Sensitivity Analysis for the Evaluation of Failure Effects on an I&C Test System

Christian Müller, Ewgenij Piljugin, Jörg Peschke, Manuela Jopen, Dagmar Sommer
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany

Abstract: Modern I&C systems increasingly consist of complex hardware and software-based components. The reliability of software-based I&C systems is highly dependent on the implemented fault detection and handling procedures as well as the architectures of the I&C systems (e.g. to handle common cause failures CCF).

For the model-based evaluation of different I&C architectures with regard to fault propagation, several simplified models of generic I&C systems have been created in the framework of a research project of GRS for the purpose to develop and test a state-of the-art tool for the sensitivity analysis of the various reliability aspects of digital I&C systems. This newly developed methodology is based on a combination of failure mode and effect analysis (FMEA) and fault tree analysis (FTA) as well as the analysis by means of Markov processes for special purposes. On the basis of the developed methodology, the influence of essential parameters (e.g. failure rates of the components, test intervals, repair time, etc.) on the reliability of the various I&C system architectures has been analyzed.

In the follow-up project, the effects of the specified failure modes will be validated and verified based on a testbed. A specified test facility is currently being built at GRS on the basis of real hardware and software (modules of an I&C platform) and the simulation of a simplified process engineering system as provision for generation of suitable input and process feedback signals.

This paper presents the results of the sensitivity analysis of the generic I&C system models as well as the current state of the development of the specified testbed.

Keywords: Architectures, digital I&C system, Modeling, Common Cause Failure (CCF), Fault Tree Analysis (FTA), Markov process, Sensitivity Analysis

1. INTRODUCTION

The developed methodology for the sensitivity analysis of digital I&C systems is a graded approach and based on the application of failure mode and effect analyses (FMEA) [1], fault tree analyses (FTA) [2] and Markov processes [3] and has been published previously [4], [5].

It has been used to analyze a series of model systems of generic I&C architectures with stepwise increased complexity. The next section gives a brief overview of the model systems. The results of the sensitivity analysis to analyze the influence of essential parameter on the reliability of the various I&C system architectures are described in section 3. The development of the GRS testbed is outlined in section 4.

2. MODEL SYSTEMS

The developed model system architectures basically consist of the same generic components (I&C unit level approach for model development [11]): acquisition units (AUs), processing units (PUs) and voting units (VUs). In addition, the VUs are always followed by an analog logic (AL), which is part of the switchgear equipment of the actuators (see figure 1). This modelling assumption is particularly necessary because some model systems have several VUs and their output signals then have to be validated by an n-out-of-m voting. For comparability, systems with a single VU also contain an AL.

The measured signals (e.g. P – pressure value) are digitized within the AUs and subsequently transmitted as data telegrams via the communication network to the PUs. There, the second maximum of the input signals is selected and compared with a limit value. If the limit is exceeded, then a binary control signal is generated and forwarded to the next level of the signal processing (VUs). In the redundant VUs, the incoming binary signals are evaluated by means of an n-out-of-m voting and, if necessary, a control signal for a component (e.g. M - motor) is formed.

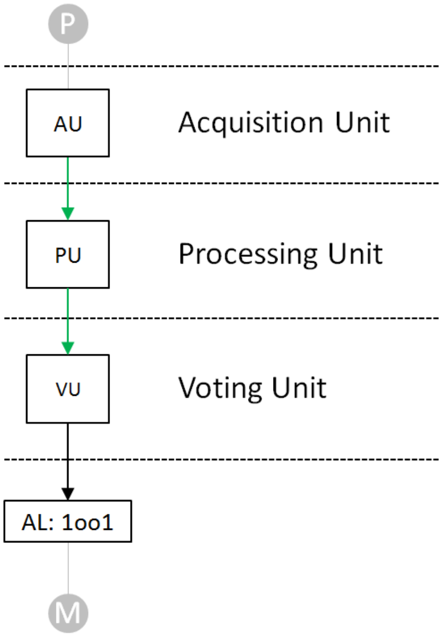

Figure 1: Basic Structure of the Model Systems

In addition, from the moment when the signals have been digitized, they are always marked with a flag that reflects the validity of each signal (“0” - valid, “1” - faulty). In particular, faulty signals are marked, so that they are not further processed on the subsequent level.

Accordingly, two different types of failures are differentiated in the models:

- self-signaling failures (SF) and
- non self-signaling failures (NSF).

The SF are recognized immediately and remedied within a specified repair time. The NSF can be only recognized during periodically repeated tests and then remedied after the specified repair time.

The output signals of the VUs to the AL do not contain error detection information, but self-signaling failures are reported and can be repaired if necessary.

For the considered models the following ancillary assumptions are made:

- The communication from each level of signal processing to the next level is carried out via networks. It is assumed that all hardware failures in the communication networks are always detected and they are therefore always self-signaling. For this reason, the failure rates of the communication paths (for example, between AUs and PUs) are taken into account directly in the failure rates of the corresponding signal-sending components (for example, self-signaling failures of AUs).
- Non self-signaling failed AUs output the minimum possible value.
- Non self-signaling failed PUs output a logical “0”.
- Failed VUs output a logical “0”.
- The software of the AUs, PUs and VUs is not modeled explicitly and the considered failure rates were determined only by probability of the corresponding hardware failures [6], [7].
- Measuring devices, power supplies and interfaces of the I&C systems are not explicitly taken into account in the models.

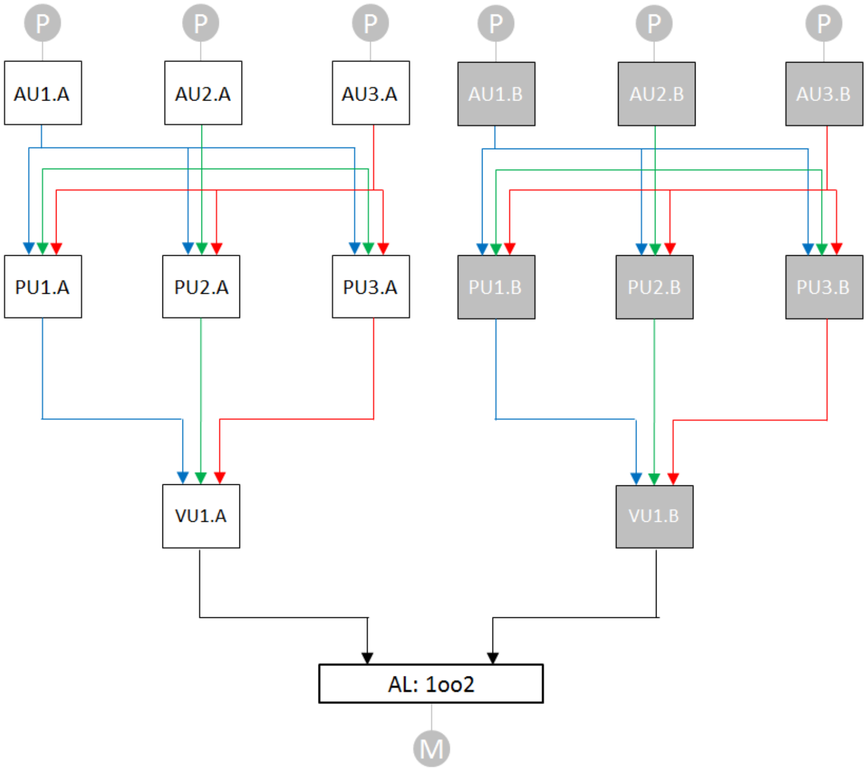

Figure 2: Model system A133B133

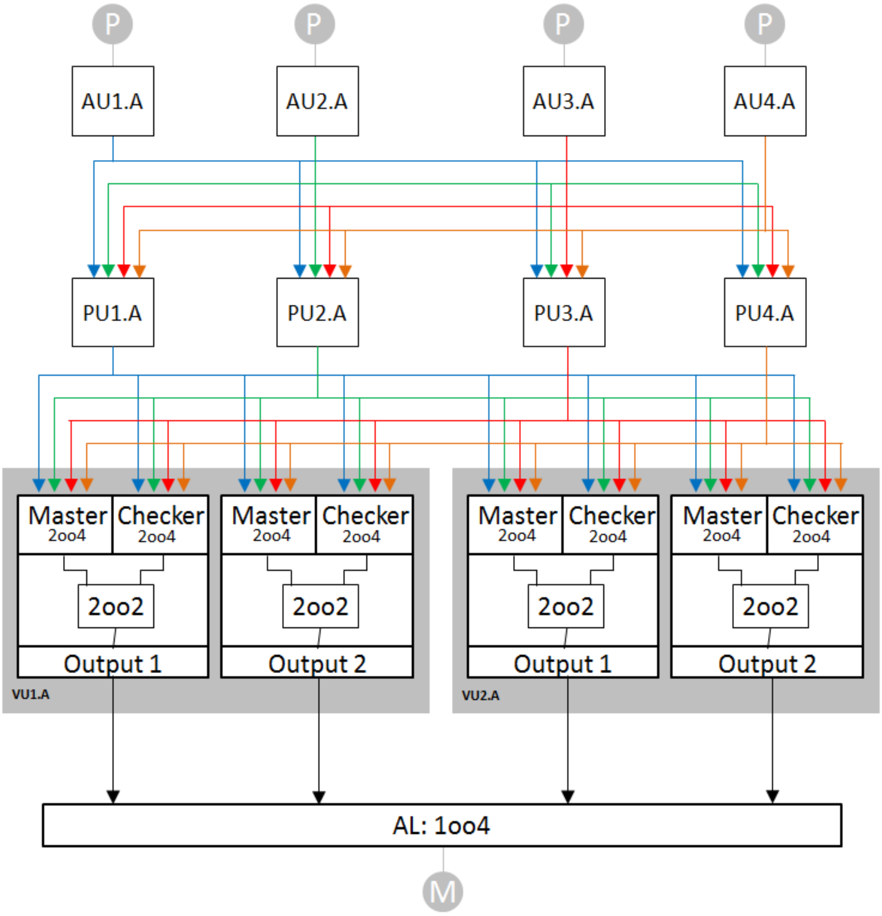

Figure 3: Model system A2MC(2)44

The following model systems have been used for development and validation of the sensitivity analyses:

- A222: 2 VUs, 2 PUs, 2 AUs
- A222 mod: corresponds to model system A222, but here in the two PUs the first maximum instead of the second maximum is compared to the limit value (explanation: see section 3)
- A133: 1 VU, 3 PUs and 3 AUs
- A333: 3 VUs, 3 PUs, 3 AUs
- A133A133: two systems of the type A133 in parallel
- A133B133: two systems of the type A133 (with diverse components - “A”, “B”) in parallel
- A2MC(1)33: 2 VUs (each with 1 sub-unit (Master-Checker)), 3 PUs and 3 AUs
- A2MC(2)44: 2 VUs (each with 2 sub-units (Master-Checker)), 4 PUs and 4 AUs

To give a better impression of the modelling process of different architectures of digital I&C systems, figures 2 and 3 show the model systems A133B133 and A2MC(2)44 as examples.

3. SENSITIVITY ANALYSES

The following subsections show results which have been obtained with RiskSpectrum, which has been used to perform the fault tree analyses [8]. The corresponding fault trees are based on (modified) FMEAs. Further results obtained with Markov processes are not subject of this publication. For more information see [4].

There have been two objectives for the sensitivity analysis of the different I&C system architecture models. On the one hand, it should be proven that the accuracy of the parameters used is more than sufficient. On the other hand, the quality (e.g. robustness) of the different architectures of the modeled I&C systems with respect to variable parameters (e. g. length of test intervals) or only relatively inaccurately known parameters should be investigated.

3.1 Initial Values of All Relevant Parameters

The initial failure rates (FR) of all components of the I&C model systems are shown in table 1. They have been obtained with a modified model of the model described in [7]. It was assumed that a total of 5 % of the failures could be attributed to common cause failures (CCF).

Table 1: Initial Failure Rates of Components

Kind of Failure	Failure Rate	Remarks
AL NSF	$1.000\cdot10^{-10}$ h^{-1}	arbitrary value
AU NSF	$8.265\cdot10^{-8}$ h^{-1}	incl. communication with PUs
AU SF	$2.098\cdot10^{-5}$ h^{-1}	
PU NSF	$8.265\cdot10^{-8}$ h^{-1}	incl. communication with VUs
PU SF	$1.573\cdot10^{-5}$ h^{-1}	
VU NSF	$8.265\cdot10^{-8}$ h^{-1}	no NSF for master-checker configuration
VU SF	$6.972\cdot10^{-6}$ h^{-1}	
VU SF (MC)	$1.029\cdot10^{-5}$ h^{-1}	MC - master-checker configuration
AU CCF	$2.175\cdot10^{-9}$ h^{-1}	CCF of all AUs of one type of system
PU CCF	$2.175\cdot10^{-9}$ h^{-1}	CCF of all AUs of one type of system
VU CCF	$2.175\cdot10^{-9}$ h^{-1}	CCF of all AUs of one type of system
All CCF	$2.175\cdot10^{-9}$ h^{-1}	CCF of all components of one type of system

For the repair time (to correct any failure) a lognormal distribution with an average of 8 hours and a variance of 1 h² was assumed. However, unlike SF, NSF are not resolved until they have been detected during a periodic test. These periodic tests initially take place every 4 weeks in alternating redundancies.

The next sections describe the results of the sensitivity analyses that have been performed. In particular, all analyses focused on failures on demand (which means for the model systems described here “the motor M does not start, although it should”).

3.2 Sensitivity to Changes in Individual Failure Rates

To check the sensitivity of the model systems to changes in failure rates (FR), the initial failure rates for SF and NSF have been increased by an order of magnitude and afterwards reduced by an order of magnitude (in comparison to the initial values). This has been done for each individual component, whereby all other values remained unchanged. The sensitivity to changes in individual failure rates can then be calculated as the ratio S of these two values (this corresponds to a calculation of the sensitivity S with a so-called SensFactor of 10 in RiskSpectrum [8]). The results of these calculations are given in table 2. A sensitivity S of approximately 1 means that no significant change in the results was observed even if the parameter was varied by two orders of magnitude. High values indicate a high sensitivity to changes in that particular failure rate.

Table 2: Sensitivity S of Model Systems to Changes in Failure Rates

Failure Rate	A2MC(2)44	A2MC(1)33	A133B133	A133A133	A333	A133	A222 mod	A222
AL NSF	1.11	1.11	15.30	1.11	1.11	1.00	1.98	1.00
AU NSF	1.00	1.97	1.01	1.00	1.95	1.02	1.55	78.50
AU SF	1.00	1.27	1.00	1.00	1.27	1.01	1.16	1.02
PU NSF	1.00	1.68	1.01	1.00	1.67	1.01	1.15	1.00
PU SF	1.00	1.00	1.00	1.00	1.00	1.00	1.12	1.01
VU NSF	-*)	-*)	3.70	1.04	1.76	13.40	1.12	1.00
VU SF	1.00	1.22	2.65	1.03	1.38	6.94	1.11	1.00

*) it is assumed that VUs in master-checker configuration can only fail self-signaling (see table 1)

Particularly striking is the very high value (78.50) of the sensitivity of the model system A222 to changes in the failure rate of non self-signaling failures of AUs (AU NSF). This results from the selection of the second maximum in the PUs. With only two input signals (from the two AUs), the second maximum is at the same time also the minimum, so that even if one single AU fails (to the minimum value, see assumptions in section 2), the entire system becomes unavailable. This weakness was corrected in the model system A222 mod by comparing the first maximum with the limit value inside the PUs instead of the second maximum.

Another high value of 15.30 for the failure rate of non self-signaling failures of the AL (AL NSF) for the model A133B133 is explained by the very high quality of this system (see also figures 4, 5, 6). All model systems only have a single AL, meaning that their failure always leads to the unavailability of the entire system. In case of A133B133, however, the overall probability of a failure on demand is already so small that, contrary to the original assumption, a failure rate of $1 \cdot 10^{-10}$ h^{-1} for the AL is no longer negligible in this case.

The last relatively high value of the sensitivity (13.40) for the failure rate of non self-signaling failures of VUs (VU NSF) for the model system A133 results from the fact that this system has only one single VU. Here, too, a single failure can already make the system unavailable.

3.3 Sensitivity to Changes in Time between Tests

Originally it was assumed that the individual redundancies are tested alternately every four weeks to detect and, if necessary, correct NSF. A variation of the time intervals between these tests yields the results in figure 4. Apart from the absolute values, all model systems show a similar behaviour.

There are clearly three distinct groups of model systems. First of all, the two model systems A222 and A133 show a relatively high probability of a failure on demand. In both cases, this is due to the fact that already single failures can lead to a failure on demand (see previous section). The second group of model systems with significantly better availability is characterized by the fact that no single failure can lead to a failure on demand due to the availability of redundant components.

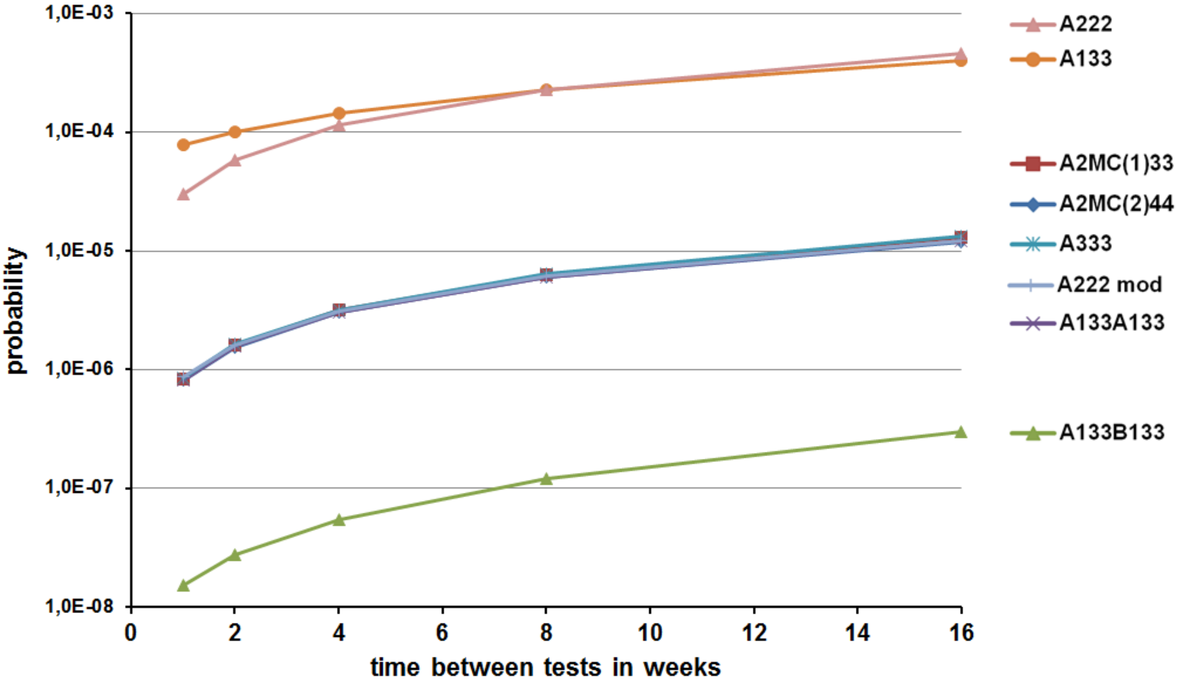

Figure 4: Probability of Failures on Demand as a Function of Time between Tests

Even better, in terms of avoiding failures on demand, is the model system A133B133. This model system not only has a redundant structure (against single failures), but also diverse subsystems (A and B) to counter common cause failures (CCF).

3.4 Sensitivity to Changes in Repair Time

In order to investigate the influence of the assumed repair time (of failed components) on the failure probabilities of the model systems, the repair time has been raised successively from 0 h to 500 h (in each model system for all AUs, PUs and VUs as well as both types of failure (NSF and SF) in common). Basically, the probability of failures on demand increases for all model systems with longer repair time (figure 5).

The biggest relative change of the probability of failures on demand with increasing repair time belongs to model system A133B133. But it loses its top position as the most reliable model system (with the lowest probability of a failure on demand) only above approximately 350 h (> 2 weeks of repair time), which should be well above realistically expected repair times.

In addition, it has also been analyzed wether the variance of the repair time (width and asymmetry) has an influence on the result. It turned out that the variance for all average repair times and model systems has no influence on the total failure probabilites.

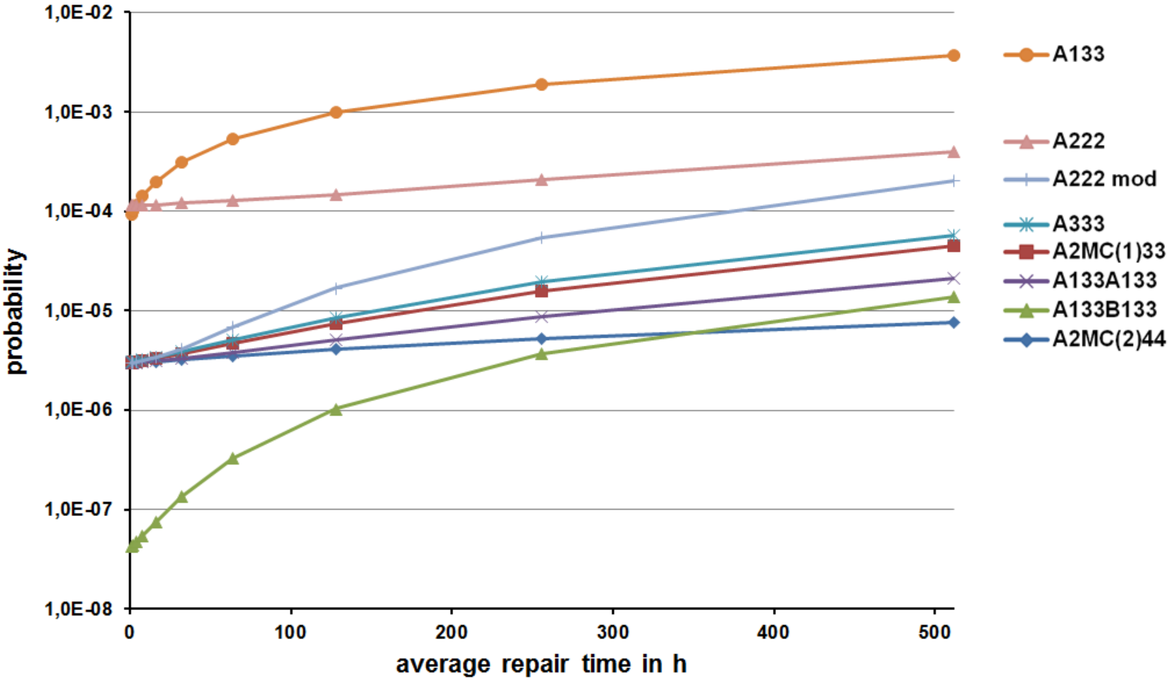

Figure 5: Probability of Failures on Demand as a Function of Average Repair Time

3.5 Sensitivity to Changes in Percentage of CCF

The varying proportion of CCF on the overall failure rate of each individual component has been calculated as follows. The starting point is a known or assumed failure rate for a specific type of component and failure (e.g. from the operating experience or in our case from the modeling of a system [7]). An unknown percentage of this failure rate is caused by CCF. This proportion (x %) has been assumed to be based in half on CCF of the total system (all components) and the other half on CCF of that particular type of component (e.g. AUs). Since the overall failure rate for the individual components remains constant for the different percentages of CCF, the failure rates for individual failures of components has to be changed in a way that the overall failure rates for the components stay constant. In this way the percentage of CCF has been varied between 0 % and 15 %.

As a rule, the probability of a failure on demand increases significantly with the percentage of CCF for the different model systems. Exceptions here are the two model systems, whose (relatively high) total failure probabilities are dominated by single failures of components (A222 and A133), and the model system A133B133. The latter one has a constant low probability of failures on demand because of its structure of relatively uncomplicated but diverse subsystems (A, B).

Although it is not yet known exactly how large the percentage of CCF of the overall failure rate of digital I&C systems is, figure 6 clearly shows that the use of diverse systems (assumption: no CCF between diversified hardware or software) has a clear advantage even for very small percentages of CCF (< 1 %), even compared to highly redundant systems (such as A2MC(2)44).

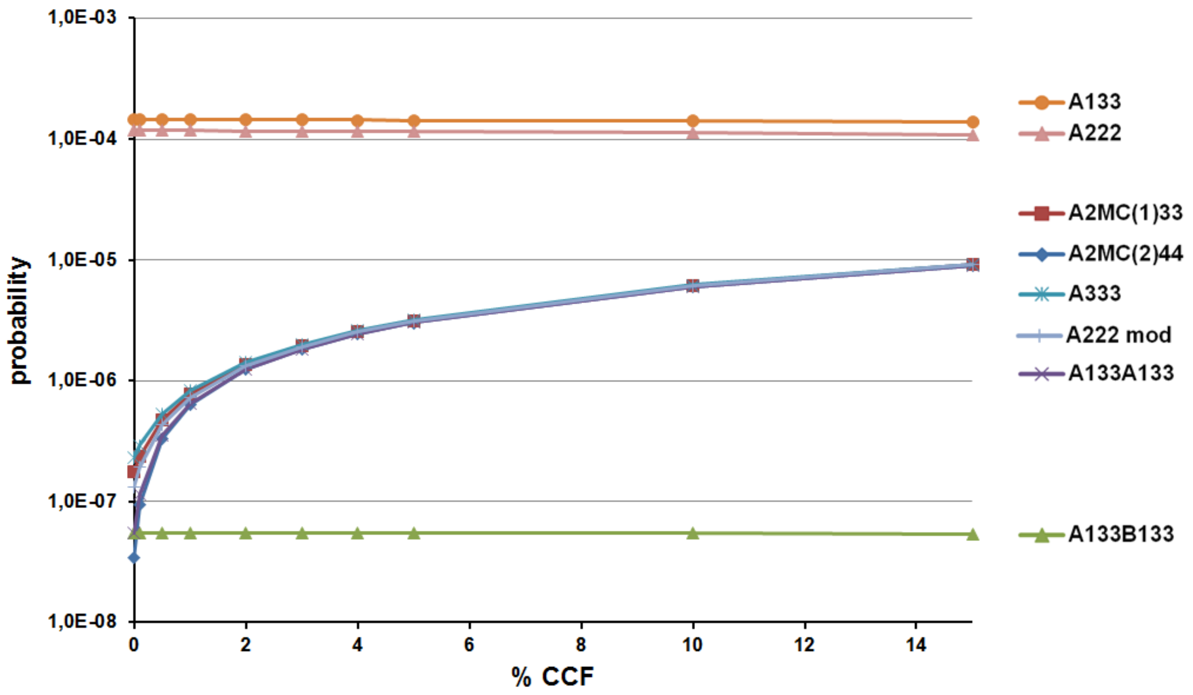

Figure 6: Probability of Failures on Demand as a Function of Percentage of CCF

4. DEVELOPMENT OF AN I&C TEST SYSTEM

Currently, a test facility consisting of a simulated process engineering system, real digital I&C equipment and a simulated I&C system is under development at GRS. Figure 7 shows the basic structure of this test environment. The design of this test system is part of a follow-up project at GRS and is still in its early stages.

The simulated process engineering system (e.g. fuel pool) will provide an interface to the testbed equipment as adequate input and output channels for the real and the simulated process parameters. The simulations are developed using MATLAB (with Simulink) [10]. After completion of the test environment, specific failures can be injected into the simulated and also into the real part of the testbed system. The comparison between the simulated and the real I&C system allows the validation of the simulated I&C. Subsequently, the simulated I&C system can be used to examine, in particular, those failures that are inaccessible to the real I&C system (e.g. because hardware would be corrupted).

The focus is currently on the modification and commissioning of a testbed I&C system based on Teleperm XS [9].

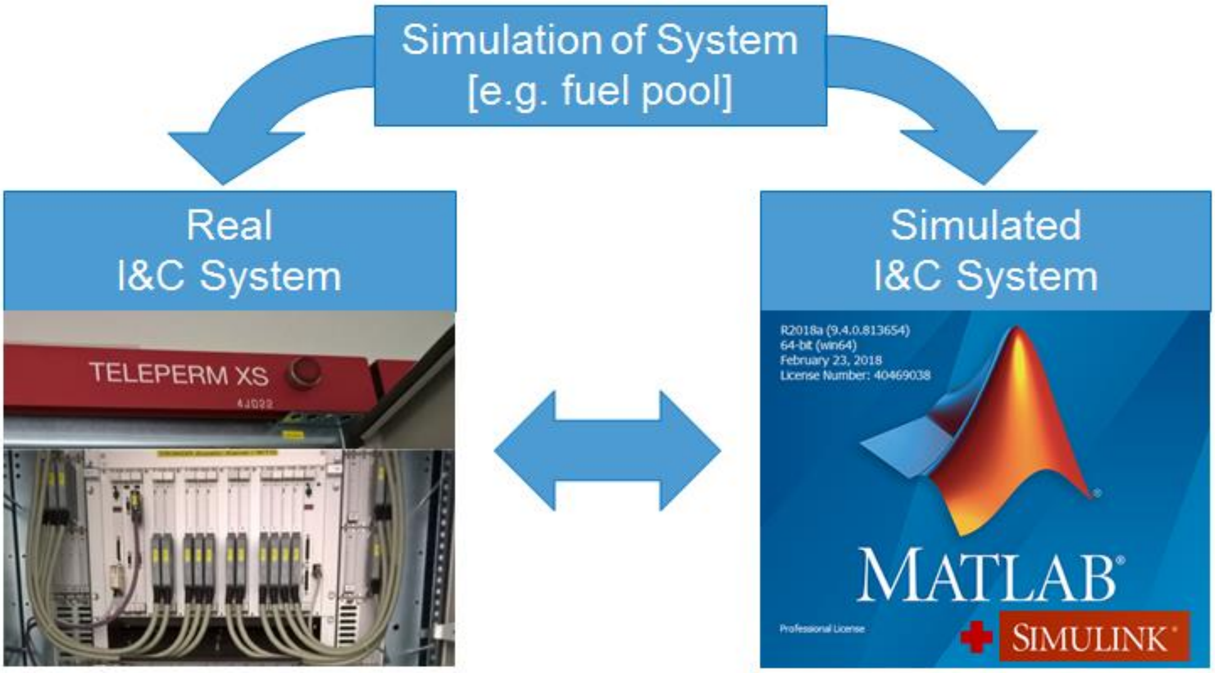

Figure 7: Basic Structure of I&C Test Environment

5. CONCLUSION

On the basis of a FMEA and a FTA as well as the analysis by means of Markov processes, a new methodology for the sensitivity analysis for the evaluation of failure effects on I&C systems has been developed. The model systems and architectures used for development and validation as well as the results of the sensitivity analyses have been presented.

The sensitivity of the model systems to the variation of failure rates of individual components has expected effects on the overall reliability of the system function and is therefore to be understood as a quality feature of the analyzed type of I&C system (and is less suitable to compare different architectures).

Basically, the likelihood of a system failure increases for all model systems with longer repair times, with architectures with higher redundancy of the signal processing (without consideration of the AL) reacting much less sensitive to the variation of repair times. In a similar way, all model systems responded to the extension of test intervals in a similar and expected manner with a higher probability of failure, whereas architectures with higher redundancy generally react less sensitive to the variation of the test intervals of individual subsystems.

The sensitivity analysis with respect to CCF showed that the probability of a system failure generally increases significantly with the percentage of CCF. One exception was the model system A133B133, whose architecture consists of diverse subsystems (assuming complete diversity of hardware and software). This model system has a consistent low probability of failures for all proportions of CCF. Despite the fact that there are no reliable findings regarding the real proportion of CCF for digital I&C systems, the evaluation has shown that diverse I&C architectures already offer a clear advantage even for very small percentages of CCF (< 1%) (even compared to very complex and highly redundant systems).

It turned out that the tools of the fault tree analysis (inter alia separate failure analysis of non-binary logic, fault tree modeling, analysis of minimal cuts, integrated sensitivity analysis of the RiskSpectrum software) can efficiently model and analyze a large number of different architectures of digital I&C

systems. In this way, many redundant architectures of modern digital I&C systems can be examined with many components, whereby CCF can also be comprehensibly taken into account in the hardware and software.

It is planned to continue the further development of analysis methods and tools in a follow-up project. In particular, GRS is currently developing a new test facility consisting of a combination of a simulated process engineering system as well as a real and a simulated I&C environment.

Acknowledgements

The authors want to acknowledge the support provided by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety for funding the GRS development of the methodological approach to the sensitivity analysis of failure effects in modern digital I&C systems and the development of the I&C test system.

References

[1] "*Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*", IEC 60812:2006 (2006)

[2] "*Fault Tree Handbook*", U.S. Nuclear Regulatory Commission, NUREG-0492 (1981)

[3] M. Röwekamp, W. Faßman, W. Frey, L. Gallner et al., „*Development and Test Application of Methods and Tools for Probabilistic Safety Analyses*", GRS-A-Bericht, GRS-A-3558 (2010)

[4] C. Müller, J. Peschke, E. Piljugin, „*Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik*", GRS-A-Bericht, (2018), to be published

[5] C. Müller, J. Peschke, E. Piljugin, D. Sommer, „*Methodological Approach to the Sensitivity Analysis of Failure Effects in Modern Digital I&C Systems*", 10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC-HMIT), American Nuclear Society (ANS) (2017)

[6] E. Piljugin, J. Märtz, H. Heinsohn, W. Frey, „*Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik*", GRS-A-Bericht, GRS-A-3258 (2004)

[7] J. Herb et al., „*Entwicklung eines Ansatzes zur Analyse der Netzwerktechnologien in sicherheitsrelevanten Leittechniksystemen hinsichtlich Verbreitung und Auswirkung postulierter Fehler*", GRS, GRS-377 (2015)

[8] RiskSpectrum PSA, Lloyd's Register Consulting - Energy AB, Sweden (http://riskspectrum.com/)

[9] Teleperm XS, Framatom GmbH (formerly known as AREVA NP GmbH), Erlangen, Germany (http://areva.com)

[10] MATLAB/Simulink, The Mathworks GmbH, Aachen, Germany (http://mathworks.com/)

[11] "*Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis Nuclear Safety*", OECD Nuclear Energy Agency (NEA), NEA/CSNI/R(2014) (2015)