and the Kernfysische Dienst (KFD).

References

[1] Department of Defense, *"Military Handbook Reliability Prediction of Electronic Equipment (MIL-HDBK-217F)"*, 2 December 1991, Washington DC.
[2] J. Schüller, *"Methods for determining and processing probabilities"*, NRG, 1997, Den Haag.
[3] NRG, "*Faalkansanalyse NSTA, NSTA - Vernieuwen NSS en Startautomaat"*, CMG Public Sector B.V., 2002.
[4] Stefan Authen, Kim Björkman, Jan-Erik Holmberg, Josefin Larsson, *"Guidelines for reliability analysis of digital systems in PSA context - Phase 1 Status Report"*, NKS, 2010.
[5] "IEC 61508-2: requirements of electrical/electronic/programmable electronic safety-related systems", CEI/IEC 61508-2:2000, first edition, 2000, Geneva.
[6] "European Utilities Requirements for LWR Nuclear Power Plants", Volume 2: Generic Requirements, Chapter 17, PSA methodology, appendix C, Method and Data for Treatment of Common Cause Failures, Revision B, November 1995.