# Analysis of Turbine Missile & Turbine-Generator Overspeed Protection System Failure Probability at NPPs: A case study from PSA perspective

**Duško Kančev, Stefan Heussen, Jens-Uwe Klügel, Thomas Kozlik, Pere Drinovac**
NPP Goesgen-Daeniken AG, Kraftwerkstrasse CH-4658 Daeniken, Switzerland

**Abstract:** The potential for main turbine overspeed, and thus a turbine missile event, gets a constant attention in the process industries, and especially heightened awareness in the nuclear industry after the Salem Unit 2 event in 1991. This paper addresses the plant-specific analysis on turbine missile probability as well as the failure probability analysis of the turbine-generator overspeed protection system at the NPP Goesgen. The two general categories of turbine failures, design overspeed and destructive overspeed failures, are considered. The importance of a detailed, plant-specific analysis is highlighted through this study. The benefits of conducting a plant-specific reliability analysis of specific hazards vis-à-vis the option of using the generic databases are emphasized. Specifically, the results of the turbine missile plant-specific analysis in NPP Goesgen indicate that the turbine missile risk would have been overestimated by at least three orders of magnitude if generic data were to be used.

**Keywords:** PSA, NPP, Turbine Missile, Turbine Overspeed Protection, CCF.

## 1. INTRODUCTION

On November 9th, 1991, a destructive turbine overspeed took place at the Salem Unit 2 NPP. There was not any radioactivity release although the event caused an extensive damage to non-safety related equipment and, in turn, implicated a 6-month outage. Consequently, a comprehensive study and analysis on turbine missile probability and evaluation of turbine-generator overspeed protection systems was conducted. In-depth examinations of common cause equipment failures and deficiencies in operation, test and maintenance of turbine overspeed protection and control systems were performed. Important differences were identified among turbine manufacturer practices in terms of equipment hardware, physical configuration and guidance for operation, test and maintenance. Regarding the operators, various deficiencies were identified in the way the turbine manufacturer guidance was implemented regarding maintenance, operations and testing of turbine overspeed protection systems. As a result of the Salem event, the awareness of the potential for main turbine overspeed, and thus a turbine missile event, rose. Many utilities modified their turbine overspeed protection systems and/or overhauled their turbo-generator sets.

The two general categories of turbine missile failures are usually referred to as “design overspeed” (up to approximately 120% of the rated speed) failures and “destructive overspeed” (any speed above the design overspeed) failures. Design overspeed conditions are expected to occur one or more times per year of operation, but destructive overspeed conditions are expected to occur rarely. Missiles resulting from design overspeed failures are the result of the brittle fracture of turbine blade wheels or portions of the turbine rotor itself. Failures of this type can occur during start-up or normal operation. Missiles resulting from destructive overspeed failures would be generated if the overspeed protection system malfunctioned and if the turbine speed increased to a point at which the low-pressure wheels or rotor would undergo ductile failure.

This paper addresses the plant-specific analysis on turbine missile probability as well as the failure probability analysis of the turbine-generator overspeed protection system at the NPP Goesgen (KKG). KKG is a 3-loop KWU PWR 1060 MWe single-unit NPP. The turbine is designed as single stage high-pressure (HP) and 3-stages low-pressure (LP) turbine. As part of the planned replacement strategy, all 3-LP turbines were replaced by Siemens AG in 2013. In addition to that, a plant-specific probabilistic assessment was performed in order to provide information on rotor burst probability,

resulting from hypothetical load case, for use in safety analysis of nuclear power plants. The most significant source of turbine missile is a burst-type failure of bladed LP-rotor. At KKG, turbine blades bursts are not considered as a "turbine missile" event since it is proofed that these blades would be contained within the casings. Hence, only rotor (shaft) bursts are accounted as potential for generating turbine missiles. Failures of the HP and generator rotors would be contained by relatively massive and strong casings, even if failure occurred at maximum conceivable overspeed of the unit. Moreover, these missiles would be much less hazardous than the LP rotor, due to low mass and energy and therefore, will not be considered. The most critical load case considered for crack growth failure of LP-rotor is that turbine reaches 120% overspeed during each start-up. This case covers the operating speed and all maximum overspeed excursions, which may occur in normal operation of the unit. Within the discussed study, the rotor rupture probability is defined as the probability of the crack growth to critical flaw size at design overspeed of 120% after 1000 start-up cycles. The Monte Carlo method was used to evaluate this failure probability. Although numerous conservative assumptions were made, the probability of the crack growth to critical flaw size at design overspeed of 120% is estimated to be well below the generic value estimates given by the U.S. NRC and the Swiss regulator. In a subsequent, second-phase and in order to cover the region of postulated “destructive overspeed” failures, analysis of the failure probability of the turbine overspeed protection system was performed. After the refurbishment, the KKG turbine overspeed protection system consists of two redundant channels – hardware and software one. In order to analyze the failure probability of this system, a fault tree model was constructed. Additionally, in order for a destructive turbine overspeed to become possible at KKG, a simultaneous failure (spurious opening) of the turbine control valve (StV) and failure of the turbine overspeed protection system is needed when the generator is disconnected from grid. Although additionally several conservative assumptions were considered in the analysis, the probability for the occurrence of a destructive overspeed rotor failure was assessed to be negligible and well below the regulators' prescribed threshold.

Through the presented study as good practice example, the importance of a detailed, plant-specific analysis is highlighted.

## 2. ANALYSIS

The analysis within this paper is divided into two parts. The first part of the turbine missile analysis is related to the design overspeed area. The second part of the turbine missile analysis considers the turbine missile analysis in the area of the destructive overspeed.

### 2.1. Design Overspeed Analysis

The turbine missile potentials given a design overspeed were analyzed by an external company [1]. The most significant source of turbine missile is a burst-type failure of bladed LP-rotor. At KKG, turbine blades bursts are not considered as a "turbine missile" event since it is proofed that these blades would be contained within the casings. Hence, only rotor bursts are accounted as potential for generating turbine missiles. Failures of the HP and generator rotors would be contained by relatively massive and strong casings, even if failure occurred at maximum conceivable overspeed of the unit. Moreover, these missiles would be much less hazardous than the LP rotor, due to low mass and energy and therefore, will not be considered. The most critical load case considered for crack growth failure of LP-rotor is that turbine reaches 120% overspeed during each start-up. This case covers the operating speed and all maximum overspeed excursions, which may occur in normal operation of the unit.

Monte Carlo method is used to evaluate the failure probability. The methodology for evaluation of probability is described in the following sections. The overall probability of turbine missile damage $P$ can be calculated as follows:

$$P = P_1 \cdot P_2 \cdot P_3 \tag{1}$$

where $P_1$ is the probability of external turbine occurrence; $P_2$ is the probability of missile striking a critical area; $P_3$ is the probability of damage due to the strike. The focus in this paper is to estimate $P_1$. The probability $P_1$ can be calculated as follows:

$$P_1 = P_{1r} \cdot P_{2r} \cdot P_{3r} \tag{2}$$

where $P_{1r}$ is the probability of rotor burst up to 120% of rated speed due to crack growth to critical size; $P_{2r}$ is the probability of casing penetration given a burst of the rotor up to 120% of rated speed; $P_{3r}$ is the probability of turbine running up to 120% of rated speed. For the purpose of this analysis, it is conservatively assumed that $P_{2r}$ and $P_{3r}$ are 1.0.

The rotor rupture probability, $P_{1r}$, is defined as the probability of the crack growth to critical flaw size at design overspeed of 120% after 1000 start-up cycles. In order to evaluate the failure probability $P_{1r}$, a Monte Carlo simulation technique involving successive deterministic fracture mechanics calculations using randomly selected value of fracture toughness was used. The results after 1E+7 simulations performed direct a 1E-7 probability for a rotor burst given 1000 start-ups.

This turbine missile probability given design overspeed conditions was subsequently used by KKG to derive the plant-specific failure frequency [2]. In KKG, the conservatively-assessed failure frequency is calculated to be:

$$1E-7/1000d \cdot 3d/y = 3E-10/y \quad (d = \text{demands}) \tag{3}$$

This conservative estimate is based on the assumptions that not more than 3 relevant transients per year took place on average; and the crack growth rate over the number of load cycles has a linear growth behavior. According to the principles of linear fracture mechanics, crack growth is caused by the stresses that a component undergoes during operation. The analysis [1] describes as the most effective influence the thermal stresses that the turbine is exposed to during the speed and power increase. Opening the turbine control valves increases the flow of steam to the turbine rotor. The outer layer of the rotor is thus raised to the steam temperature, while the middle layer is delayed by heat conduction in the direction of the outer layer temperature. The faster the steam temperature is raised, the greater the resulting stresses. These stresses are kept small taking into account the operation model according to the plant's operating procedures (OP). The temperature display in the main control room limits the permissible speed and power gradients by allowing the possible temperature or power amounts. It is conservatively assumed that these allowances are not credited. This leads to counting of the first effective load cycle as part of the annual startup of the turbine after the revision, i.e. 1/y.

The operational shutdown procedure used for the annual overhaul & refueling outage is rated as follows: Starting with a small power gradient (approximately 5 MW/min), the turbine run down is released after turbine trip (TUSA), i.e. without further steaming. The turbine rotor is therefore not exposed to significant tension. For this reason, the shutdown is not counted as a load cycle.

Fault-related transients that lead to load shedding (load shedding to own demand, load shedding by pump failures or faults) are designated as the second effective load cycle with 1/y. This value is calculated as follows from the statistics of the last 20 years and is conservatively derived from the statistics of the last 20 years, in which the plant had 17 such occurrences (6 LAW-EB, 5 YD-PUMA, 1 RL-PUMA, 5 various power reductions). Reactor scram (RESA) transients with automatic TUSA or TUSA transients are not counted because the steam flow to the turbine is shut off completely and the shaft cools convectively.

The operational starting procedure following all power transients is included as the third load cycle. This leads, according to the transients operating manual [3], starting the system 0-100%, to the above-mentioned 17 operations, i.e. conservatively 1/y.

The complete discussion above, i.e. the values discussed, justify an approach of 3 load cycles per year.

The conservative assumption for the calculation of the critical crack size is based on the theory of linear fracture mechanics (see [1]). The relationship between crack growth per load change and cyclic stress intensity factor is usually represented by the Paris-diagram as follows [4]:

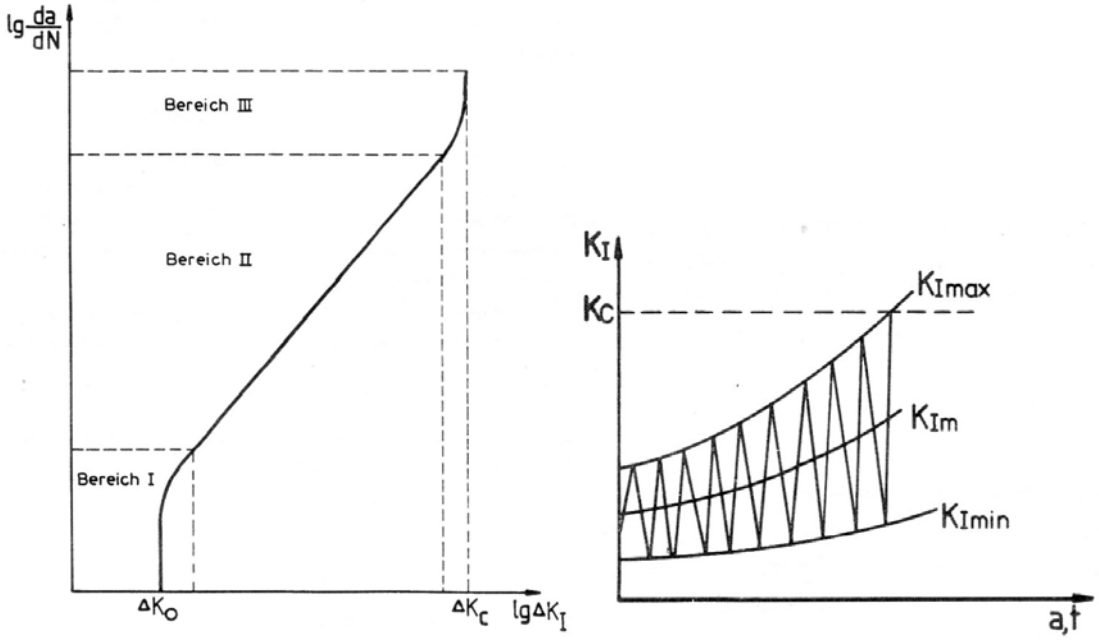


**Figure 1. Relationship between crack growth rate (*da/dN*) and cyclic stress intensity factor ($\Delta K_C$) [4]**

The *da/dN* is the crack growth rate (the first derivative of the crack length a to the number of cycles), and $\Delta K_I = K_{I_{max}} - K_{I_{min}} = \left(\sigma_{max} - \sigma_{min}\right) \cdot \sqrt{\pi \cdot a} \cdot Y_I$ , where $\sigma$ is the applied tension and $Y_I$ is the geometry correction function.

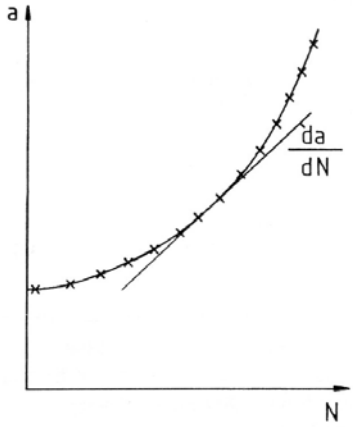


**Figure 2. Relationship between the crack length (*a*) and the number of cycles (*N*) [4]**

The crack growth rate shows a monotone increasing behavior associated with the stress intensity factor, i.e. with increasing number load cycles, the cyclic stress intensity factors and thus the crack growth rates increase. If the dependency of crack growth rate over the number of load cycles is linearized, this leads to an overestimation of the crack growth in the area of small numbers of load cycles. Hence, the conservative assumption used for the screening leads to the turbine rotor shaft failure frequency of $F_{design}$ = 1E-7/1000 * 3/y = 3E-10/y in the area of the design overspeed [2].

## 2.2. Destructive Overspeed Analysis

This section addresses the turbine missile failure probability due to destructive overspeed. In that direction, firstly the failure probability of the turbine overspeed protection system was assessed [5].

The overspeed protection system, which is one of the obligatory safety installations, has the task of quickly switching off the turbine when the permissible speed is exceeded [6]. The speed is recorded by inductive measuring systems from the company JAQUET. Their mode of operation is based on the frequency measurement method. A speed-proportional frequency signal is generated with the aid of a 60-rotor pole wheel revolving on the turbine shaft. The flywheel is scanned contactless by 12 rigidly mounted speed sensors. This results in 12 independent speed signals: 3 hardware transmitters for the overspeed protection; 3 software transmitters for the overspeed protection; 3 transmitters for the turbine control; 3 transmitters as a reserve. The three speed signals of the overspeed protection are electronically processed in such a way that three trip channels each with a 2-from-3-quiescent current principle are created. The trip signals are then coupled via relay modules in the electrical SS trip system. The new quick trip block triggers TUSA in 2-from-3 operation.

For the turbo set the overspeed protection is the most important protection device, which must master the danger potential of the large rotating mass by safe switching off the turbine in case of failure of the control devices. The high requirements with regard to safety, without sacrificing availability, are fulfilled with the present 2 x 2-from-3 structure.

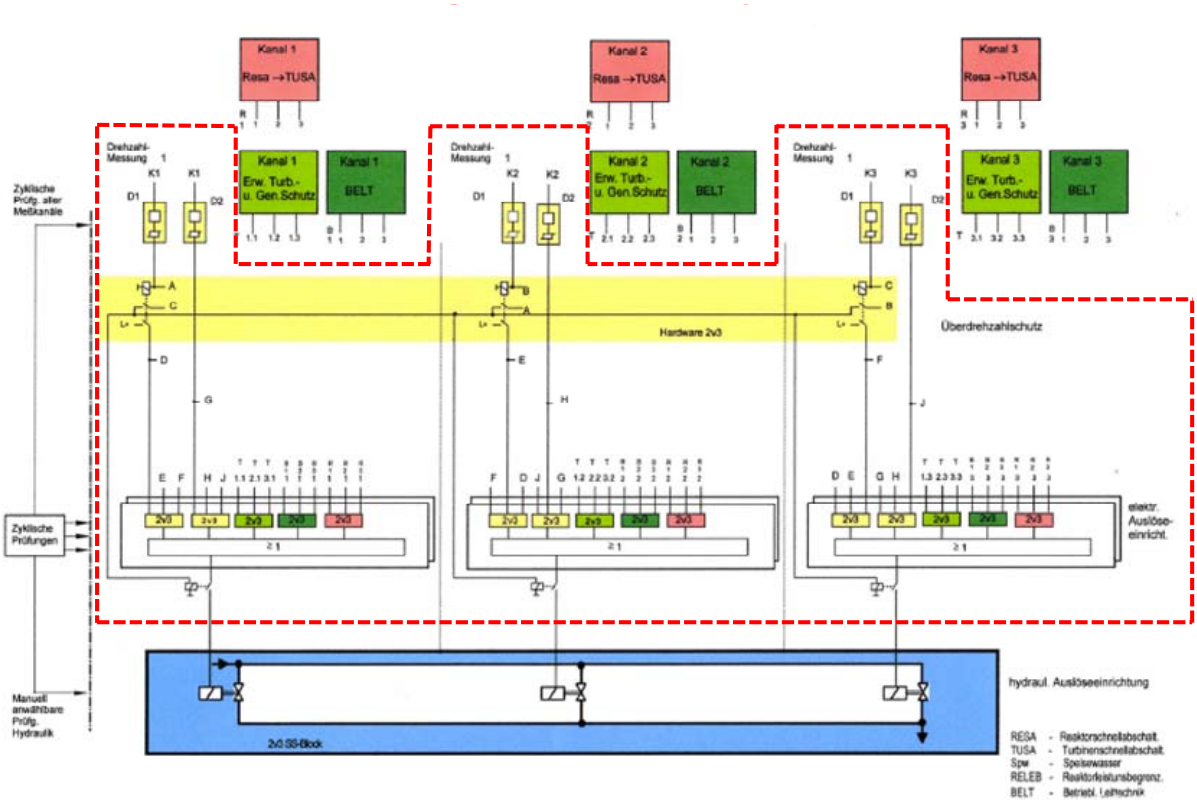


**Figure 3. The turbine overspeed protection system [5]**

The turbine overspeed protection system discussed above, which is marked by a red-dashed line in Figure 3, is modeled and analyzed by a fault tree model. The reliability characteristics are determined by means of fault tree models, which are calculated using the RISKMAN® software. The two parts (software, 3 speed channels and hardware, 3 speed channels) are considered. In the hardware part, the following components are modeled per speed channel: transducer, limiting value transmitter, relay and logical comparator. In the software section, the following components are modelled per speed channel: transducer, limiting value transmitter and logical comparator. In view of the logic of the system, it can

be concluded that the two redundancies (i.e., the hardware as well as the software part) must fail in order to result in a malfunction of the entire overspeed protection system of the turbine set.

The following table summarizes the components reliability input data:

**Table 1. Reliability input data of the turbine overspeed protection system [5]**

| Description | Probability distribution | Distribution parameter (Mean, Error factor) |
|---|---|---|
| Transducer | Lognormal | (8.81E-3/d, 5) |
| Limiting value transmitter | Lognormal | (4.46E-6/d, 1.3) |
| Relay | Lognormal | (1.90E-6/d, 8.6) |
| Logical comparator | Lognormal | (8.50E-5/d, 9.8) |

In view of the logic setup (Figure 3), the system's failure probability per demand is calculated by a fault tree model in the RISKMAN® software. This results in a value of 1.02E-5/d.

The following two initiator groups can be defined as relevant for the accident scenarios that are related to turbine missile events in the area of destructive overspeed:

**$IE_1$** - all transients and system states where the turbine is not synchronized with the grid or disconnected from the grid. These transients include:

a. Faulty (spurious) opening of the generator circuit breaker (GCB);
b. Faulty (spurious) opening of the block circuit breaker;
c. All the transients related to opening of the block and / or generator circuit breaker by the protective functions;
d. Speed control during the starting process of the turbine.

**$IE_2$** - all transients that lead to TUSA.

The transients of the initiator groups are adopted from the available data (statistics) and conservatively estimated. In the $IE_1$ transient group of transients no transients of the type a) or b) were counted at the KKG. The transients of type c) dominate. The number of these events is 44. The trigger rate is after 38 years of operation at 44/38y = 1.15/y. The operating time of the turbine (disconnected from the power grid) is acc. [11] conservatively estimated at 6 h per year. With 4 independently malfunctioning turbine control valves, the from current KKG PSA model [8] adopted distribution function *TSE1VT* (spurious opening failure rate of a StV=1.63 E-6/h) results in an additional contribution of 4E-5/y. This latter contribution is negligible compared to the other former (1.15/y). Hence, the initiating frequency of group $IE_1$ is set conservatively with $f_1$ = 1.25/y. The event tree for initiator group $IE_1$ is structured as follows (Figure 6):

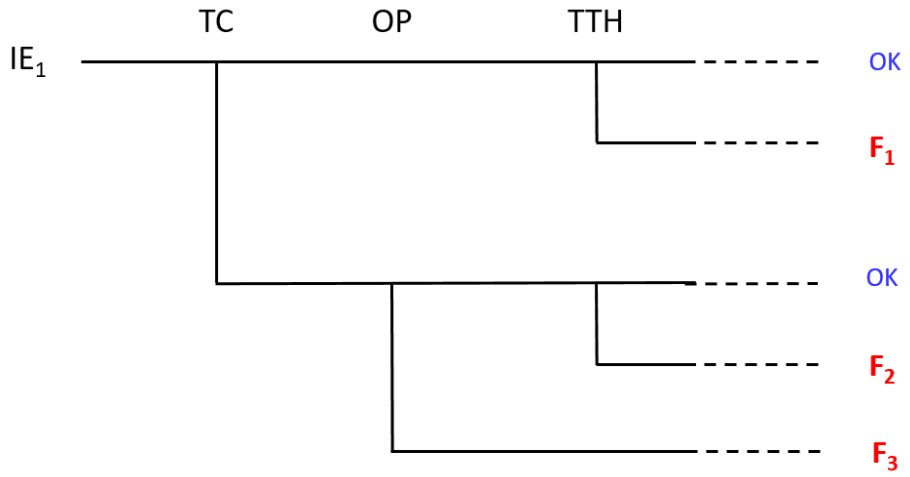


**Figure 4. Event tree for the possible scenarios given initiator group $IE_1$ [7]**

- The **Top Event (TE) "TC"** represents the failure probability of the turbine governor SE10 C010. Since the current KKG PSA model does not explicitly include the controller, the controller is modelled for the purpose of this paper by the failure probability of similar components. By adopting the TELC2D (failure probability on demand = 8.52E-5/d) and *TELC2R* (failure rate = 2.7E-06/h) the distributions for the probability of failure of the turbine bypass controller are calculated according to the current KKG PSA model [8]. Hence, for a mission time of 24 h, the probability of failure of the turbine governor is:

$$Q(TC) = TELC2D + (1 - TELC2D) \cdot TELC2R \cdot 24 \approx 1.5E-04 / d \quad (4)$$

- The **TE "OP"** represents the failure probability of the turbine overspeed protection system. As discussed and analysed earlier in text, this failure probability is derived as:

$$Q(OP) = 1.02E-05 / d \quad (5)$$

- The **TE "TTH"** represents the failure probability of the non-closure of a StV and the assigned turbine stop valve (SSV) of one of the 4 trains. In this top event, the CCF potential has been studied, and consequently two common cause component groups (CCCGs) have been implemented. As Figure 4 above shows, the failure of TTH immediately leads to destructive overspeed. For the purposes of this study, the TE TTH is modelled using the RISKMAN® software (Figure 5).

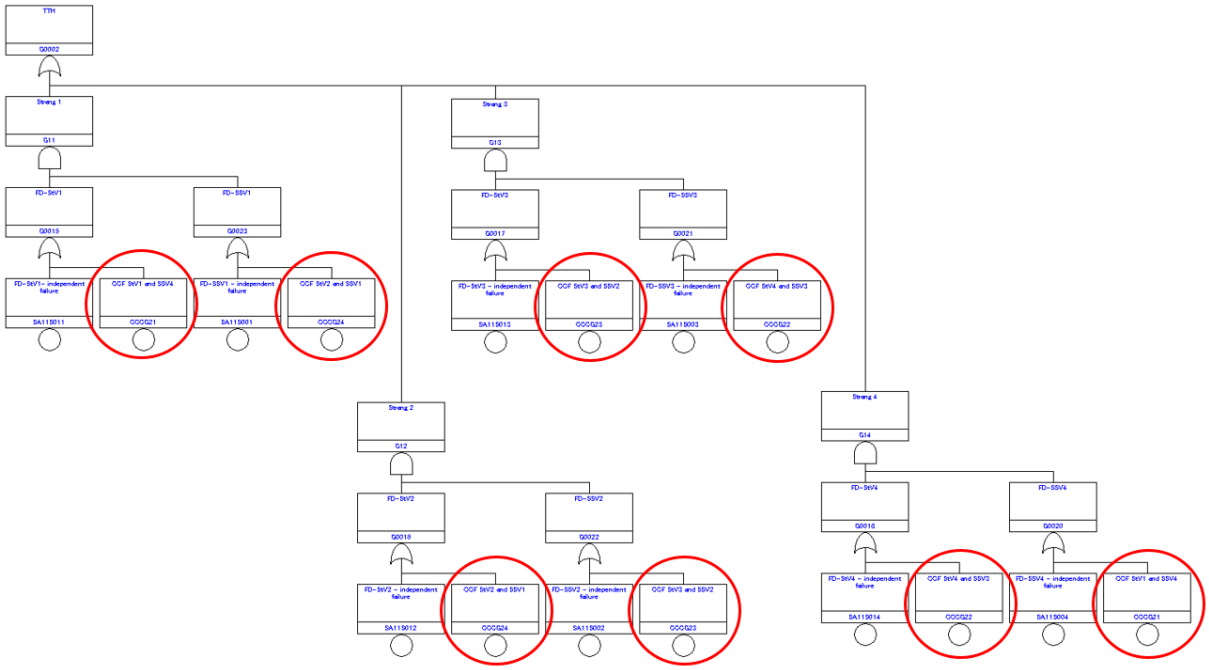

**Figure 5. Fault tree for TE TTH with consideration of two CCCGs related to the StV and the SSV [7]**

As mentioned, the CCF potential among the four StVs and the four SSVs was analysed. Firstly, the existence of common cause coupling mechanism, seen as prerequisite for a CCF, was investigated.

The result of the analysis shows that maintenance with 56% and design with 28% are the two main contributions to CCF regarding valves [9]. This data is now 14 years old and reflects the current state only satisfactory, since in the 40-year operating experience of the KKG significant improvements in the field of "human factor" were achieved. Nevertheless, it can never be conscientiously ruled out that a CCF may be the result of a design flaw or maintenance. For this reason, the KKG has a qualitative analysis of possible coupling mechanisms with regard to CCF of valves [10]. The key statements can be summarized as follows:

i. The valves are often from the same component type and from the same manufacturer so that a CCF coupling mechanism potential can be assumed here;
ii. A common maintenance of valves is discussed as the dominant coupling mechanism in the literature;
iii. Different operating conditions (temperatures, flow rates, pressures, etc.) reduce the probability of occurrence of coupling factors;
iv. The functionalities of valves for safety-related functions are predominantly of a simple nature, i.e. the valves usually need to open or close, and the performance of this function, such as an opening operation, is carried out on request in a short time.

The SSVs and StVs are neither the same or similar, i. e. are not the same type of component - nor are they operated in the same or similar manner. The risk for a design or operational CCF coupling mechanism between these two valve types is therefore low. However, the CCF potential over all SSVs (SA11S001 / 002/003/004) and StVs (SA11S011/012/013/014) is, for the purpose of this study, conservatively considered where an improperly performed maintenance is assumed as a CCF coupling mechanism. For this purpose, the following CCF groups are formed:

- **CCCG2** - between a StV and a SSV that are not installed in a common inflow line of the high-pressure turbine (i.e. 4 CCF groups with 2 components each)

- **CCCG4** - among all the four StVs (single CCF group comprised of 4 components).

Figure 6 shows that every year exactly one StV and one SSV are being maintained. This results in a cycle of 4 years, in which all turbine inlet valves (StVs and SSVs) are serviced once. The potential for a CCF over all turbine inlet valves is very low due to these extended test intervals in the KKG and is therefore not investigated in detail. On the other hand, the CCF potential of two turbine valves (SSV and StV), which do not belong to a same turbine inlet line, should be discussed. These couples are serviced annually and provide CCF potential through common/similar maintenance. Hence, the following pairs CCCG21 (SA11S004; SA11S011), CCCG22 (SA11S003, SA11S014), CCCG23 (SA11S002; SA11S013), CCCG24 (SA11S001; SA11S012) can be formed. From these pairs, the CCF Group (CCCG2) is being established.

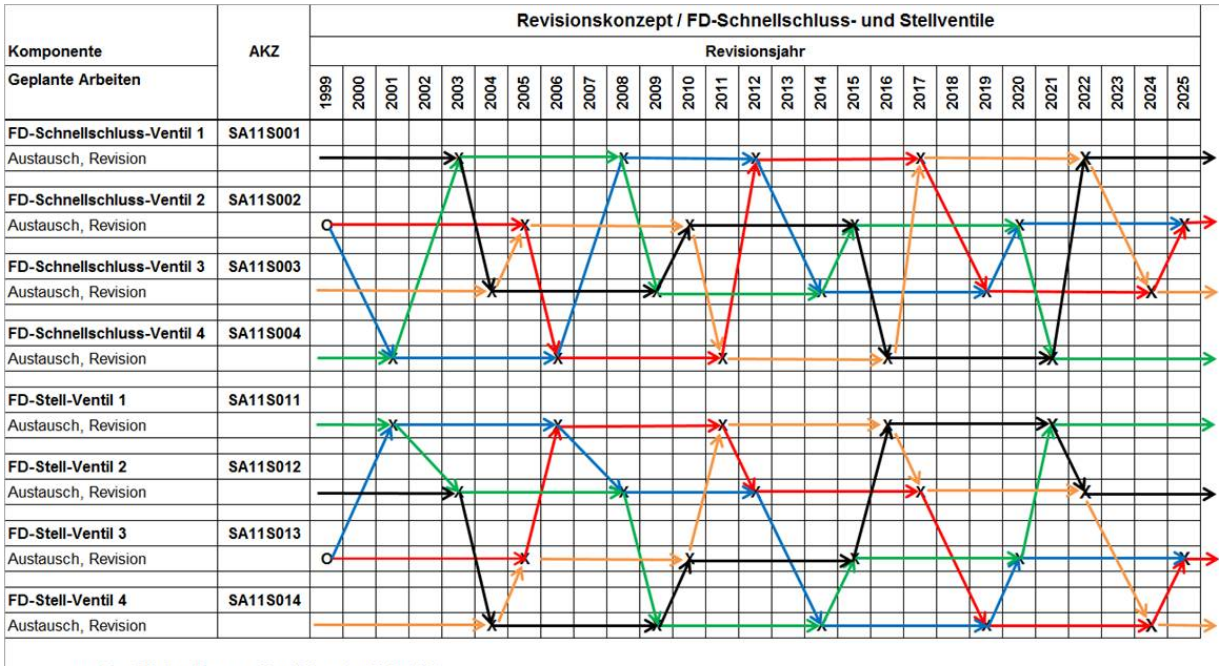


**Figure 6. Maintenance program for the StVs and the SSVs [7]**

On the other hand, given the work instructions, revision work on StV [11], it is clear that all 4 StV simultaneously subjected to an additional maintenance / revision outside the main revision of the main steam system. Based on this maintenance practice, the CCF group (CCCG4) is formed.

The biggest difficulty in modelling of CCF is the data search and definition of appropriate CCF parameters, especially when personnel-focused CCF (HCCF) is in the foreground. Because plant-specific data is unavailable, generic data is used. A thorough study of HCCF can be found in [9], [12], [13], [14], [15], [16], [17]. On the basis of a MGL modelling, the data in the reference [15] prove useful. This document contains a thorough and well-organized database of CCF parameters broken down into component types and CCF models. All CCF groups that concern different types of components and are mainly related to personnel or maintenance-related causes have been examined for MGL parameters. These are discussed within the sections 1.3.8.5, 1.3.8.6, 1.8.2.1, 1.8.2.3, 1.8.2.4, 1.9.2.1, 1.9.6.1 of the referenced document [15]. From these values averages are derived, which are then used as MGL parameters for the above-defined groups CCCG2 and CCCG4. These MGL-parameter values are presented in the following tables.

**Table 2. MGL-parameter for the CCCG2 [7]**

| Parameter | Mean value |
|---|---|
| β ("BETA2") | 1.46E-02 |

**Table 3. MGL-parameter for the CCCG4 [7]**

| Parameter | Mean value |
|---|---|
| β ("BETA4") | 1.22E-02 |
| γ ("GAMMA4") | 3.91E-01 |
| δ ("DELTA4") | 1.76E-01 |

Now, after the definition of the CCCGs relevant for the TE TTH and obtaining the needed CCF MGL-parameter, the final quantification of the TE is possible. Hence, the TTH failure probability is calculated as follows:

$$Q(TTH) = 4.40E-08/d \tag{7}$$

Once the TTH failure probability is quantified, we can proceed with the second initiator group scenario, $IE_2$, presented on Figure 7.

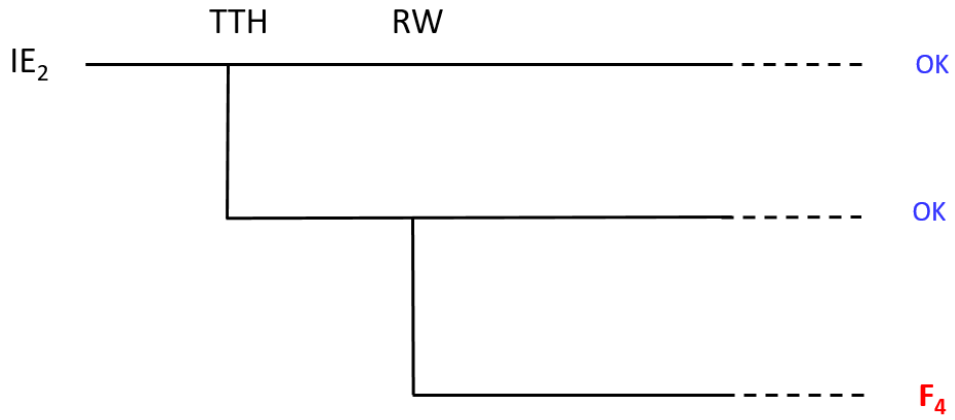


**Figure 7. Event tree for the possible scenarios given initiator group $IE_2$ [7]**

With TE: RW, the so-called power reversal protection of the generator is modelled here. For a grid disconnection to occur, the generator breaker should spuriously open. In this context, the distribution OG1=2.66E-04 /d is adopted [8]. The initiator frequency of group $IE_2$ is set conservatively to $f_2$ = 1/y.

## 3. RESULTS AND DISCUSSION

The risk contribution of turbine missile as a result of a overspeed scenario is quantified through the conditional core damage frequency (CCDF).

Taking into consideration the ET for the first initiator group, depicted on Figure 4, the following value can be derived for the failure frequency of the turbine due to destructive overspeed conditions:

$$F_{TZK1} = F_1 + F_2 + F_3 \approx IE_1 \cdot \left[Q(TTH) + Q(TC) \cdot Q(TTH) + Q(TC) \cdot Q(OP)\right] \approx 5.7E-08/y \tag{8}$$

Regarding the ET for the second initiator group, depicted on Figure 7, the following value can be derived for the failure frequency of the turbine due to destructive overspeed conditions:

$$F_{TZK2} = F_4 \approx IE_2 \cdot Q(TTH) \cdot Q(RW) \approx 1.2E-11/y \quad (9)$$

Both the $F_{design}$, related to the turbine missile frequency due to design overspeed scenario from chapter 2.1, as well as the $F_{TZK2}$ are negligible in comparison to the $F_{TZK1}$. Hence, the CCDF is calculated for $F_{TZK1}$. In this sense, it is conservatively assumed that at a destructive overspeed, the rotor debris will likely penetrate the casing and exit. The affected buildings in which safety relevant SSK are housed, are the following: the electrical building - ZE, the emergency diesel generator 1&2 building - ZK01, as well as the emergency feedwater injection building ZV. Furthermore, it is conservatively assumed that all three buildings are hit simultaneously and all PSA-relevant SSK are destroyed with a conditional probability of 1.0. The resulting CCCF becomes:

$$CCDF\left(IE->F_{TZK1}\right) \approx 2.3E-11/y \quad (10)$$

With this quantitative estimate, it has been shown that the CDF contribution is below 1E-9/y. Consequently, the risk of turbine collision due to a destructive overspeed can be screened out according to the Swiss Regulator [18].

## 3. CONCLUSIONS

This paper addresses the plant-specific analysis on turbine missile probability at the NPP Goesgen. The two general categories of turbine missile failures, i.e. the design overspeed (up to approximately 120% of the rated speed) failures and the “destructive overspeed” (any speed above the design overspeed) failures, are considered within the analysis. The main idea of this analysis is to present an example approach how a plant-specific turbine missile failure analysis can be conducted and simultaneously emphasize the high difference vis-à-vis the by some regulators proposed generic turbine missile failure probabilities (order of magnitude ~ 1E-4) that are still being used.

The most significant source of turbine missile is a burst-type failure of bladed LP-rotor. At KKG, turbine blades bursts are not considered as a "turbine missile" event since it is proofed that these blades would be contained within the casings. Hence, only rotor bursts are accounted as potential for generating turbine missiles. The turbine missile potentials given a design overspeed were analysed by an external company, which is simultaneously the producer of the turbine. In order to evaluate the failure probability due to rotor burst at speeds up to 120% of the rated, a Monte Carlo simulation technique involving successive deterministic fracture mechanics calculations using randomly selected value of fracture toughness was used. The results after 1E+7 simulations performed direct a 1E-7 probability for a rotor burst given 1000 start-ups. KKG has adopted these results and used them further to assess the final turbine rotor failure frequency within the design overspeed area. Given its plant-specific number of 3 relevant transients pro year (conservative), the assessed plant-specific turbine missile failure probability given design overspeed conditions was assessed to be 3E-7/y.

Subsequently, the plant-specific turbine missile failure probability due to destructive overspeed was analyzed. In that direction, firstly the failure probability of the turbine overspeed protection system was assessed. Two initiator groups can be defined as relevant for the accident scenarios that are related to turbine missile events in the area of destructive overspeed. They cover all transients and system states where the turbine is not synchronized with the grid or disconnected from the grid ($IE_1$) as well as all transients that lead to TUSA ($IE_2$). To each of the two initiator groups scenarios, a corresponding ET was defined, each with its relevant functional (top) events - TE. Consequently, the failure probabilities of these functional events were assessed. The failure probabilities of the turbine overspeed protection system as well as the 4-trains redundant system of turbine control and stop valves are derived and assessed based on separate fault tree models done for the purpose of this paper,

which, again reflect the plant-specificity of the problem. The final quantification of the turbine missile failure frequency, given a conservatively assumed conditions, is derived to ca. 5.7E-08/y. In terms of conditional plan risk, this value implicates a conditional CDF ≈ 2.3E-11/y, which is well below the screening out value of 1E-9/yr prescribed by the Swiss regulator. Hence, the turbine missile scenario can be effectively removed from the KKG PSA model.

The main conclusion of this paper is seen in the direction of emphasizing the benefits of conducting a plant-specific reliability analysis of specific hazards vis-à-vis the option of using the generic databases. On one hand, one minimizes the relatively wide inherent uncertainties of the available generic databases, on the other hand - the absolute risk values obtained through such a plant-specific analysis can be much lower than the ones suggested by the generic databases. Specifically, by conducting its own, plant-specific analysis of the turbine missile potential, KKG in close cooperation with the turbine producer has shown that the turbine missile risk would have been overestimated by at least three orders of magnitude by using the generic data.

**References**


[1] SIEMENS. "*DAR Turbine Missile Probability*", Report DPTRP-700209 Rev. A (2012) - proprietary document.

[2] S. Heussen & D. Kancev. "*Aktionspunkt 111 zur Aktualisierung der Leistungs- und der Stillstands-PSA (gem. PEG-S-53)*", ANO-S-92703, KKG (2017) - internal document.

[3] KKG. "*Transientenhandbuch*", ROL-B-20214 Rev. A (2012) - internal document.

[4] H. A. Richard. "*Grundlagen und Anwendungen der Bruchmechanik*", Technische Mechanik 11(1990), Heft 2, (1989).

[5] D. Kancev & S. Heussen. "*Fehleranalyse des Überdrehzahlschutzsystems der Turbine*", ANO-S-92717, KKG (2017) - internal document.

[6] KKG. "*Technologiekurs, Kapitel 4.18, Turbine SA (Teil 2)*", HDB-B-16827 Rev. A (2005) - internal document.

[7] D. Kancev & S. Heussen. "*Leistungs- und Stillstands-PSA, Aktionsliste GPSA2009, Geschäftsnr. 17/12/065, 17/12/066, 17/12/067 und 17/12068 - Aktionspunkt 111 / CCF der SSV und StV*", ANO-S-92760, KKG (2017) - internal document.

[8] ABS Consulting Ltd. "*GPSA 2015 Gösgen Probabilistic Safety Assessment*", R-2129227-1853, (2015) - internal document.

[9] U.S. NRC. "*Common-Cause Failure Event Insights- Motor-Operated Valves*", NUREG/CR-6819, U.S. NRC, Vol. 2, (2003).

[10] P. Drinovac. "*Leistungs- und Stillstands-PSA, Aktionsliste GPSA2009, Geschäftsnr. 17/12/065, 17/12/066, 17/12/067 und 17/12068 - Aktionspunkt 8*", ANO-S-92704, KKG (2017) - internal document.

[11] KKG. "*Arbeitsanleitung/Revisionsarbeiten an FD-Stellventil*", VOR-M-SA-26058, (2016) - internal document.

[12] U.S. NRC. "*Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications*", NUREG/CR-1278, U.S. NRC, (1983).

[13] U.S. NRC. "*Guidelines on Modelling Common-Cause Failures in Probabilistic Risk Assessment*", NUREG/CR-5485, U.S. NRC, (1998).

[14] U.S. NRC. "*Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding*", NUREG/CR-6268, U.S. NRC, (2007).

[15] U.S. NRC. "*CCF Parameter Estimations 2012*", U.S. NRC, (2013).

[16] Nuclear Energy Agency (NEA). "*Human Factor Related Common Cause Failure*", NEA/CSNI/R(95)10/Part 1, (1995).

[17] IAEA. "*Procedures for conduction common cause failure analysis in probabilistic safety assessment*", IAEA-TECDOC-648, IAEA, (1992).

[18] Eidgenössisches Nuklearsicherheitsinspektorat (ENSI). "*Probabilistic Safety Analysis (PSA): Quality and Scope*", ENSI-A05, ENSI, (2018).