Estimation of specific Common Cause Factors for Digital I&C Modules in the PSA

Mariana Jockenhövel-Barttfeld[a*], Yousef Abusharkh[a], Christian Hessler[a] and Heiko Kollasko[a]
[a] Framatome GmbH, Erlangen, Germany

Abstract: Instrumentation and control (I&C) systems of power plants are upgraded from analog to digital as part of the operating life extension of nuclear plants. The impact of such a modernization on the plant is usually assessed using the probabilistic safety analysis (PSA) in an early phase of the modernization project. Common cause failures (CCF) of hardware modules are one of the main contributors to the reliability results, given the redundant design of safety-relevant I&C architectures. For this reason, component-specific CCF parameters are very important input data for the impact assessment and risk evaluation of the I&C modernization using the PSA. This paper presents a methodology for estimating CCF-parameters of I&C modules using the digital system platform TELEPERM XS for safety I&C developed at Framatome for illustration purposes. The use of the estimated CCF parameters considerably improves the reliability of the I&C functions, leading to more realistic PSA results. In addition, the CCF parameters assessment also validates the conclusions found in the literature and confirms that simple CCF models for safety-instrumented systems, such as the Multiple Beta Factor model proposed in the Standard IEC 61508, lead to reasonable results and are sufficient.

Keywords: Digital hardware module, common cause failure, Alpha Factor model.

1. INTRODUCTION

Instrumentation and control (I&C) systems are upgraded from analog to digital as part of the operating life extension of nuclear power plants. The impact of such a modernization on the plant (e.g. on the total core damage frequency) is usually assessed using the probabilistic safety analysis (PSA), usually in an early phase of the modernization project or even before the project is launched.

The assessment of the digital I&C reliability in the PSA is a challenging task. First, the level of modelling detail to be adopted in the PSA (e.g. at I&C module level, I&C unit level) has to be decided. This is an important point given the large number of I&C functions processed by different I&C systems, which are usually considered in the PSA. A too detailed I&C modelling can lead to a PSA model which is difficult to handle as well as to results (i.e. minimal cut sets) which are difficult to interpret. As pointed out in NUREG/CR-6962 [1], reliability analyses of digital systems have to be developed to a level of detail that captures the design features affecting the system reliability, provide the outputs needed for risk evaluation, and for which probabilistic data is available. In addition, special features of digital systems, such as fault-tolerance and fault-coverage[†] design features, should be captured in the reliability modelling, as well as the dependencies between the I&C functions and systems[‡] involved in the PSA (for more details, refer e.g. to [2]).

[*] mariana.jockenhoevel-barttfeld@framatome.com
[†] Capability of the I&C system to diagnose failures and to re-configure to reduce or eliminate the impact of the failure. The fault detection coverage is a measure of the system ability to perform the fault detection, isolation and recovery.
[‡] The dependency between I&C systems can be given, for example, if the systems acquire the same measurements.

One of the main contributors to the failure of I&C functions are the common cause failures (CCF), given the redundant design of safety-relevant I&C systems. For this reason, the use of component-specific CCF parameters is a crucial point for the impact assessment and risk evaluation of the I&C modernization using the PSA. The use of too conservative CCF parameters can lead to an overestimation of the CCF potential of the hardware modules and may hide real risk contributors and lead to unnecessary complexity of the I&C design.

CCF parameter data collections are available for many populations of mechanical components, such as the Alpha Parameters in NUREG/CR-5497 [3]. However such data collections are not available for I&C components. As a consequence, generic CCF parameters have to be used for I&C modules, such as those reported in NUREG/CR-5497 [3] for components for which no operating experience is available. The use of generic CCF parameters leads to very conservative reliability results, which do not reflect the specific characteristics of the digital I&C systems operation, for which CCF events are seldom observed[§]. In addition, the overestimation of the CCF potential may hide the real risk contributors and may lead to unnecessary complexity of the I&C design. Another possibility is to use the less conservative Beta Factors suggested by the IEC 61508 [4] for the Multiple Beta Factor Model, however with difficulties to justify the proposed values.

This paper presents a methodology for estimating CCF parameters of I&C modules using the TELEPERM XS safety system platform developed at Framatome for illustration purposes. The methodology includes an analysis of the TELEPERM XS operating experience and identifies relevant events for the quantitative analysis (see Section 3), which follows the approach suggested in NUREG/CR-6268 [5] to estimate CCF parameters using impact vectors (see Section 4). The paper illustrates the CCF parameters estimation for different groups of I&C modules relevant for the PSA (e.g. input/output modules, priority control modules, see Section 5.1), the impact of the selection of different CCF models and parameter sources (see Section 5.2) and the impact of using specific CCF parameters on the reliability of I&C functions (see Section 5.3). In the next chapter, CCF for I&C modules are first briefly defined.

2. COMMON CAUSE FAILURES OF I&C MODULES

A CCF affecting an I&C system is defined as a result of a triggering event causing coincident failures of two or more separate divisions (channels) in a multiple channel system. According to this, common cause failures of hardware modules can result from:

- Systematic faults (e.g. errors introduced in the design, specification, installation, maintenance) leading to the so called *simultaneous CCF*, which denotes that the failure of redundant channels occur simultaneously, or
- The accumulation of independent random faults in redundant channels, which remain undetected in the system during a critical time interval until the faulty modules are requested to operate (operating demand or testing), turning the hidden faults into a failure. This is a so called *non-simultaneous CCF* because the faults are randomly distributed in time but linked through demand (dependency).

The concept of a non-simultaneous CCF is also defined in the Standard IEC 61508 [4], which states that there is a finite associated probability that independent random hardware failures occur in all channels of a multi-channel system. As a result, all of the channels are simultaneously in a failed state, if these components were requested to operate.

[§] This is because of the monitoring features of digital I&C systems (e.g. diagnostic tests), which reveal a large fraction of the hardware failures before they can accumulate and affect redundant channels.

In view of probabilistic analyses and based on NUREG/CR-6268 [5], the definition of a CCF event consists of components failures that meet the following four criteria:

1. Two or more individual redundant components of the same/similar failure, are degraded or have deficiencies that would result in component failures if the components had been requested to operate through a demand,
2. Components fail within a selected period of time such that success of the PSA mission would be uncertain,
3. Components fail because of a single shared cause and coupling mechanism, and
4. Components fail within the established component boundary.

Dependent failures can therefore be thought of as resulting from the coexistence of two factors. A susceptibility for components to fail (simultaneously or non-simultaneously) from a particular failure cause and a coupling mechanism that creates the conditions for multiple components to be affected by the same cause.

3. CCF DATA ANALYSIS PROCESS

Component-specific CCF parameters can be estimated if operating experience of the digital platform is available. In this paper, the digital I&C platform for safety I&C TELEPERM XS is considered for illustration purposes.

The TELEPERM XS operating experience is based on feedback collected during the last 20 years from several sources of information, such as feedback from the development, engineering, integration test fields and commissioning as well as feedback from customers worldwide, and includes quantitative (operating time, number of failures) as well as qualitative data (nature of failures, root-cause investigations). The analysis of events observed until end of 2016 during commissioning and commercial operation of these reference plants is used as a piece of evidence for estimating CCF parameters for a target (generic) plant.

The analysis focuses on events with the potential of affecting the plant safety or availability as possible candidates for the identification of *CCF events* (see definition in Section 2) or *potential CCF events* caused by failures of hardware modules.

The concept of potential CCF events has been also considered in the CCF analysis done in NUREG/CR-6268 [5] and in the guidelines defined in NUREG/CR-5485 [6]. In this analysis, potential CCF events are events observed in the plant, where one or more components within one division (i.e. non-redundant components) are revealed to be faulty and no failures of redundant components can be identified. Although the redundant components did not fail they share the same cause and could be affected by the same coupling mechanism (trigger). The term potential CCF event is used from a practical point of view, to capture a broader category of CCF events, that includes all foreseeable causes that may result in a CCF based on the review of recorded failures and causes. Even when using a practical CCF definition, it is very challenging to decide whether a failure event is a CCF or not when performing the data analysis and classification.

4. QUANTITATIVE ANALYSIS OF CCF EVENTS

The quantitative analysis of CCF events is based on the definition of *impact vectors* given in NUREG/CR-6268 [5], which assesses the failure impact of a CCF event on a system, providing a numerical representation of the event. The CCF parameters are assessed using estimators, which provide an expression that relates measurable quantities that can be obtained from the operating experience.

According to NUREG/CR-6268 [5], for a component group of size *m* the impact vector has *m*+1 elements. The *k*+1 element, denoted by F_k , equals 1 if the failure of exactly *k* components occurred and 0 otherwise:

$$I = [F_0 , F_1 , F_2 , ..., F_m] \quad (1)$$

Possible impact vectors for a two-component system are:

[1, 0, 0] no component failed
[0, 1, 0] one component failed (independent failure)
[0, 0, 1] two components failed due to a shared cause

The use of failure vectors also allows for a systematic way to record CCF events and for treating uncertainties in the event classification. CCF events usually have uncertainties associated to the number of affected components or the event description is not clear. In these cases the event classification may involve the definition of different hypothesis, each providing a different interpretation of the event, such as (see NUREG/CR-6268 [5]):

- Events involving degraded component states
- Events involving multiple component failures closely related in time but not simultaneously
- Events involving multiple failures for which the presence of a shared cause cannot be established with certainty.

This analysis assumes a common cause component group (CCCG) size of four (four redundant divisions with a 2-oo-4[**] success criterion). This is a realistic assumption because most of the safety-relevant I&C systems are built with four redundancies. In this case, each CCF event *j* has an associated total impact vector $\overline{I_j}$ defined as:

$$\overline{I_j} = \left[\overline{F_{0,j}}, \overline{F_{1,j}}, \overline{F_{2,j}}, \overline{F_{3,j}}, \overline{F_{4,j}}\right] \quad (2)$$

with

j: denoting the CCF events, with *j* = 1, 2, …, *J*, being *J* the total number of CCF events found in the operating experience

$F_{k,j}$: being the *kth* element of the impact vector for event *j* (failure of *k* components out of four).

[**] The system is successfully actuated if at least two-out-of-four divisions are actuated. The system fails it at least three-out-of-four divisions fail.

5. RESULTS

This section presents the component-specific CCF parameters for digital hardware modules estimated from the TELEPERM XS operating experience (see Section 5.1). The impact of the selection of CCF models and parameter sources for I&C modules in the PSA is assessed in Section 5.2. Finally the impact of using hardware-specific CCF parameters on the estimation of the probability of failure on demand of one I&C function is illustrated in Section 5.3.

5.1. Results of estimated TELEPERM XS-specific CCF Parameters

The estimated Alpha parameters are illustrated for two populations of TELEPERM XS hardware modules: input and output (I/O) modules and priority control modules. For these modules no evidence of CCF events could be found in the operating experience. For this reason, the main focus lies on the analysis of potential CCF events. As previously described, potential CCF events usually involve failed components in only one redundancy and shared causes and triggers can be identified, which could potentially affect redundant components.

The Alpha factor values for the I/O and the priority control modules are presented in Figure 1 in comparison with the generic Alpha factors from NUREG/CR-5497 [3] for a CCCG size of four.

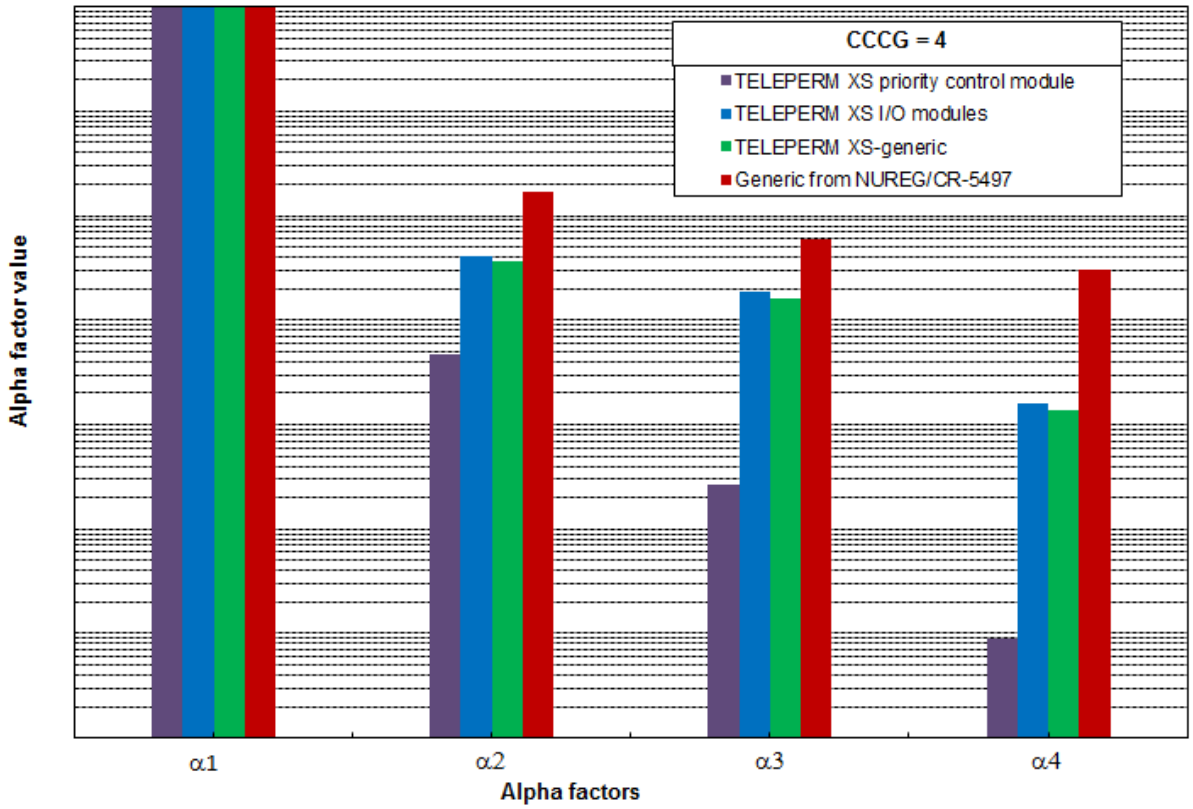

Figure 1: Estimated Alpha factors for TELEPERM XS for a CCCG = 4 in comparison with generic Alpha factors from NUREG/CR-5497

Additionally, a TELEPERM XS-generic population was built out of these specific component groups in order to estimate TELEPERM XS-generic Alpha parameters to be use in the PSA (see Figure 1). Generic specific CCF parameters of the digital platform can be very useful for the PSA, especially if the reliability modelling is done at an “I&C unit level” (instead of at a “module level”, see Section 1). Note that the TELEPERM XS-generic Alpha parameters estimated in this analysis are considerably lower than the generic parameters from NUREG/CR-5497 [3] estimated for mechanical components. These result proves that the generic parameters from NUREG/CR-5497 [3] are very conservative for

I&C modules and do not reflect the characteristics of digital I&C systems for which CCF events are seldom observed.

The TELEPERM XS-generic Alpha parameters shown in Figure 1 can be extended to other CCF common cause group sizes using mapping techniques (see NUREG/CR-6268 [5]). Also for CCCG sizes two and three, the TELEPERM XS-generic Alpha parameters are considerably lower than the generic values from NUREG/CR-5497 (see Figure 2).

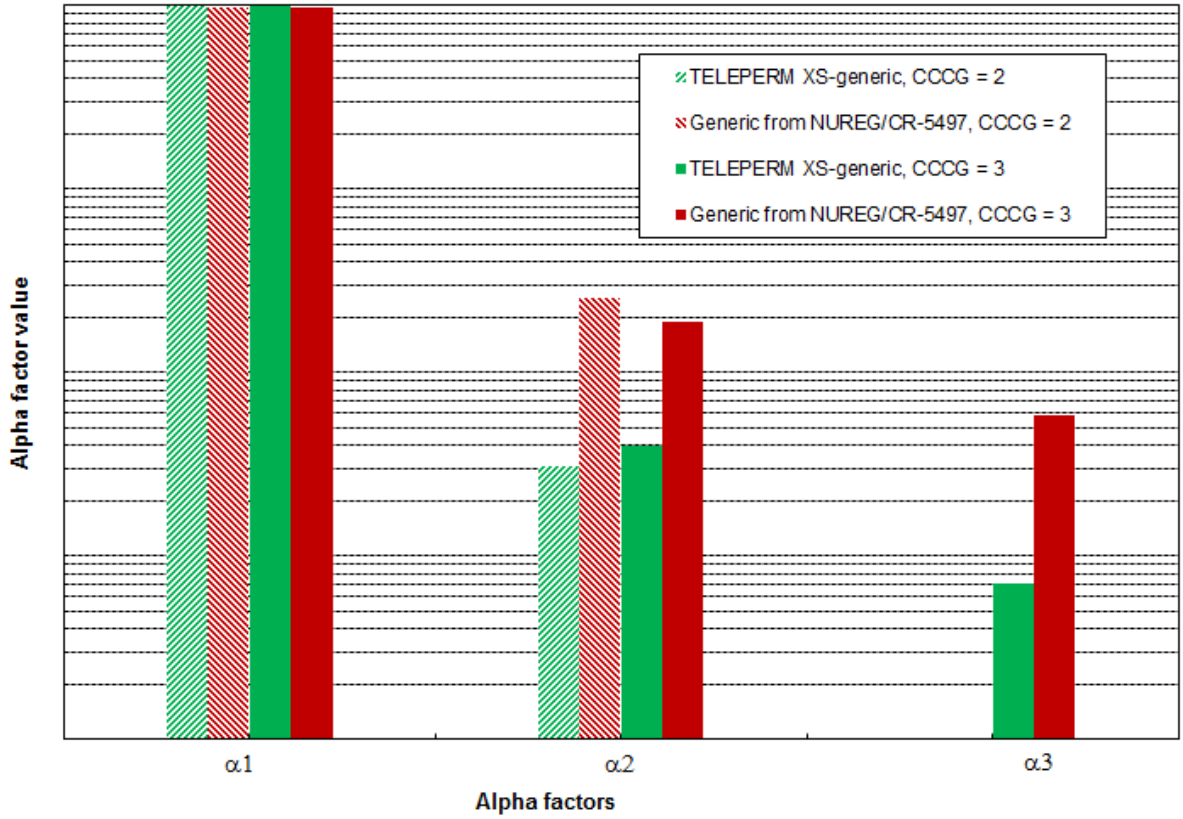

Figure 2: Estimated Alpha factors for TELEPERM XS-generic Alpha factors for CCCG = 2 and CCCG = 3 in comparison with generic Alpha factors from NUREG/CR-5497

5.2. Impact of the Use of Different CCF Models and Parameters Sources

For the purpose of comparing different CCF models and parameter sources for I&C modules, the *probability of failure on demand (PFD) due to CCF* of a four-redundant system with a success criterion of 2-oo-4 (Q_{CCF}) is estimated as:

$$Q_{CCF} \approx 4\,Q_3^4 + Q_4^4 \tag{3}$$

with Q_3^4 and Q_4^4 as the probability of three-out-of-four and four-out-of-four failed divisions. The PFD for a CCCG size of four (failure of at least three components due to CCF, estimated with equation (3)) is shown in Figure 3 as a fraction of the total failure probability[††] using different CCF models. The estimated PFD due to CCF using TELEPERM XS-generic Alpha factors is approx. five times lower than the value obtained using the generic Alpha factors from NUREG/CR-5497. This result validates again the fact that the generic non-specific Alpha factors are not suitable for digital I&C modules.

[††] The total failure probability (Q_T), defined as $Q_T = Q_{IND} + Q_{CCF}$, is estimated as the independent failure probability (Q_{IND}), under the assumption that $Q_{CCF} << Q_{IND}$.

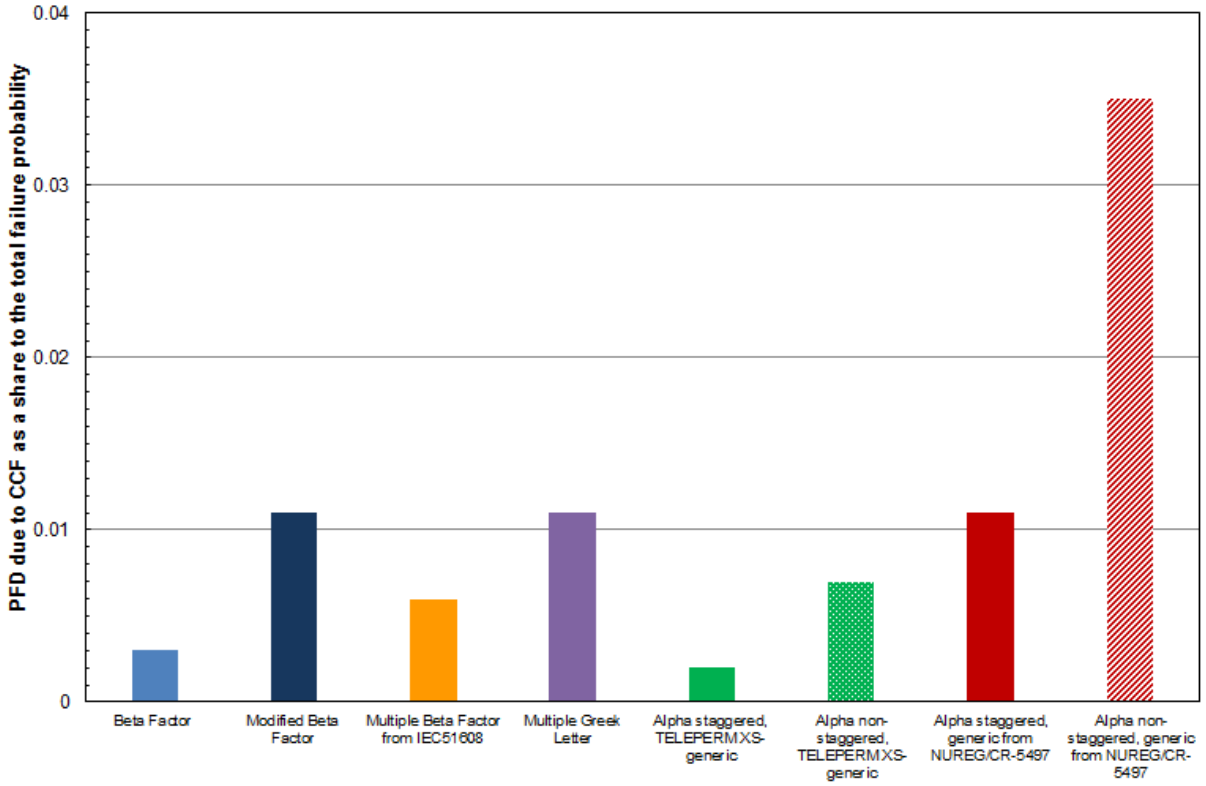

Figure 3: Comparison of estimations of PFD due to CCF for a CCCG size of four (2-oo-4) using different CCF models and parameter sources

Figure 3 also shows a comparison of the results using TELEPERM XS-generic Alpha factors and the Modified Beta Factor factors suggested by the IEC 61508 [4]. The PFD due to CCF estimated using TXS-generic Alpha factors and a non-staggered testing strategy is slightly higher than the PDF obtained with the Modified Beta Factor factors from IEC 61508 (see Figure 3). If a staggered testing strategy is assumed, the PFD due to CCF estimated using TELEPERM XS-generic Alpha factors is approx. three times lower than the value obtained with the Modified Beta Factor factors from IEC 61508 [4].

These results validate the conclusions found in the existing literature (e.g. [7]), which state that simple CCF models for safety-instrumented systems, such as the Modified Beta Factor model, lead to reasonable results and are sufficient.

5.3. Impact of the Use of Specific CCF Parameters on the PFD of one I&C Function

The estimated TELEPERM XS-generic Alpha parameters presented in the previous section were tested in one fault tree model which estimates the probability of failure on demand of the I&C function "Auxiliary Feedwater Signal". In this fault tree model CCCG sizes of 2, 3 and 4 are involved.

The following results were obtained:

PFD estimated with generic Alpha factors from NUREG/CR-5497 [3]	1.08E-05/demand
PFD estimated with TELEPERM XS-generic Alpha factors	3.56E-06/demand

This example illustrates the important reduction of the PFD (approx. 66%) achieved by using specific-CCF parameters in the fault trees modelling the I&C functions reliability.

6. CONCLUSION

This paper presented a methodology for estimating specific CCF parameters for I&C modules, which can be applied if operating experience of the digital platform is available.

The TELEPERM XS digital platform was considered for illustration purposes. No evidence of CCF events could be found in the analysis of the TELEPERM XS operating experience of input/output and priority control modules. For this reason, the event assessment was based on the definition of *potential CCF event*, which are characterized by failures of modules affecting only one redundant channel.
The quantitative analysis of CCF events is based on the definition of impact vectors given in NUREG/CR-6268 [5], which assess the failure impact of a CCF event on a system, providing a numerical representation of the event. The CCF parameters are assessed using estimators, which provide an expression that relates measurable quantities that can be obtained from operating experience. The use of failure vectors also allows for a systematic way to record events and provides a systematic way for treating uncertainties in the events classification.

The use of the estimated CCF parameters considerably improves the reliability of the I&C functions involved in the PSA, leading to more realistic results. The use of realistic CCF parameter for the I&C systems is very important, when using the PSA to assess the risk impact of I&C modernizations from analog to digital systems. Otherwise, the overestimation of the CCF potential may hide real risk contributors and may lead to unnecessary complexity of the I&C design.

In addition, the CCF parameters assessment also validates the conclusions found in the literature and confirms that simple CCF models for safety-instrumented systems, such as the Multiple Beta Factor model proposed in the IEC 61508 [4], lead to reasonable results and are sufficient.

Future work involves the analysis of further TELEPERM XS modules to update the TELEPERM XS-generic CCF parameters.

References

[1] NUREG/CR-6962 "*Traditional Probabilistic Risk Assessment Methods for Digital Systems*".

[2] M. Jockenhövel-Barttfeld, S. Karg, C. Hessler and H. Bruneliere "*Reliability Analyses of Digital I&C Systems within the Verification and Validation Process*", Probabilistic Safety Assessment and Management PSAM 14, September 2018, Los Angeles, CA.

[3] NUREG/CR-5497 "*CCF Parameter Estimations 2015*", update to NUREG/CR-5497 from May 1998; October 2016.

[4] IEC 61508 "*Functional safety of electrical/electronic/programmable electronic safety-related systems*", 2010

[5] NUREG/CR-6268 "*Common-Cause Failure Database and Analysis System: Event Data Collection, Classification and Coding*".

[6] NUREG/CR-5485 "*Guidelines on Modelling Common-Cause Failures in Probabilistic Risk Assessment*".

[7] H. Jin, M. A. Lundteigen and M. Rausand "*Common-cause failures in safety instrumented systems*", PSAM 11 & ESREL 2012, p. 6121-6131.