# Using Proxel-based Simulation for Reliability Analysis of a Hazardous System

**Fabian Wickborn, Graham Horton**

Otto-von-Guericke-Universität Magdeburg, Germany

*Abstract: In this paper a Proxel-based reliability analysis for the safety mechanism of a hazardous nuclear power reactor, which failures may represent an imminent danger to the environment, is proposed. The system consists of multiple valves and pumps which are set up in a way to provide a redundant route for a high-pressure water flow. An existing larger model for the system is decomposed into three independent parts which are thought to be analysed with much less effort. A Boolean logic for combining the reliability of the subcomponents is derived from a Fault-tree like view on the system and later used to generate reliability information of the original system as a function of time.*

*Keywords: Simulation, Proxel, reliability, nuclear reactor*

## 1 Introduction

The purpose of this paper is to illustrate the use of the Proxel-based simulation method for reliability analysis of systems which malfunctions can present an imminent danger to their ecological environment such as a nuclear power plant (NPP). For this kind of application, precise estimates for the probabilities of the system (un-)availability are a must. Otherwise, emergency procedures and systems derived from this analysis may not be sufficient. If any NPP safety system is not available in the case of an emergency a nuclear accident may occur. Accurate availability information helps refining emergency strategies and thereby decreasing the danger of an environmental disaster.

Until now, such hazardous systems were modelled using discrete-event paradigms, e.g. General Stochastic Petri Nets (GSPN), and simulated by means of Monte Carlo methods. The main disadvantage of the Monte Carlo approach is the need for the generation of multiple independent system histories to gain statistically useful results, due to the use of (pseudo-)random numbers. The computed results of the simulation are random variables. In case of a system with rare events, which the failure of a component of a NPP hopefully is, the large number of needed histories for a sufficient degree of significance leads to large computation times. And even then, there is no guarantee that enough of the repairing or

maintenance states have been considered. Hence, the obtained data may not reflect the changes of the availability well enough.

Since a GSPN is a Markov process, it can be transformed into a Markov chain for which many numerical solution algorithms exist that eliminate the random character of the results. However, for models with general time distributions this approach cannot be applied easily. Distributions for describing infant mortality or wear-out failures such as Weibull distribution or Lognormal distribution cannot be described directly as a Markov process but have to be replaced by an approximation like phase-type distributions. Because of that, such non-markovian models still are usually analysed by using Monte Carlo simulation.

Marseguerra and Zio suggested the use of a so-called **forced Monte Carlo simulation**, in which rare events are forced to occur within the considered time span, to handle the disadvantage of randomness. This modified Monte Carlo approach has already been used to analyse the availability and reliability of a NPP [Ion+03, pp. 6]. However, this method still depends on random numbers so that its output is a random variable itself.

Another way to avoid high computation times and even randomness was introduced by Horton. **Proxel-based simulation** is a new paradigm for analysing discrete-event models. The Proxel method computes the possible flows of probability mass through the states of a simulation model for a finite number of discrete time steps in a deterministic way. It uses the age information of the enabled state transitions to compute a probability of a given state change (by means of the instantaneous rate function of a probability distribution). The age information is stored as supplementary variables together with the discrete state and the probability of that individual state, forming a **Probability Element** (short**: Proxel**). [Hort02, LaHo03]. The method discovers and tracks all possible developments of the dynamic behaviour of the system over the simulation time, including the probability of rare events and the thereby reached system states. The method has shown to be applicable for the analysis of Stochastic Petri Nets [LaHo03a], Fault-trees [LaHo03b] and even project schedules [IsHo04].

Since the handling of rare events is guaranteed, the Proxel method is assumed to be a good choice for reliability and availability analysis. This study illustrates the use of the Proxel-based method for reliability analysis to gain accurate non-random results in a deterministic way.

# 2 A Model for a High-Pressure Injection System

The system serving as an example for this study is a High-Pressure Injection System (HPIS), which can be found in modern NPPs (Figure 1). The HPIS is a safety system that provides a high pressure flow from the radioactive water storage tank

(RWST) to the cooling system. It consists of a set of valves and pumps which are connected in a redundant way to make up multiple possible flow routes from the RWST to two independent entry points of the cooling system X and Y [Ion+03]. Each component can fail independently of the others.

The availability of the HPIS is considered to be mission-critical for the emergency procedures of the power plant. Availability in this case, that is, a high pressure water flow can be established to both of the insertion points X and Y, so that the inner temperature of the reactor is lowered quickly after a possible coolant loss. Otherwise, chances are that a chain reaction could lead to a disastrous nuclear accident.

Additionally to multiple flow routes, the availability of the real system is improved by three independent maintenance cycles. Each cycle consists of a team of engineers who regularly test and maintain multiple subcomponents and repair or replace non-functional subcomponents, if necessary. While the engineers are working on the subcomponent it is disabled and has to be considered unavailable. The cycles are:

- Cycle 1: Valve 1, Valve 2
- Cycle 2: Pump A, Pump B, Pump C, Valve 3, Valve 5
- Cycle 3: Valve 4, Valve 6, Valve 7

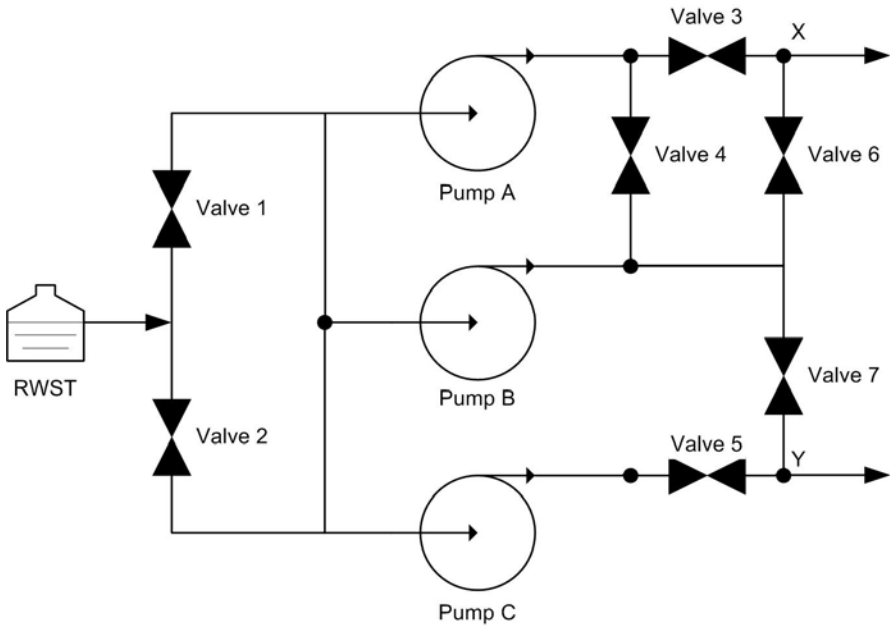


Figure 1: Schematics of the High-Pressure Injection System

Maintenance and repair times are deterministic for both types of subcomponents, whereas the failure rates a given by a stochastic distribution, e.g. Exponential distribution.

[Ion+03] developed a General Stochastic Petri Net (GSPN) for this HPIS model, containing both the dynamic behaviour of the maintenance cycles and the availability check, and stated parameters for the time distributions. However, restricting the model to the GSPN paradigm, no other time distributions than Exponential could be used for describing failure times. Due to the memorylessness of a Markovian process, maintenance will have no effect on the failure behaviour of the subcomponents. In case of different failure time distributions, the underlying stochastic process is no longer markovian, and thus cannot be analysed easily by calculating Markov chain solutions.

# 3 Modelling System Availability

The availability check of the HPIS can be described as part of the dynamic behaviour within the model [Ion+03]. In this case, a part of the Petri net consisting of nine places and 22 immediate transitions represents the flow of the water within the system. After each timed event such as the failure or the start of maintenance work of a component the immediate transitions are enabled and fired to determine the availability of the high pressure flow.

However, doing so will increase the number of states of the model exponentially and decelerate any used simulation algorithm, since many more state transitions have to be considered. A different approach would be the computation of the availability by a rate reward function, that is going to be computed while the simulation runs, eliminating the need for additional state transitions. Such a function would return a value of 1.0 in case the HPIS was available, and a value of 0.0 otherwise, for any state the system can be in. After standardisation with reference to the analysed mission time the result of the reward function is a floating-point value between 0.0 and 1.0, denoting the probability that the entire HPIS is available.

Figure 2 shows a Fault-tree-like Boolean representation for the reliability of the HIPS. Each of the circles on the left denotes the availability of one of the ten subcomponents (seven valves and three pumps), i.e., that system has not failed and is not currently maintained, as a binary information. Together, they are combined by a set of Boolean gates resulting in a Boolean expression denoting the availability of the entire HPIS ($A$). $A$ is true if and only if a high-pressure water flow can reach both points, $X$ and $Y$. The complete expression reads as follows, whereas $V_n$ stands for the operational status of Valve $n$ ($n$=1, 2,…, 7) and $P_x$ stands for the operational status of Pump $x$ ($x$ = A, B, C):

$$A = (V_1 \vee V_2) \wedge ((V_3 \wedge P_A) \vee ((V_6 \vee (V_3 \wedge V_4)) \wedge (P_B \vee (V_7 \wedge V_5 \wedge P_C)))) \wedge ((P_C \wedge V_5) \vee (V_7 \wedge (P_B \vee (P_A \wedge (V_4 \vee (V_3 \wedge V_6))))))) \quad (1)$$

A rate reward function is determined by the result of this expression and returns an appropriate indicator value of 0.0 or 1.0, respectively, while the simulation runs. This method reduces the number of states and hence the number of state transitions dramatically. Hence, the computation time of any analysis – may it be Monte Carlo driven or based on the state space – is reduced.

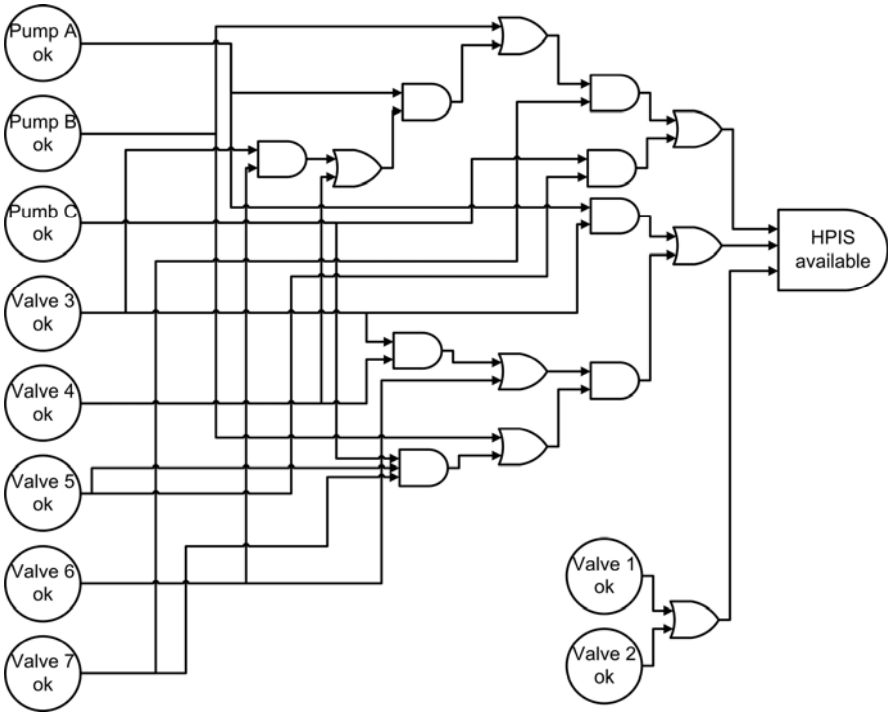


Figure 2: Fault-tree-like model for the availability of the HPIS

# 4 Proxel-based Simulation of the Dynamic Behaviour

The Proxel-based simulation method operates on the state-space and the reachability graph (RG) of the model. The RG can be generated prior to the actual computation or on-the-fly, that is, new nodes (states) and arcs (state transition) will be

added to the RG when they are found during the simulation. The latter method is the only choice for a solution of models with an infinite state space.

Indeed, for our model the reachability graph is finite, exactly holding 129,024 discrete states, timed and vanishing. Currently, the existing Proxel simulators are not able to compute accurate results for models of this size in reasonable time, not to mention faster than Monte Carlo Simulation of , say, $10^6$ system histories.

Instead, Proxel simulation performs very well for models with a small state space and rare events, such as a model that considers only one of the maintenance cycles. Since all three different cycles are independent of each other, the complete model can be split into three such models, one for each cycle. A simulation of one single cycle results in availability information for the subcomponents tested and/or repaired in that cycle for the time span of the simulation. Figure 3 shows the conceptual model of the first maintenance cycle as Stochastic Petri Net. The parameters for the distributions of the state transition are as follows:

- Cycle starts: Deterministic at 2184 hours
- Valve *n* is maintained: Deterministic at 0.75 hours
- Valve *n* fails: Exponential with a rate of 5.83E-6 failures per hour
- Valve *n* gets repaired: Deterministic with 2.4 hours

Proxel-based simulation of this model consists of two analysis runs with different discretisation step sizes $dt_1 = 4h$ and $dt_2 = 2h$ and a extrapolation of the simulation result with a theoretical dt=0, since the Proxel-based method has shown to make a first-order error for this model according to the discretisation step size. [Hort02], [LaHo03].

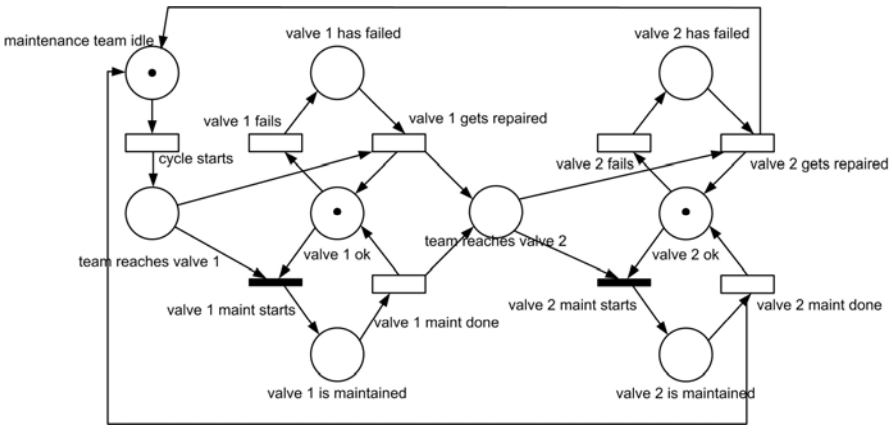


Figure 3: Petri net model for a maintenance cycle

Table 1 shows a comparison of the computation times of a Monte Carlo simulation with $10^6$ generated histories and two Proxel-based runs with the step sizes mentioned above. The simulated time span was $10^4$ hours. All computations were performed with a Pentium IV processor with 3 GHz. The Monte Carlo returns the mean and the standard deviation of a random variable describing the result. The results of the computation are shown in Figure 5.

| **Method** | **Comp. time in s** |
|---|---|
| Monte-Carlo ($10^5$ replications) | 18.14 |
| Monte-Carlo ($10^6$ replications) | 179.21 |
| Proxel (dt=2h) | 21.211 |
| Proxel (dt=1h) | 45.068 |
| Proxel ($dt_1$ = 2h, $dt_2$ = 1h) | 67.179 |

Table 1: Comparison of computation times for Cycle 1 model

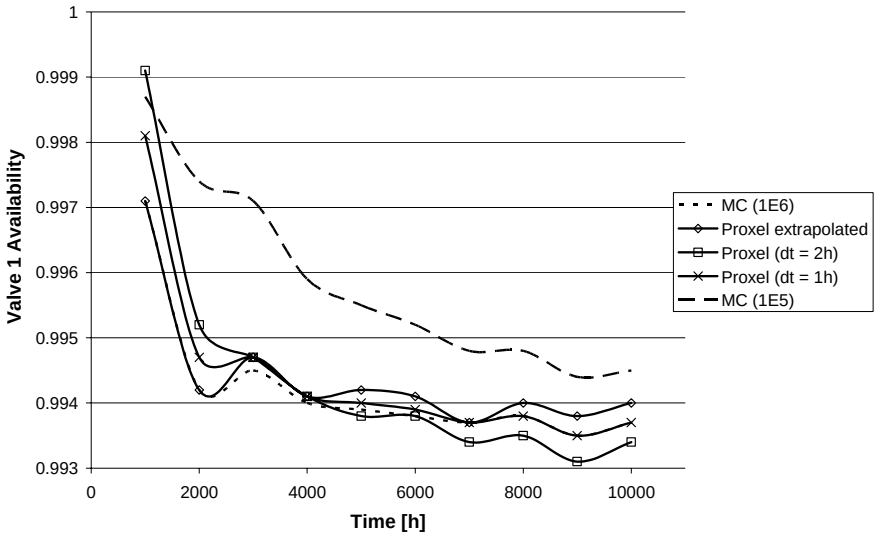


Figure 5: Computed availability of Valve 1 as a function of time

The Monte Carlo simulation with $10^5$ replications is not very accurate, because it does not discover the rare failure events often enough. A simulation of $10^6$ replications shows a much better curve. The Proxel-based computation with a step size of two hours is not as accurate as the second Monte Carlo simulation. A step size of

one hour proves to be more appropriate since it approaches the Monte Carlo simulation well. An extrapolation of the two Proxel method results leads to an even more accurate approximation of the availability.

The Proxel-based method with extrapolation needed less time to compute a mean value which can be assumed to be more accurate, since no (pseudo-)random numbers underlie the computation and all events are guaranteed to be considered. After being run one year (8760 hours) chances are, that the first valve has not been available for overall two days.

After simulation of each cycle, one knows the probability of being available for each subcomponent as a function of time. Furthermore, using probability calculation and the Boolean expression for the HPIS availability (1) one can also compute the probability of its disposability as a function of time. Figure 6 shows the results of this Proxel-based computation as a function of time. The computation took 17.2 minutes. A Monte Carlo driven simulation of the whole model would have needed 42.5 minutes. Thanks to the redundancy provided within the HPIS and its regular maintenance will be unavailable for altogether just about one hour within the whole considered mission time of $10^4$ hours (approx. 420 days).

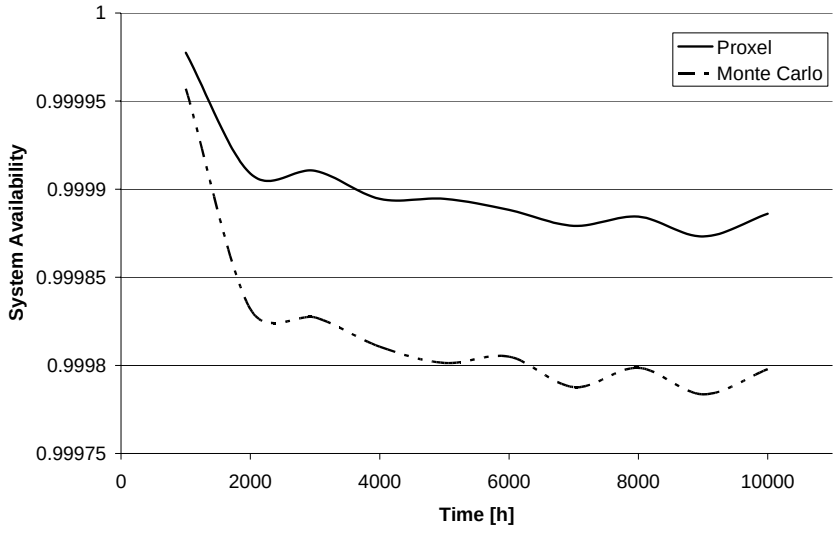


Figure 6: Computed availability of the HPIS as a function of time.

# 5 Conclusions

In this paper we have studied the reliability of a safety mechanism of a hazardous system in which the components are maintained or repaired in three independent cycles. We have decomposed an existing model into three independent models which we analysed with a Proxel-based simulation each at a time. This kind of simulation allows for a deterministic computation of reliability while not prohibiting general time distributions.

The combination of the components was modelled as a Fault-tree and an appropriate Boolean expression. The latter was used to combine the results of the simulation in a way that resulted in reliability of the system as a function of the mission time.

The main observations on the methodology are:

- Modelling availability by a Boolean expression and a rate reward function reduces the number of model states and state transitions, and thus the computation time of any analysing paradigm.
- Proxel-based simulation can be easily applied to reliability analysis of small systems with rare events.
- The results will be of higher accuracy since all possible developments of the model are guaranteed to be considered.
- Larger systems can be simulated by first decomposing the system into independent parts, simulating the received sub-models and joining the results by Boolean logic and probability arithmetic.

In our oppinion the Proxel method is suitable for the analysis of systems where rare events can result in a hazardous situation to the environment. The method ensures an accurate computation of the probability of those events and though helps estimating risks.

Our ongoing research is aimed towards further enhancing the Proxel-based algorithm by using different discretisation step sizes in order to gain a lower number of Proxels to process within the computation.

# References

[Hort02] Horton, G.: A New Paradigm for the Numerical Simulation of Stochastic Petri Nets with General Firing Times. In: European Simulation Symposium. SCS European Publishing House: Dresden, 2002

[IsHo04] Isensee, C.; Horton, G.: Proxel-Based Simulation of Project Schedules. In: European Simulation multiconference 2004. SCS European Publishing House: 2004.

[Ion+03] Ionescu, D.C.; Zio, E.; Constantinescu, A.C.: Embedding Monte Carlo simulation within the stochastic Petri network formalism for the evaluation of the availability of a nuclear safety system. In: Risc Decision and Policy, 8:1-10, Taylor & Francis: 2003.

[LaHo03] Lazarova-Molnar, S.; Horton, G.: An Experimental Study of the Behaviour of the Proxel-Based Simulation Algorithm. In: Simulation und Visualisierung 2003. SCS European Publishing House: Magdeburg, 2003.

[LaHo03a] Lazarova-Molnar, S.; Horton, G.: Proxel-Based Simulation of Stochastic Petri Nets Containing Immediate Transitions. In: On-Site Proceedings of the Satellite Workshop of ICALP 2003 in Eindhoven, Netherlands. Forschungsbericht Universität Dortmund: Dortmund, 2003.

[LaHo03b] Lazarova-Molnar, S.; Horton, G.: Proxel-Based Simulation for Fault Tree Analysis. In: 17. Symposium Simulationstechnik (ASIM 2003), SCS European Publishing House 2003.

[MaZi02] Marseguerra, M.; Zio, E.: Basics of the Monte Carlo method with application to system reliability. LiLoLe-Verlag GmbH (Publ. Co. Ltd.): 2002.