# GOVERNING OF COMMON CAUSE FAILURES

H-W. BOCK
Siemens/KWU NLL
Erlangen, Germany

**Abstract**

Agreed strategy is to govern common cause failures by the application of diversity, to assure that the overall plant safety objectives are met even in the case that a common cause failure of a system with all redundent trains is assumed. The presented strategy aims on the application of functional diversity without the implementation of equipment diversity. In the focus are the design criteria which have to be met for the design of independent systems in such a way that the time-correlated failure of such independent systems according a common cause can be excluded deterministically.

## 1 Introduction

The design of safety systems - of mechanical process systems as well as of I&C systems - is from the beginning of the development of nuclear power plants characterised by the requirement on failure tolerance. Proven design principle is the application of redundancy to fulfil the required safety functions even in case of a failure of one of the redundant subsystems including consequential failures (Single Failure Criterion ). Additionally it is an established requirement (e.g. in the German KTA 3501) to consider a potential design fault in the definition of the I&C safety functions such that generally for each design basis accident two physically divers initiation criteria should be implemented in the I&C safety system.

Common cause failures generally originate in unknown design faults, which cause a malfunction of redundant but identical subsystems due to a specific loading. The other general failure possibility, that random hardware faults accumulate in a hidden way in redundant subsystems and lead to the total system failure on demand, has proven to be irrelevant for carefully maintained safety systems and is not object of this paper.

Since the start of introducing digital I&C systems for safety relevant functions, the focus lies on the development of strategies to overcome problems of common cause failures. Accepting the severe safety importance of undetected design errors which may be the potential cause of the common failure of redundant safety systems to fulfil their intended functions sometimes, from present discussions, one may have the impression that the common cause failure problem is typical for digital I&C systems.

Design faults originate in the design process. It is the experience from the operation of redundant systems that hidden design faults generally become evident in the case of specific random loadings. The experience from the operation of non-redundant industrial digital systems doesn't help, because often we cannot differ between a systematic failure and a random component failure in case of a system malfunction.

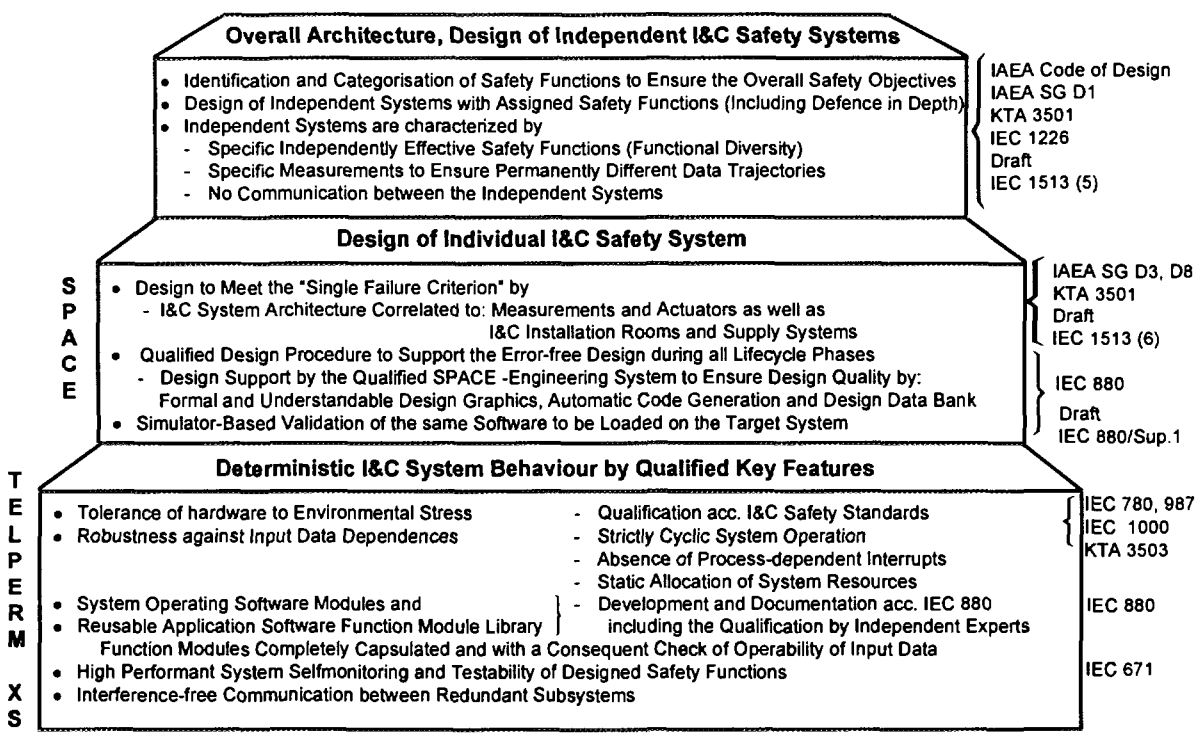
The probability, whether a system contains inherent unknown design faults generally cannot be quantified. What is decisive, is the quality of the design process and therefore the weak points correlated with the technology of the target system have to be reflected for the design process. The experience from the occurrence of the malfunction of systems built with other technologies or for other applications gives no quantitative information, which can be used for statistical means.

## 2 The Three Level Strategy

To govern the problem of „Common Cause Failure" (CCF) of I&C safety systems, Siemens/ KWU has developed the „Three Level Strategy". The three levels form different defence-in-depth design barriers which include the I&C system development, the design of the overall I&C systems architecture as well as the design of individual I&C systems. Thus the global plant safety objectives are met even if the occurrence of common cause failures is assumed.

The analysis of failures of redundant systems always leads to an erroneous specification of the intended functions or an erroneous design of software or hardware modules or to faults in the manufacturing process of I&C systems. However, such occurrences are rather improbable and the causes change with the I&C technology. Therefore probabilistic approaches are generally not feasible to manage the CFF problem.

The strategy that has been developed by Siemens/KWU in parallel to the development of the TELEPERM XS system comprises three design levels to govern the CFF problem (figure 1) .




**TELEPERM XS : The Three Level Strategy** Figure 1

## 2.1 The deterministic I&C system behaviour

The first design level in the strategy to govern CCF was elaborated during the development of the requirement specification to ensure the key features of the TELEPERM XS system. The system is characterised by deterministic I&C system behaviour. This means that the overall system behaviour in response to any input data trajectories is determined by the validated application software and is free of any unintended interferences on the operating system software and the system hardware.

The deterministic behaviour is ensured by the following key features of the TELEPERM XS system:

- The hardware modules are designed and qualified by theoretical analysis as well as tests to perform their intended functions even under environmental stress. This ensures that system failures caused by environmental effects can be excluded within the design requirements of the relevant German as well as international I&C safety standards.

- To ensure the independence of the systems' operating behaviour from any input data trajectories, the following set of system features is implemented:
  Strictly cyclic system operation
  No process dependent interrupts
  Static allocation of system resources

- Interference-free communication between subsystems as fault barrier so that single failures in one train cannot propagate to a system CCF

- The operating system software is developed strictly according to IEC 880. To ensure highest quality, the complete development documentation was input to the qualification process by independent experts.

- The function block modules kept in the library for generating the application software are developed and qualified in the same way according to IEC 880. All function block modules are completely capsulated and equipped with consequent checks on operability of the input data.

Finally these key system features that are relevant for ensuring the deterministic system behaviour were confirmed during generic tests on a redundant four-train system performed in the presence of independent experts from GRS-ISTec and TÜV-North. The confirmed deterministic system behaviour is the essential precondition for that the correct design of application software and architecture for an individual I&C system determines the final behaviour of the integrated system in correspondence to the design requirements.

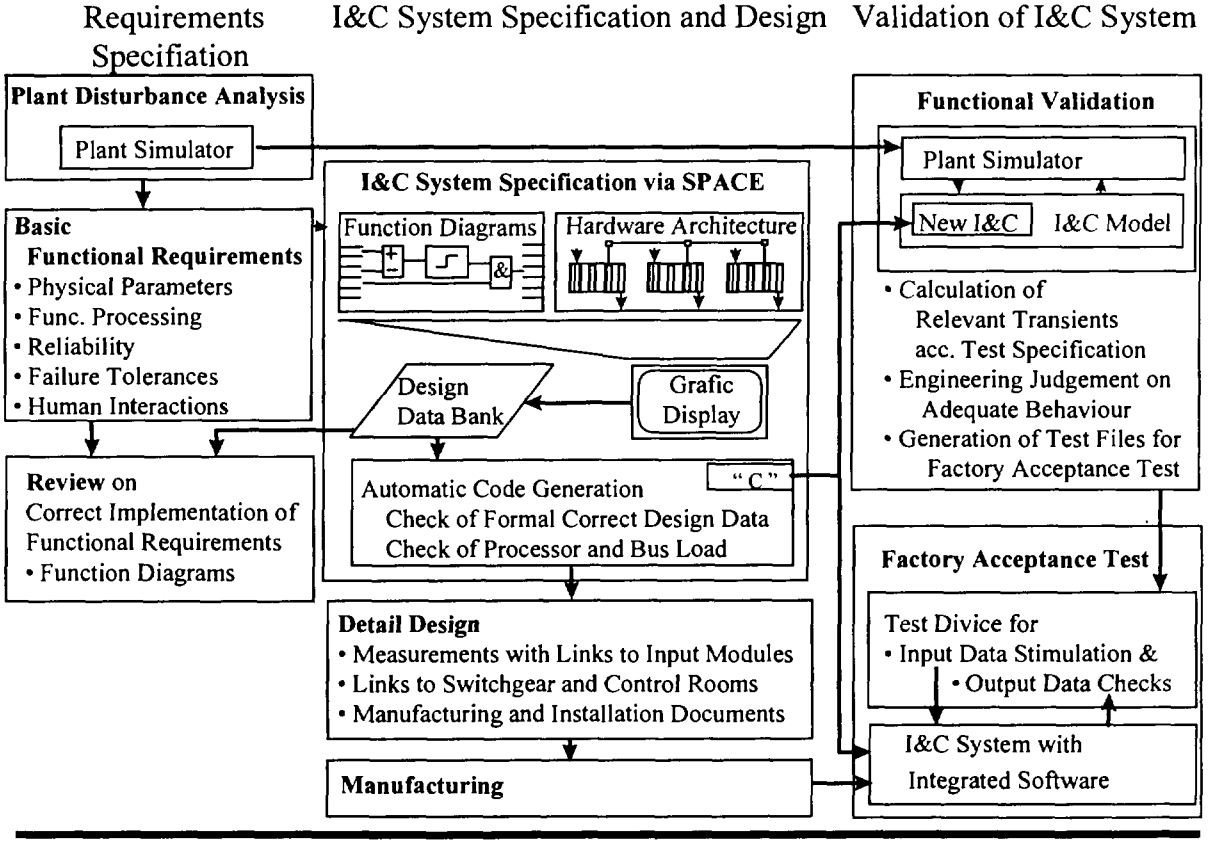
## 2.2 The design of individual I&C safety systems

The quality requirements on the design of individual I&C safety systems form the second level in our strategy to cope CCFs. The main requirements within this design level focus on meeting the „Single Failure Criterion" and ensuring that the functional requirements from the plant process are fulfilled by the application software.

The „Single Failure Criterion" is interpreted such, that in the case of the trip of one of the redundant trains, the designed safety functions are performed without deficiencies on the basis of the measured process information by the available trains. Relevant for ensuring compliance with this requirement are:

- The design of an adequate redundant architecture correlated to the redundant measurements and supply systems and including a suitable voting principle.
- Furthermore, the interference-free communication and the absence of any central synchronising mechanisms between the trains is essential for ensuring the continued operation of the non-tripped trains in the case that one train has failed.

The application software is designed by means of the advanced SPACE engineering system.
To reduce the probability of hidden design errors to the lowest possible extent, the indented functions are designed in the proven format of function diagrams, which are easy-to-understand for I&C engineers as well as for the designer of the mechanical process systems. The I&C system architecture is also designed by means of SPACE such that each function is allocated to a dedicated processor. The code generation is performed for the complete set of functions for a redundant I&C system including all communications.




TELEPERM XS : Quality Management in the Enginering Process

Figure 2 shows the straightforward engineering process to design I&C systems in correlation to the verification and validation phases:

Advanced automatic checks are integrated in the SPACE engineering system to eliminate formal errors of input data. Furthermore, the possibility to design processor and bus loads by optimising the architecture (e.g. by parallel processing) and the functional allocation to different processors inside the I&C system is provided. These checks also include the prediction of the overall response time. The documentation of the I&C system specification - stored in the design data bank - is reviewed against the basic requirements specification.

The most effective possibility to eliminate hidden design errors is provided with the functional validation of the generated application software. For the functional validation, the generated application software (not only the pure code for the designed functionality but the complete code for the redundant system including the communication between the redundant trains) is linked to an already validated simulator code (e.g. on a powerful workstation) and than checked by computing the relevant design transients. As a real time simulator is not required for the functional validation, it is possible to use the same simulator that was already used for the disturbance analysis. The functional validation can additionally be used to generate the input - output data test files for the factory acceptance tests.

For the reactor control and limitation system for the NPP Unterweser (delivery 7/97; 20 cubicles) we had performed in parallel the above mentioned software validation in an „one computer environment" as well as the factory acceptance tests with the integrated system linked to a real time simulator. The comparison of the calculated transients showed excellent correspondence which confirms the deterministic behaviour of the TELEPERM XS system. The possibility of the direct validation of the application software which is later integrated in the target system establishes an advanced possibility to ensure the required functionality as well as to eliminate hidden design errors much better than it was possible for proven technology with hardwired I&C protection systems.

## 2.3 The design of independent I&C safety systems

On the first and second level the focus is laid on features and methods that reduce the probability for remaining hidden design errors to the lowest possible extent.
On the development level of the I&C product system these are the

qualified features to ensure the deterministic system behaviour

and on the design level for individual I&C systems especially these are the

qualified design of the application software including its validation.

As complementary design barrier, on the 3rd level the application of independent I&C safety systems is superposed to ensure that the global safety goals are met despite of an assumed CCF of one of the systems. In the strategy to govern CCFs this forms a deterministic approach by the design of independent I&C systems in such a way that

the synchronous failure of two or more systems can be excluded.

I&C safety systems are not burdened by environmental stress during plant internal accidents (except the sensors inside the containment) and are designed and tested to tolerate plant externally triggered stress conditions from seismic or lightning events in accordance with the relevant standards. Only input data trajectories during plant transients can form potential loadings to trigger the failure on demand of an I&C system by the activation of hidden design errors in the application software. Special care has to be taken for input data

trajectories with partly wrong and inconsistent input data, because the sensors are stressed during the environmental conditions during plant transients.

This fact that hidden design errors in the software can be activated to initiate system CCFs only by specific input data trajectories is discussed in the following:

Essential for managing this generic problem for digital I&C systems are those features which establish the barrier against interferences from the application software on the operating system software and the hardware. This encapsulation of the application software reduces respectively the scope of software which can contain design errors with the potential of CCFs. With the additional quality features of the application software library (capsulated function block modules with consequent operability checks), the I&C system operation cannot be jeopardised by any input data trajectories.

This limitation of process dependent interferences on the application software serves for the following advantage:
As the application software is the only object which is specifically loaded by process depended input data trajectories, only the application software needs to be diverse for realising independent I&C systems which are not vulnerable to fail on this common cause. The application of functional diversity is the most effective way to ensure diverse application software.

Additionally to the barrier against interferences from the application software level on operating system software and hardware the following design requirements have to be met to realise independent I&C systems:

- The main plant safety objectives have to be ensured by independently effective I&C safety systems with
  - different safety functions and as far as possible individual input measurements, to ensure permanently different data trajectories for the independent systems and
  - initiations via independent means (e.g. actuators in the switchgear).
- Absence of direct communication between the independent systems.
- Service activities (e.g. for periodic tests) are permitted only for one of the independent systems and within one system only related to one of the redundant trains at the same time.

For the design of independent I&C systems in cases where the barrier against interferences from the application software on the operating system software cannot be claimed, the application of diversity of the system operating software or even equipment diversity has to be considered instead. The application of diverse I&C systems, however, gives additional burden on the utility with respect to:

- increased costs for qualification and licensing of two different systems
- establishing and maintaining the know-how for servicing two operated systems in parallel
- the more complex configuration management for spare parts and in consequence of modifications of components
- increased potential of errors during a later I&C systems redesign in consequence of process modifications

## 3 Conclusion

The Siemens „Three Level Strategy" is based on proven features of the TELEPERM XS system and enables us to govern the problem of common cause failures of safety I&C systems without the need to apply equipment diversity.
On the first and the second design level the probability of hidden design errors is reduced to an extent that is at least compatible with the proven design for hardwired I&C safety systems. This is achieved by:

- The deterministic system behaviour which is confirmed in the qualification process by independent experts and which ensures that the resultant functionality and behaviour of an individual I&C system corresponds to the application specific design.

- The qualified design process for system architecture and application software based on the SPACE engineering system by means of formal and understandable graphic presentations and the validation of the generated application software to prove its adequate behaviour during design basis accidents.

Based on the confirmed key features of the product system TELEPERM XS and the qualified design process for realising individual I&C systems, independent systems are designed such that a simultaneous failure of these independent systems by a common cause can be excluded.

- Essential is the design according to deterministic requirements to ensure the absence of potential common influencing factors. By the assignment of divers individual safety functions to these independent safety I&C systems, it is ensured that the overall plant safety objectives are met even in the case of an assumed failure of one of these independent systems.