Estimating Common Cause Failure Probabilities for a PRA Taking into account Different Detection Methods

Kalle E. Jänkälä
Fortum Power and Heat Oy, Espoo, Finland

Abstract: The methodology to estimate residual parametric common cause failure (CCF) probabilities consists of the selection of the data source, source plants, source systems and component type, failure mode, assessment of the impact vectors, determination of equivalent observations, calculation of CCF rates of different multiplicities with uncertainties using an empirical Bayes estimation method and finally determining explicit CCF basic events and their probabilities to be used in the probabilistic safety assessment model. The CCF probabilities are obtained as the result of unavailability estimation accounting for different detection methods and corresponding outage times. Typically CCF events of safety system components are detected by tests during plant operation or during annual overhaul. In CCF quantification this is often regarded as the only way of detection. This leads into CCF unavailability quantification in which the CCF rate is based on all kinds of CCF events and the corresponding outage time is always determined by the test interval and testing scheme. This approach might be overly conservative or sometimes optimistic. This paper improves CCF unavailability estimation by taking into account monitoring and different kinds of tests and outage times and considering failure modes in the failure rate estimation.

Keywords: PRA, CCF, unavailability, probability, failure rate.

1. INTRODUCTION

Typically CCF events of safety system components are detected by testing during plant operation or during annual overhaul. In CCF quantification this is often regarded as the only way of detection. This leads into CCF unavailability quantification in which the CCF rate is based on all kinds of CCF events having outage times from minutes to years. This approach might yield overly conservative CCF unavailability estimates or sometimes optimistic.

For example diesel generators of Loviisa Nuclear Power Plant (NPP) have once started spuriously due to a false signal (this event is recorded in the ICDE database [1]). The diesel generators stopped simultaneously when the large leakage signal disappeared, because at that time there was no delay circuit of the start-up signal. All the diesel generators were simultaneously completely unavailable a couple of minutes. CCF coupling factor and time factor measuring the simultaneity were high. Thus, this event is clearly a complete CCF and it has a high effect when estimating the CCF rate of diesel generators, if it is taken us such in the estimation. However, such an event is always detected immediately which means that the unavailability due to such complete CCF failures is negligible. Therefore it is important to take into account detection methods and corresponding outage times. It is clear that immediately detected failures have a minor effect on the overall unavailability when the repair times are short compared to the test intervals.

Sometimes CCF events are not found out in the normal tests during power operation, but in the annual or more rarely made more profound tests. These kinds of events can be important contributors to the unavailability. They should be properly taken into account in the estimation, or the result could be optimistic.

Detection methods are recorded in the ICDE CCF event data collection. If there are many events it might be possible to estimate rates of different types of events. However, the data is usually sparse so that we do not get sufficient amounts of data to estimate dedicated rates of those different types. If we only have events with immediate detection does not mean that other kinds of events would have zero

failure rate. Another problem in the data handling is that other plants might have different testing methods.

Plant-specific testing methods and schemes have to be taken into account. Their effectiveness can be studied by analyzing single failure data. In case of Loviisa NPP we have studied how the events have been detected in the failure histories of the safety systems. Scheduled tests were found to be the most important way of detection, except in case of measurements. The results of this study indicate that there are differences in the detection methods not only between component types but especially between different systems. This study of single failure histories was utilized in estimating the shares of different kinds of events with different detection methods.

The methodology to estimate residual parametric common cause failure (CCF) rates consists of the selection of the data source (OECD ICDE, EPRI, other), source plants, source systems and component type, failure mode and detection methods, assessment of the impact vectors, calculation of CCF rates with uncertainties using a parametric empirical Bayes estimation method and finally determining CCF basic event probabilities to be used in the probabilistic safety assessment model. The methodology was first introduced in 2001 [2], later to a wider audience [3] and a more comprehensive description and further developed methodology was presented in 2005 [4]. This paper takes into account failure modes and improves the unavailability estimation by taking into account different detection methods and corresponding outage times.

Plant-specific test intervals and schemes and detection methods were used to calculate the common-cause unavailabilities. All different CCF multiplicities were modeled as basic events in the system fault trees, connected by OR-gates to the components affected. This approach facilitates many PRA applications like the evaluation of test interval modifications and risk-informed optimization of allowed outage times.

This paper gives at first an overview of the CCF methodology that has been used for Loviisa PRA. CCF rate estimation is briefly presented pointing out some principles in the data handling. More emphasis is put on the unavailability estimation which yields the probability values that are used in the PRA.

2. CCF METHODOLOGY

2.1 Overview

The analysis of dependencies has consisted of the following subtasks:

A. Designed dependencies
- A.1 Initiator dependencies
- A.2 System dependencies and interactions

B. Statistical dependencies
- B.1 Dependent/repeated human errors
- B.2 Plant-specific hardware dependencies
- B.3 Residual parametric common cause failures.

The designed dependencies are to be taken into account in the normal process of logical modelling of the plant. This includes identification of specific initiating events that degrade one or more safety functions, development of event trees that account for mutual dependencies of safety systems, and linking fault trees for systems that depend on each other or common components for functional performance.

Statistical dependencies are not necessarily recognized or quantitatively accounted for in the design stage. Yet they can significantly increase the probability of multiple failures, which is the main motive for dependency analysis.

The human reliability assessment includes special consideration of factors affecting the likelihood of repeated errors in maintenance activities [5].

The analysis of plant-specific hardware dependencies covers mainly dependencies caused by physical phenomena, like risen temperature, humidity, vibration etc. which increase failure probability in other systems or components [6]. Cascade and propagating failures are also covered as well as such human errors, which are not covered by a systematic study of scheduled periodic tests or maintenance measures [5]. Cascade failures occur when one equipment failure causes changes in operating conditions, environments or requirements to cause another item or items of equipment to fail or to increase the failure probability, which might fail a third item and so on. Examples of such cases are missiles from a failing turbine, steam jets or a leakage in a room where a flood may cover and fail a pump.

Residual parametric common cause failures are dependent simultaneous multiple failures that have not been specifically identified and quantified as vulnerabilities through plant-specific walk-throughs in a normal fault tree modelling process. Their causes are typically a priori unforeseen events, conditions or phenomena. They affect normally identical redundant components within each system. The focus of this paper is in the estimation of these probabilities.

2.2 Factors of unavailability

One basic observation even with single failures is that they occur at random times, mostly due to time-related stresses (corrosion, temperature, humidity, sticking, loosening, wear) rather than stresses associated with true demands (initiating events) or test demands. Consequently, they are modelled by failure rates λ_j, probability of failure of component j per unit time, rather than by probability per demand. When the test interval is T, the basic event probability $z_j = Pr(Z_j) = ½\ \lambda_j\ T$ is the average probability for single-failed state of component j. When used in a fault tree model it approximately yields the system average unavailability. In a more exact quantification repair time and logistic delay contributions have to be taken into account, approximately

$$u = q + ½\lambda T + \lambda\tau + p\tau/T + f\tau + h(T), \qquad (1)$$

where q = probability of a demand (startup and operation stress) to cause a critical failure
λ = rate of critical failures caused by stresses during standby and revealed by tests; probability per unit time
T = test interval
τ = restoration time including repair time and logical delays
p = probability of a demand to cause a non-critical failure
f = rate of non-critical failures caused by stresses during standby
$h(T)$ = human error probability, some may depend on T.

For simplicity the terms like $\lambda\tau\ /(1+\lambda\tau)$ are replaced by the usual approximation. Some earlier studies [7, 8, 9] have indicated that the standby failure rate term $½\lambda T$ typically dominates for motor-operated valves and diesel generators, with virtually zero q, and f about 3 to 6 times larger than λ, and similarly p larger than q.

In addition to the unavailability according to Eq. 1 immediately detected failures cause an unavailability $\lambda_o(\tau+T_o)$ where T_o is the mission time. These are typically modeled as "fail to run" or "fail to remain open" or corresponding running time failures.

2.3 Equivalent observations

With similar arguments the common cause failures occur at random times and are modelled by general multiple-failure rates λ_i, λ_{ij}, λ_{ijk} etc. so that $\lambda_{ij..}dt$ is the failure probability of exactly components i, j, .. in dt due to a common cause. Such rates can easily be estimated directly from the observed total

number of *k/n*-events, $N_{k/n}$, over the system observation time T_n: $\Lambda_{k/n} = \binom{n}{k}\lambda_{k/n} \sim X^2(2Nk/n + 1) / (2T_n)$. Here we assume symmetry, i.e. $\lambda_{ij} = \lambda_{2/n}$, $\lambda_{ijk} = \lambda_{3/n}$ etc. for all *i, j, k* etc. The mean value and variance of this gamma distribution are

$$E(\Lambda_{k/n}) = [N_{k/n} + \alpha]/T_n, \quad \sigma^2(\Lambda_{k/n}) = [N_{k/n} + \alpha]/T_n^2, \qquad (2)$$

where $0 < \alpha \leq ½$, usually $\alpha = ½$. Unfortunately, due to uncertainties in observations and interpretations each event is not with certainty known to be a certain *k/n*-event. One has to assess for each plant ν for each observation *i* the impact vector weights $w_{k/n}(i,\nu)$ = probability (conditional on symptoms) that in observation *i* at plant ν exactly *k* components out of *n* identical components failed due to a common cause (CCF–group size *n*).

Assessing and quantification of these weights are based on component degradations, shared causes and timing to measure the simultaneity of the failures. Vaurio [10] has shown that the moments for plant ν in terms of the weights are

$$E(\Lambda_{k/n}) = [\sum_{i=1}^{N_n} w_{k/n}(i,\nu) + \alpha]/T_n, \quad \sigma^2(\Lambda_{k/n}) = \{\sum_{i=1}^{N_n} w_{k/n}(i,\nu)[2 - w_{k/n}(i,\nu)] + \alpha\}/T_n^2, \qquad (3)$$

where N_n is the total number of events in time T_n for plant ν. The variance can be written in the form

$$\sigma^2(\Lambda_{k/n}) = \left[\sum_{i=1}^{N_n} w_{k/n}(i,\nu) + \alpha\right]/T_n^2 + \{\sum_{i=1}^{N_n} w_{k/n}(i,\nu)[1 - w_{k/n}(i,\nu)]\}/T_n^2$$

where the first term corresponds to the statistical variance and the second term can be viewed as the subjective variance. Making Eqs. 2 and 3 equal yields the "equivalent" data pairs $N_{k/n}$ and T_n that without uncertainties would give the same moments

$$\tilde{N}_{k/n}(\nu) = \frac{(\sum_{i=1}^{N_n} w_i)^2 + \alpha\sum_{i=1}^{N_n} w_i^2}{\sum_{i=1}^{N_n} w_i(2 - w_i) + \alpha}, \qquad \tilde{T}_n(\nu) = \frac{\sum_{i=1}^{N_n} w_i + \alpha}{\sum_{i=1}^{N_n} w_i(2 - w_i) + \alpha} T_n, \qquad (4)$$

where N_n is the total number of events at plant ν in time T_n and $w_i = w_{k/n}(i,\nu)$. Due to the variance of $N_{k/n}$ the virtual observation time is shorter than the real time T_n.

This CCF estimation methodology applying the idea of equivalent observations has been extended to cover cases in which multiple events of different multiplicities *k/n* are allowed [11, 4], because there is a need to accept impacts of even two events of the same multiplicity *k* in a single observation. How this affects the equations can be found from [4].

2.4 Empirical Bayes estimation

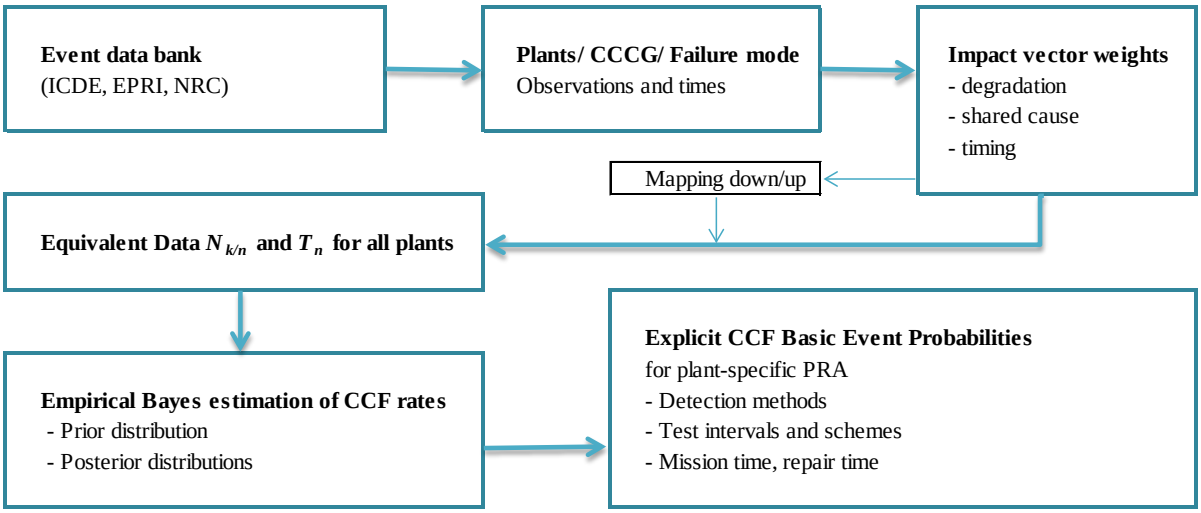
The equivalent data pairs for selected plants ν are input to a robust parametric moment matching method that yields the population distribution of the rate $\Lambda_{k/n}$ of *k/n*–events for the whole plant population. This is the empirical prior distribution used in the Robust Parametric Empirical Bayes (PREB) estimation process [12, 13] to obtain the posterior distribution of $\Lambda_{k/n}(\nu)$ for the target plant. The computerised procedure calculates the posterior distributions for all plants included in the prior calculation, not only for the target plant. The distribution of the rate of *specific k* failures out of *n*, $\lambda_{k/n}(\nu) = \Lambda_{k/n}(\nu)/\binom{n}{k}$ is obtained easily by dividing the mean value and the standard deviation by the Binomial factor. The key idea in PREB is to use a biased positive variance estimate to guarantee realistic solutions with all kinds of data, even for small samples with small empirical variance. PREB gives efficiently realistic results with all kinds of data.

The PREB method has been developed also for probabilities per demand, $Q_{k/n}$, in which case $T_n(v)$ is the total number of system–demands (opportunities) [14, 13]. Then the parameters $q_{k/n} = Q_{k/n}/\binom{n}{k}$ are directly the basic event probabilities, but this approach ignores the dependencies on detection methods, test interval and test staggering, which may be important for optimisation.

2.5 Quantification tasks

The quantification tasks that are needed for estimating CCF probabilities for Loviisa PRA are presented in Fig. 1. This procedure is slightly modified from the one presented by Vaurio [4]. At first the database is selected. Then we select a specific system and component type for the analysis. The target plant has a certain number n of redundant trains or components in that system. This is the size of the Common Cause Component Group (CCCG).

Figure 1: CCF quantification procedure



The next task is to select a set of relevant plants and systems, i.e. CCCG that has components similar enough to those of the target plant. We define as detailed CCCG as reasonable, e.g. centrifugal pumps are divided into several groups like high pressure safety injection pumps, low pressure safety injection pumps, containment spray pumps, auxiliary feed water pumps, component cooling water pumps and service water pumps. Especially service water pumps and component cooling water pumps have very different failure histories from the other pumps. For each of those pump groups we estimate specific CCF probabilities.

The next step is to select the failure mode that we are interested in. Fail to start and fail to run as well as fail to open and fail to close can have completely different failure cause, entry and detection mechanisms. Therefore these different failure modes can have different failure rates and different unavailability factors leading to different unavailability times.

In order to avoid mapping up and mapping down we take into account only such CCCG's that have the same redundancy level n as the plant under study. If data is too scarce in this subset, an option is to accept data from all plants and use "mapping up" (when $n' < n$) and "mapping down" (when $n' > n$) rules to obtain weights supposed to be valid for plants with the same system size n as the target plant [15]. This option, especially mapping up is avoided for Loviisa PRA, because it is based on some severe assumptions about the external nature of causes, and assume the same frequencies and consequences of cause events, independent of the system size n.

Then for each observation we determine the impact vector weights $w_{k/n}(i,v)$ for k = 2, 3,.., n by studying the event descriptions and other relevant information like degradation values, shared cause

factors and time factors. We determine them for the plant where the event took place, not for the plant for which the CCF probability is to be estimated. In estimating the weight probabilities the weighting procedure by Vaurio [4] is applied. The method is slightly modified from [16]: More than one cause-event can be involved in one observation, and component degradations are not assumed mutually independent but coupled (e.g. the smallest degradation rather than the product of degradations determines the probability of a complete *n/n*-failure).

After defining the impact vector weights we estimate effective data pairs (K_i, T_i) for each CCCG (plant), failure mode and failure multiplicity.

In the next step PREB calculations are performed separately for each CCCG and failure multiplicity to obtain posterior CCF rates with uncertainties for the plant under study and for all other plants as well. We obtain also the sampling (prior) distribution that describes the variability between all the plants. The rates of specific *k* failures out of *n* are obtained by dividing with the binomial factor: $\lambda_{k/n}(\nu) = \Lambda_{k/n}(\nu)/\binom{n}{k}$. The PREB procedure yields individual failure rates as posterior distributions, which describe the statistical variabilities of those failure rates. PREB gives also the sampling distribution from which all individual failure rates are samples.

Thus, the data pairs, numbers of observations and observation times, of each CCCG is the only data that is needed in this estimation to obtain CCCG-specific failure rates as posterior distributions for specific failure modes.

Finally we calculate CCF probabilities of different multiplicities as unavailabilities taking into account monitoring, test intervals, testing schemes and rules applied in the plant under study for failure modes that are detected by tests or other demands. That is why we estimate the shares of failures that are detected in different kinds of tests or demands. We estimate the shares or rates of immediately detected failures. The unavailabilities are used as the CCF basic event probabilities for the PRA of Loviisa NPP.

3. UNAVAILABILITY ESTIMATION

3.1 CCF unavailability

Like single failures common cause failures have also different kinds of restoration times. Some of the failures are immediately detected during standby or mission, some in demands at scheduled tests, maintenance tests or other start-ups. Scheduled tests at plant shutdown annually or more rarely can be more profound and reveal other kinds of failures than the more frequently performed tests during power operation. Tests can be staggered or consecutive. In case of a staggered testing scheme a complete common cause failure can only have a latent unavailability time that is the test interval of one train divided by the number of redundant trains.

When we consider only failures that are detected by tests with test interval *T* we define the probabilities $z_{ij..}$ of the basic CCF-events $Z_{ij..}$ (failing exactly specific *k* components *i, j,..* out of *n* similar components) needed in the system fault tree. For standby safety components tested with test interval *T* these values are

$$P(Z_{ij..}) = c_{k/n}\lambda_{k/n}T, \qquad (5)$$

where $0 < c_{k/n} < 1$. The coefficients $c_{k/n}$ depend on *k*, *n*, test staggering, repair policy and the system success criterion [17, 4]. They can be determined so that correct time-average risk is obtained by a single fault tree calculation. In case of sequential or simultaneous testing the average residence time of the failures would be approximately one half of the test interval, which gives us a general approximation similar to the single failure practice, $c_{k/n} = ½$, for $n = 1, 2, 3,\ldots$ and $1 \le k \le n$.

When we consider also other detection methods we obtain a more general expression for the probabilities $z_{ij..}$

$$P(Z_{ij..}) = a \cdot \lambda_{k/n} \cdot (c_{k/n} \cdot T + \tau) + b \cdot \lambda_{k/n} \cdot (T_L / 2 + \tau) + \lambda_{dk/n} \cdot (T_o + \tau) + \lambda_{ok/n} \cdot (T_o + \tau), \quad (6)$$

where

$\lambda_{k/n}$ = the rate of multiplicity *k/n* failures (detected in periodic tests),
a = share of failures that are detected by scheduled tests during power operation,
b = share of failures that are detected in broader tests that are performed during plant shutdown,
$c_{k/n}$ = coefficient that depends on *k*, *n*, test staggering, repair policy and the system success criterion,
T = test interval during power operation (typically 4 weeks or 12 weeks),
T_L = test interval of broader, consecutive tests, typically one year or longer,
$\lambda_{dk/n}$ = the rate of multiplicity *k/n* failures that are immediately detected,
$\lambda_{ok/n}$ = the rate of running time multiplicity *k/n* failures,
T_o = mission time.

The share of failures that are detected in broader tests that are performed during plant shutdown maybe split into two parts: those that are only detected in the annual tests and those that are detected in a different broad test after maintenance or due to some other reason. These latter ones are important but difficult to estimate, because the latent time can be long, even several years, and it can vary a lot. One possibility is to estimate an average latent time based on the CCF experiences of a component type.

For some components $\lambda_{dk/n}\tau$ -term can be dominating like for measurements and automation modules but typically the contribution of $\lambda_{dk/n}\tau$ is small. Those failures tend to be more often complete common cause failures and that is a good reason to estimate specific rates for them also in case of other components. Their observation time is the same as the calendar time from the beginning to the end of the observation period. An example of such a case is the diesel generator failure due to a spurious signal described in the introduction. It was a complete failure but it had a very short unavailability time.

If there is not enough data to estimate $\lambda_{dk/n}$ it is possible to estimate the overall CCF rate $\lambda_{k/n}$ that covers failures detected in periodic tests or demands and immediately detected. Then these different contributions are estimated by using shares that are based on CCF histories and/or on plant specific data on single failures.

The contribution of $\lambda_{ok/n}$ cases can be large because their observation time is only the running time of the component, which is usually very short for standby components. This is modeled as separate basic events representing running failure modes. Because of the short running times it is not always possible to estimate specific rates for them and they are included e.g. in the fail to start estimation.

It is also possible that a failure is detected in a scheduled test and it disappears in a short time. For example two out of four Loviisa diesel generators had a relay jamming failure that disappeared by itself after 14 seconds in the first case and after 150 seconds in the second case 2 weeks later. One diesel generator has a test interval of four weeks and the testing scheme is staggered. Thus, in this case the CCF was effective only 14 seconds. In case of Loviisa so short unavailability does not prevent an emergency operation, except maybe in case of a large LOCA, and therefore this case must not be taken into account as a CCF. The replacement times of the relays are then taken into account as single failure unavailabilities. If such a short time was critical this case must be considered as a CCF and the test interval contribution must be taken into account in the unavailability estimation. Similar single event cases were found from other diesel generators and those relays were found to be from the same batch. Therefore eventually we consider this case of two failures to be an incipient CCF having an impairment vector IIWW, where I refers to Incipient and W refers to Working.

The non-critical failure terms $p\tau/T$ and $f\tau$ of Eq. 1 can be neglected in the CCF unavailability estimation. Incipient failures are such defects that a component is still able to perform its intended

function (if needed), but the repair itself takes the component out of service, and this is how we quantify such unavailabilities for single failures: $f\tau/(1+f\tau)$. Correspondingly we could consider the same approach for CCF events. However, redundant components are not repaired at the same time during power operation. Only single incipient failures can cause unavailability when they are repaired. CCF events are considered to be incipient when at least two incipient failures due to a same reason have been found. If the other redundant components have also been repaired or replaced it is a rule in the ICDE database to classify them as incipiently failed. This affects the impact vector as a degradation value of 0.1. Thus, the incipient failures are taken into account in the CCF rate estimation.

The average values according to Eq. 6 are applied in the power operation PRA. In the shutdown PRA we take into account the latest testing time of each component prior to each plant operating state. So instead of the term $c_{k/n}\ T$ we use time from the previous test. This is more realistic than assuming the same constant unavailabilities as in full power operation. However, 10 % of the average unavailability is assumed to represent a constant unavailability term q (see Eq. 1) that is otherwise neglected. Thus, the failure probabilities vary from state to state and can differ considerably from those of power operation. Components that have been tested already a year ago have two times higher unavailabilities than in the average in power operation. Components that have been tested in the previous plant operating state might have an order of magnitude smaller unavailability value because the time-related unavailability is minimal.

Restoration times τ are estimated based on the single failure experiences of the target plant. In this way they represent the maintenance practices in the target plant. The last term of Eq. 1, $h(T)$, is not presented in Eq. 6 because it is not estimated in the process of CCF unavailability quantification based on histories, but as a part of human reliability assessment (see Ch. 2.1).

3.2. Detection methods

Failures of standby safety systems are usually considered to be detected by scheduled tests. This is not always true. In case of Loviisa NPP we have studied how the events have been detected in the failure histories of the safety systems. The first unit of Loviisa NPP has been in operation since 1977 and the second unit since 1980. Scheduled tests were found to be the most important way of detection, except in case of measurements.

The following detection methods have been recorded in the maintenance history: 1) monitoring in the control room from symptoms or alarms, 2) direct observation immediately after failure, 3) monitoring on shift walk down, 4) scheduled test, 5) scheduled maintenance, 6) demand event, 7) QA/C inspection, condition monitoring, 8) repair or trial run after repair, 9) random check. Altogether in the history scheduled tests revealed 68 % of all the failures, demand events revealed 7 %, monitoring in control room found out 14 % and other immediate detections 5 %. The results [18] are presented in Table 1 classified according to component types and in Table 2 according to systems.

Table 1: Detection methods of component types

Detection method	**1** Imm.	**2** Imm.	**3** Shift	**4** Test	**5** Maint.	**6** Dem.	**7** Insp.	**8** Repair	**9** Rand.
Alternating pumps	4.5 %	4.5 %	0.0 %	68.2 %	0.0 %	22.7 %	0.0 %	0.0 %	0.0 %
Standby pumps	5.4 %	1.8 %	1.8 %	80.4 %	1.8 %	1.8 %	1.8 %	3.6 %	1.8 %
Diesel generators	12.6 %	5.3 %	1.1 %	72.6 %	2.1 %	0.0 %	1.1 %	5.3 %	0.0 %
Check valves	0.0 %	0.0 %	0.0 %	100 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
Isolation valves	0.0 %	7.1 %	0.0 %	92.9 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
Relief valves	14.3 %	14.3 %	14.3 %	57.1 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
Motor operated valves	15.8 %	5.5 %	0.7 %	66.3 %	0.7 %	10.0 %	0.3 %	0.3 %	0.3 %
Control valves	36.7 %	10.0 %	3.3 %	40.0 %	0.0 %	6.7 %	0.0 %	3.3 %	0.0 %
Pressure and level m.	78.7 %	1.9 %	5.2 %	5.8 %	3.2 %	1.3 %	1.3 %	0.6 %	1.9 %
Temperature m.	88.9 %	0.0 %	5.6 %	0.0 %	0.0 %	2.8 %	2.8 %	0.0 %	0.0 %

Imm. = immediate, Maint.= maintenance, Dem.=demand, Insp.=Inspection, Rand.=random

Table 2: Detection methods of systems

Detection method	**1** Imm.	**2** Imm.	**3** Shift	**4** Test	**5** Maint.	**6** Dem.	**7** Insp.	**8** Repair	**9** Rand.
Main steam	4.9 %	4.9 %	4.9 %	80.5 %	0.0 %	0.0 %	0.0 %	2.4 %	2.4 %
Feed water	40.2 %	2.4 %	1.2 %	37.8 %	0.0 %	17.1 %	0.0 %	1.2 %	0.0 %
Residual heat removal	20.0 %	20.0 %	0.0 %	40.0 %	0.0 %	20.0 %	0.0 %	0.0 %	0.0 %
Secondary makeup	28.6 %	28.6 %	4.8 %	28.6 %	0.0 %	9.5 %	0.0 %	0.0 %	0.0 %
Primary coolant purification	0.0 %	0.0 %	0.0 %	100 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
Component cooling water	2.3 %	2.3 %	0.0 %	84.1 %	0.0 %	9.1 %	0.0 %	2.3 %	0.0 %
LPSI[a]	3.8 %	0.0 %	0.0 %	90.6 %	3.8 %	1.9 %	0.0 %	0.0 %	0.0 %
HPSI[b]	8.3 %	0.0 %	0.0 %	87.5 %	0.0 %	0.0 %	4.2 %	0.0 %	0.0 %
Primary make-up	27.8 %	13.9 %	2.8 %	36.1 %	0.0 %	13.9 %	0.0 %	5.6 %	0.0 %
Containment spray	2.7 %	0.0 %	0.0 %	95.9 %	0.0 %	1.4 %	0.0 %	0.0 %	0.0 %
Service water	8.6 %	14.3 %	2.9 %	48.6 %	0.0 %	25.7 %	0.0 %	0.0 %	0.0 %

Imm. = immediate, Maint.= maintenance, Dem.=demand, Insp.=Inspection, Rand.=random
a) Low Pressure Safety Injection b) High Pressure Safety Injection

The differences between such component types as pumps, diesel generators and valves are rather small. The role of scheduled tests is only 6 % in case of measurement failures. Monitoring in control room found out 78 % in case of measurement failures. On the other hand the differences between systems are statistically significant (Table 2). An essential factor is the usage of the system. Scheduled tests are important for standby systems, but not so important for operating systems.

The detection methods of single failures can be different from those of CCFs. The role of more profound or exceptional tests can be more important with CCFs. For example in Loviisa NPP the testing procedure of high pressure safety injection pumps was changed in 1993 leading to increased test durations. This revealed a CCF that caused the temperatures of the motor bearings to rise unacceptably high. Therefore it is important to study the detection methods of the CCF events even if the testing procedures were different from those of the plant under study. If the CCF database has CCF events with long latent times we take those into account and estimate their shares on the basis of CCF data, unless there is a very good reason to believe that the plant under study has better tests or detection methods. We quantify the shares of annual overhaul tests and exceptional more rare tests according to the CCF data.

Concerning immediately detected failures we estimate their shares, typically for valves, or we estimate separately their failure rates, typically for some pumps. Monitoring on shift walk down is treated as an immediate detection in the unavailability estimation, because the latent time is so short. When estimating a failure rate it is important to take into account the correct observation time. For running time failures only the running time is considered, whereas for standby time failures the calendar time is considered. One should also notice that running failures are immediately detected. This must be taken into account when estimating and utilizing the shares of detection methods.

The detection methods of the common cause failures in ICDE database seem not to differ too much from those of the Loviisa failure history. Therefore we consider that we can utilize Loviisa shares of detection methods when estimating the CCF unavailabilities for Loviisa NPP, except in case of failures found out by more profound tests. Long latent times are estimated based on CCF histories.

3.3. Examples

An example of check valve CCF probabilities is given in Table 3 concerning low pressure safety injection (LPSI) system pump discharge lines. The PRA model has a basic event for each CCF event presented in the left column. Failure multiplicity and the corresponding failure rate is given in the next two columns. Then the coefficient $c_{k/n}$ and testing scheme are given. The last column gives the

unavailability value that is used as the corresponding basic event probability. These components have a staggered testing with a test interval of four weeks and success criterion 1/4. The share of the immediately detected failures is 4 %, 95 % in monthly tests and the share of failures detected only in more rare tests, in this case annual tests, is 1 %. In this case the number of CCF events is so small (17) that we have pooled histories of all systems together, including events from reactor core isolation cooling, auxiliary and emergency feed water, residual heat removal, chemical and volume control, emergency core cooling, component cooling water and essential service water. Concerning the emergency core cooling system this approach is conservative. The rate estimates are

- $1.76 \cdot 10^{-8}$ ($2.45 \cdot 10^{-7}$) for 2/4 failures,
- $1.18 \cdot 10^{-8}$ ($2.07 \cdot 10^{-7}$) for 3/4 failures and
- $9.74 \cdot 10^{-9}$ ($1.62 \cdot 10^{-7}$) for 4/4 failures

per hour with standard deviations shown in the parentheses. The shares of the detection methods were estimated based on all the 88 check valve CCF events, not only fail to open cases. The $u_{m/n}$ values would be 15…27 % lower if we assumed that all failures are detected by scheduled tests.

Table 3: CCF Unavailabilities of LPSI Pump Discharge Line Check Valves

CCF event	*m/n*	$\lambda_{k/n}(\nu)$ /h	$c_{k/n}$	Test	$u_{m/n}$
TH11/12S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH11/51S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH11/52S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH12/51S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH12/52S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH51/52S02 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$6.68 \cdot 10^{-7}$
TH11/12/51S02 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$5.34 \cdot 10^{-7}$
TH11/12/52S02 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$5.34 \cdot 10^{-7}$
TH11/51/52S02 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$5.34 \cdot 10^{-7}$
TH12/51/52S02 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$5.34 \cdot 10^{-7}$
TH11/12/51/52S02 fail to open	4/4	$9.74 \cdot 10^{-9}$	0.125	Staggered	$1.44 \cdot 10^{-6}$

Another example of check valves of LPSI system is given in Table 4 concerning accumulator line check valves. In this case the test interval is two years so that two of the four valves are tested in the same outage, so that they have sequential testing. For the other valve combinations the testing scheme is staggered, as shown in Table 4. For those two valve CCF combinations with sequential testing the unavailability estimate is more than two times higher. The shares of the detection methods are the same as above assuming that the more rare tests are two times longer. This estimate is not considered to be optimistic even if in the CCF history of check valves the long latent time was in the average three times longer than the test interval. The $u_{m/n}$ values would be 1…4 % higher if we assumed that all failures are detected by scheduled tests.

Table 4: CCF unavailabilities of LPSI accumulator line check valves

CCF event	m/n	$\lambda_{k/n}(\nu)$ /h	$c_{k/n}$	Test	$u_{m/n}$
TH41/42S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$1.28 \cdot 10^{-5}$
TH41/81S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.577	Sequential	$2.88 \cdot 10^{-5}$
TH41/82S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$1.28 \cdot 10^{-5}$
TH42/81S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$1.28 \cdot 10^{-5}$
TH42/82S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.577	Sequential	$2.88 \cdot 10^{-5}$
TH81/82S01 fail to open	2/4	$2.94 \cdot 10^{-9}$	0.25	Staggered	$1.28 \cdot 10^{-5}$
TH41/42/81S01 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$9.32 \cdot 10^{-6}$
TH41/42/82S01 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$9.32 \cdot 10^{-6}$
TH41/42/82S01 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$9.32 \cdot 10^{-6}$
TH42/81/82S01 fail to open	3/4	$2.95 \cdot 10^{-9}$	0.178	Staggered	$9.32 \cdot 10^{-6}$
TH41/42/81/82S01 fail to open	4/4	$9.74 \cdot 10^{-9}$	0.25	Staggered	$4.25 \cdot 10^{-5}$

Some safety related components have considerable running times. For example Lo NPP has four essential service water and four component cooling water pumps of which two are running and two are standby. The running time is two weeks and then the pump is stopped and the redundant pump is taken into use. For them we have modelled separately fail to run and fail to start failures: six 2/4 failures, four 3/4 failures and a 4/4 failure for both failure modes. In case of fail to run of the service water pumps the rate estimates are

- $1.43 \cdot 10^{-7}$ ($1.03 \cdot 10^{-6}$) for 2/4 failures,
- $1.50 \cdot 10^{-7}$ ($6.43 \cdot 10^{-7}$) for 3/4 failures and
- $1.31 \cdot 10^{-7}$ ($8.73 \cdot 10^{-7}$) for 4/4 failures

per hour with standard deviations shown in the parentheses. The corresponding unavailability is obtained by multiplying by the mission time of 24 hours. In case of fail to start we take into account the test intervals of Loviisa NPP and the essential detection methods for quantification are considered to be: 24 % immediately detected, 75 % detected in scheduled tests and demands, 1 % detected only annually. These long latent times, e.g. due to design errors, require special conditions, because pumps are started several times per year in normal conditions and failures are revealed. Special conditions are such that the pumps should operate in them according to the technical specifications. The CCF histories include such long latent times in two and three line systems, less than 10 % of all CCF cases. Although Loviisa NPP has four pumps we take this possibility into account with 1 % value. In this way we obtain for the two standby pumps 2/4 fail to start event a probability $1.98 \cdot 10^{-5}$. This probability would be 20 % lower if we assume 0 % for long latent times and 76 % for scheduled tests according to Loviisa history and it would be five times higher if we assume 4 % for long latent times, 76 % for scheduled tests and demands and 20 % for immediate detection according to all CCF history of such pumps. If we assumed that all failures are detected by scheduled tests the estimate would be $1.97 \cdot 10^{-5}$, which is almost the same as the basic case.

This approach is useful for different kinds of PRA applications. For example the knowledge of the effect of the test intervals on the basic event probabilities has been utilized in the risk-informed evaluation of test intervals and limiting conditions of operation.

4. CONCLUSIONS

CCF events of safety system components are mostly detected by testing during plant operation or during annual overhaul. In CCF quantification this is often regarded as the only way of detection. This leads into CCF unavailability quantification in which the CCF rate is based on all kinds of CCF events having outage times from minutes to years. This approach might yield overly conservative CCF unavailability estimates or sometimes optimistic.

Plant-specific testing methods and schemes have to be taken into account. Their effectiveness can be studied by analyzing single failure data of the target plant in addition to the common cause failure histories of a world-wide database. Scheduled tests were found to be the most important way of detection, except in case of measurements and automation. The results of this study indicate that there are differences in the detection methods not only between component types but especially between different systems.

Measurement failures are usually found out immediately via alarms or symptoms in the control room. Scheduled tests play an important role in finding out failures of conventional components like valves, pumps and diesel generators. However, the systems in which these components are used affect significantly to the detection methods. Detection methods are different in systems that are normally in operation compared to the systems that are normally standby.

If we only have events with immediate detection does not mean that other kinds of events would have zero failure rate. Failures that are detected in the annual overhaul or more rare and profound tests can affect the CCF probability more even if their rates were thousand times smaller.

Failure modes and detection methods have to be taken into account already in the estimation of CCF rates, not only when estimating the CCF unavailabilities.

This approach of estimating CCF probabilities by estimating CCF rates and accounting for failure entering and detection methods when estimating unavailabilities facilitates many PRA applications. This approach does not assume anything about single failure probabilities and CCF dependency on them, what is not shown in the CCF histories. We can think that common cause failure probabilities are not dependent on single failure probabilities.

Changes in the test intervals and in the testing schemes affect the CCF probability estimates in a consistent way. CCF probabilities can be estimated more correctly for different shutdown plant operating states taking into account that the components have been tested some hours ago.

References

[1] "*International common cause failure data exchange (ICDE)*". NEA/CSNI/R(2011)12, OECD Nuclear Energy Agency, Committee on the Safety of Nuclear Installations, February 2012.
[2] J.K. Vaurio. "*From failure data to CCF-rates and basic event probabilities*". Proceedings ICDE seminar and workshop on qualitative and quantitative use of ICDE data, 12-13 June 2001, Stockholm. Report NEA/CSNI/R(2001)8, OECD Nuclear Energy Agency, CSNI 2012.
[3] J.K. Vaurio & K.E. Jänkälä. "*Quantification of common cause failure rates and probabilities for standby-system fault trees using international event data sources*", Proceedings of PSAM 6 Conference, San Juan, Puerto Rico, 23-28 June, 2002. Amsterdam, Elsevier.
[4] J.K. Vaurio. "*Uncertainties and quantification of common cause failure rates and probabilities for system analyses*", Reliability Engineering and System Safety, 90, pp. 186-195, (2005).
[5] J. K. Vaurio & U. M. Vuorio. "*Human Reliability Assessment in Loviisa 1 PSA*", Probabilistic Safety Assessment and Management, Editor G. Apostolakis, Elsevier, 1991, New York. Pp. 841-846.
[6] K. E. Jänkälä and J. K. Vaurio, "*Dependent failure analysis in a PSA*", Probabilistic Safety Assessment and Management, Editor G. Apostolakis, Elsevier, New York. Pp.607-612
[7] E. V. Lofgren and M. Thaggard, "*Analysis of standby and demand stress failure modes,*" NUREG/CR-5823, 1992.
[8] U. Pulkkinen et al., "*Reliability of diesel generators in the Finnish and Swedish nuclear power plants*", Research notes 1070, Technical Research Centre of Finland, 1989, Espoo.
[9] W. E. Vesely et al., "*Evaluation of diesel unavailability and risk effective surveillance test intervals*", NUREG/CR-4810, USNRC, 1987.
[10] J. K. Vaurio, "*Estimation of Common Cause Failure Rates Based on Uncertain Event Data*", *Risk Analysis,* 14**,** pp. 383-387, (1994).
[11] J.K. Vaurio, (2002). "*Extensions of the uncertainty quantification of common cause failure rates*", Reliability Engineering and System Safety, 78, pp. 63-69, (2002).
[12] J.K. Vaurio, "O*n analytic empirical Bayes estimation of failure rates*", Risk Analysis, 7, pp. 329-338, (1987).
[13] J.K. Vaurio & K.E. Jänkälä. "*Evaluation and comparison of estimation methods for failure rates and probabilities*", Reliability Engineering and System Safety, 91, pp. 209–221, (2006).
[14] K.E. Jänkälä and J.K. Vaurio, "*Empirical Bayes data analysis for plant specific safety assessment*", Probabilistic Safety Assessment and Risk Management PSA'87, Volume I, 281-286, Verlag TŰV Rheinland GmbH, Köln. Proc. of PSA'87, Zurich, Switzerland, Aug. 30 to Sep. 4, 1987.
[15] J.K. Vaurio, "*Consistent mapping of common cause failure rates and alpha factors,*" Reliability Engineering and System Safety, 92, pp. 628-645, (2007).
[16] T.E. Wierman, D.M. Rasmuson and A. Mosleh, "*Common-cause failure database and analysis system: event data collection, classification and coding,*". NUREG/CR-6268, Rev. 1. US NRC, 2007. Original version published in June 1998.
[17] J.K. Vaurio, "*Implicit and explicit modelling and quantification of dependencies in system reliability and availability analysis*", EN A - 48, Lappeenranta University of Technology, 2000.
[18] R. Kleinberg, "Turvallisuudelle tärkeiden laitteiden koestusten merkitys vikojen havaitsemisessa," Bachelor's thesis (in Finnish), Aalto University, Espoo 2012, Finland.