STUK

STUK-YTO-TR 178 June 2001

RELIABILITY ESTIMATION OF SAFETY-CRITICAL SOFTWARE-BASED SYSTEMS USING BAYESIAN NETWORKS

Atte Helminen
VTT Automation

STUK • SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

PLEASE BE AWARE THAT
ALL OF THE MISSING PAGES IN THIS DOCUMENT
WERE ORIGINALLY BLANK

The conclusions presented in the STUK report series are those of the authors and do not necessarily represent the official position of STUK.

ISBN 951-712-449-X
ISSN 0785-9325

Edita Oyj, Helsinki 2001

HELMINEN Atte (VTT Automation). Reliability estimation of safety-critical software-based systems using Bayesian networks. STUK-YTO-TR 178. Helsinki 2001. 23 pp.

ISBN 951-712-449-X
ISSN 0785-9325

Keywords: safety, safety analysis, reliability analysis, bayesian belief networks, automation, programmable systems, software-based systems, reactor protection systems, nuclear reactor safety

ABSTRACT

Due to the nature of software faults and the way they cause system failures new methods are needed for the safety and reliability evaluation of software-based safety-critical automation systems in nuclear power plants. In the research project "Programmable automation system safety integrity assessment (PASSI)", belonging to the Finnish Nuclear Safety Research Programme (FINNUS, 1999–2002), various safety assessment methods and tools for software based systems are developed and evaluated. The project is financed together by the Radiation and Nuclear Safety Authority (STUK), the Ministry of Trade and Industry (KTM) and the Technical Research Centre of Finland (VTT).

In this report the applicability of Bayesian networks to the reliability estimation of software-based systems is studied. The applicability is evaluated by building Bayesian network models for the systems of interest and performing simulations for these models. In the simulations hypothetical evidence is used for defining the parameter relations and for determining the ability to compensate disparate evidence in the models. Based on the experiences from modelling and simulations we are able to conclude that Bayesian networks provide a good method for the reliability estimation of software-based systems.

HELMINEN Atte (VTT Automaatio). Bayes-verkkojen soveltaminen turvallisuuskriittisten ohjelmoitavien automaatiojärjestelmien luotettavuuden arviointiin. STUK-YTO-TR 178. Helsinki 2001. 23 s.

ISBN 951-712-449-X
ISSN 0785-9325

Avainsanat: Turvallisuus, turvallisuusanalyysi, luotettavuusanalyysi, Bayes-verkot, automaatio, ohjelmoitavat järjestelmät, reaktorin suojausjärjestelmät, reaktoriturvallisuus

TIIVISTELMÄ

Ohjelmistovikojen luonteesta ja vaikutustavasta johtuen ydinvoimalaitosten turvallisuuskriittisten ohjelmoitavien automaatiosovellusten luotettavuuden ja turvallisuuden arviointiin tarvitaan uudenlaisia menetelmiä. Kansalliseen ydinturvallisuuden tutkimusohjelmaan (FINNUS, 1999–2002) kuuluvassa "Ydinvoimalaitosten ohjelmoitavien automaatiojärjestelmien turvallisuuden arviointi (PASSI)"-tutkimushankkeessa kehitetään, kokeillaan ja arvioidaan tähän soveltuvia menetelmiä. Hanketta ovat rahoittaneet Säteilyturvakeskus (STUK), Kauppa- ja teollisuusministeriö (KTM) sekä Valtion teknillinen tutkimuskeskus (VTT).

Raportissa tarkastellaan erityisesti Bayes-verkkojen soveltuvuutta ohjelmoitavien järjestelmien luotettavuuden arviointiin. Soveltuvuutta arvioidaan rakentamalla kiinnostaville järjestelmille Bayes-verkkoihin pohjautuvia malleja ja tekemällä simulointeja kyseisillä malleilla. Simuloinneissa selvitetään kuvitteellisen informaation avulla mallien parametrien välisiä riippuvuuksia, sekä kykyä korvata erilaista informaatiota keskenään. Mallinnuksesta ja simuloinneista saatujen kokemuksien perusteella voidaan sanoa, että Bayes-verkot soveltuvat hyvin ohjelmoitavien järjestelmien luotettavuuden arviointiin.

CONTENTS

1 INTRODUCTION

In the existing nuclear power plants the technical and economical ageing of analogue automation systems is causing more pressure for their replacement. The rapid increase of computer based systems in automation is favouring the gradual replacement of the current analogue systems with software-based digital systems. However, the replacement is not a straightforward operation when the system under replacement is classified as a safety-critical system such as the primary protection system of nuclear power plant. One of the main reasons why a substitution of safety-critical automated systems causes extra trouble lies in the question of reliability of the software-based systems and in the ability to assess this reliability.

When estimating the reliability of software-based systems there are some special characteristics to consider. First of all, the reliability of software-based system is a property of the operation environment as well as that of the system itself. Although there may be errors in the software, these errors can cause a loss of safety function only when certain inputs occurring with very low probability are introduced into the system. In other words, the reliability of a programmable system depends on the operational profile, which as the probability distribution of input sequences varies from one environment to another. This restricts the use of generic operational experience in the determination of reliability parameters. On the other hand, the quantitative reliability estimates should always be based on certain evidence, which is most often the operational experience statistics. Usually in the case of safety-critical software-based systems this evidence is either very limited or not applicable due to the differences between the operational profiles of the data sources and the actual system. Another source of evidence is obtained from the dynamic testing of system. If high reliability with high confidence level is required, the number of tests is very large, and it may be practically impossible to test a system extensively enough. Thus the use of additional evidence from other sources is inevitable for proper reliability estimation.

To obtain better estimates for the reliability of programmable systems, all possible evidence should be applied in the analysis. This requires extensive applications of expert opinions about the weight of various pieces of evidence. A most suitable approach for combining disparate evidence together using expert judgements is based on Bayesian inference. In Bayesian inference, all uncertainties in the model are expressed with probability distributions, and statistical inference is applied to the model. This means that the model does not actually estimate any model parameter but it determines the parameter probability distribution, which estimates the uncertainty about the value of the parameter. The excellence of Bayesian models is not evident only due to the subjective, degree of belief interpretation of probability, but also due to transparent modelling and consistent application of probability calculus.

The consistent application of probability calculus applied in Bayesian inference is a powerful tool when some variables are observed, and the distributions of other variables are updated based on these observations. The updating requires methods for the modelling of the joint distribution of all variables and methods for the modelling of conditional or marginal distributions of certain variables in the target system. All this can be done by means of probability calculus, and especially using Bayesian models. The reliability analysis of a software-based system usually involves a large number of variables and different potential sources of evidence. To manage in weighting and combining various pieces of evidence of a target system into a reliability estimate based on Bayesian

models, there is a technical solution called Bayesian networks. The Bayesian networks provide formalism with easily assimilable graphical representation for dependency models with efficient computational tools. Bayesian networks provide therefore a useful and attractive method of constructing models, which are based on the Bayesian inference.

In this work we use Bayesian networks to the reliability estimation of software-based systems. Our special interest lies in the automation systems classified as safety critical systems. Characteristic of these kind of systems is a multiple number of reliability related variables with very little evidence. Many of these variables are interrelated by dependencies of an experimental, probabilistic and even subjective nature, which are not always well understood formally. We try to clarify and relate these dependencies between different variables in the models, which we build using Bayesian networks. In the models, the construction of the automation system is left with little consideration and most of the interest is pointed towards the parameters reflecting the reliability of the system.

Similar studies on the reliability of software-based digital systems using Bayesian networks have been made previously for example in Littlewood et al. [1] and Fenton et al. [2]. The main differences between our study and the previous studies lie in the difference of focus areas. Our study is mainly focused to the explicit analysis of prior estimations and to the investigation of combining statistical evidence from disparate sources and operational profiles together. Also, the usage of continuous distributions in our work provides some new perspectives to the research area.

2 BAYESIAN NETWORKS

2.1 Bayesian inference

The basic idea of Bayesian inference is to express the uncertainty of all the unknown parameters of the model by probability distributions. This means that a parameter, which is unknown a priori is modelled as a random parameter. In the text the random parameters of our interest is denoted as $\Theta = (\Theta_1,...,\Theta_n)$, where the index n is assumed finite. In addition to random parameters Θ_i, i $\in$ $(1,...,n)$, there is a set of variables, which are observable. We denote these random variables by $\mathbf{Y} = (Y_1,...Y_m)$, where index m is finite. The observable variables Y_j, $j \in (1,...,m)$, may consist of statistical observations or various experts judgements.

The observed variables, or the evidence $\mathbf{y} = (y_1,...,y_m)$, are modelled by their joint distribution, i.e. the likelihood function $p(\mathbf{y}|\boldsymbol{\theta})$, which can be described as the probability to observe the evidence $\mathbf{y}$. Before observations are made, the uncertainty about the value of the random parameter Θ is modelled by a probability distribution, the prior distribution, which we denote by $p(\boldsymbol{\theta})$. The updated distribution, the posterior distribution, is the conditional distribution of Θ given the evidence, and we denote it by $p(\boldsymbol{\theta}\,|\,\mathbf{y})$. The evidence $\mathbf{y}$ provides additional information about Θ, and the posterior distribution is updated by using the Bayes' rule: [3],[4]

$$p(\boldsymbol{\theta}|\mathbf{y}) = \frac{p(\mathbf{y}|\boldsymbol{\theta})p(\boldsymbol{\theta})}{\int p(\mathbf{y}\,|\,\boldsymbol{\theta})p(\boldsymbol{\theta})d\boldsymbol{\theta}} \tag{1}$$

or when taken to a single random parameter level:

$$p(\theta_1,...,\theta_n|y_1,...,y_m) = \frac{p(y_1,...,y_m|\theta_1,...,\theta_n)p(\theta_1,...,\theta_n)}{\int_{\theta_1}\cdots\int_{\theta_n} p(y_1,...,y_m|\theta_1,...,\theta_n)p(\theta_1,...,\theta_n)d\theta_1...d\theta_n}. \tag{2}$$

The model under interest is usually complex, and to make the model more flexible, we assume further a random parameter $\boldsymbol{\Phi} = (\Phi_1,...,\Phi_k)$. So called hidden or auxiliary parameter, which cannot be valued or observed directly. When the model contains random parameter $\boldsymbol{\Phi}$, the equations (1) and (2) become:

$$p(\boldsymbol{\theta}|\mathbf{y},\varphi) = \frac{p(\mathbf{y},\varphi|\boldsymbol{\theta})p(\boldsymbol{\theta})}{\int p(\mathbf{y},\varphi|\boldsymbol{\theta})p(\boldsymbol{\theta})d\boldsymbol{\theta}} \tag{3}$$

and

$$p(\theta_1,...,\theta_n|y_1,...,y_m,\phi_1,...,\phi_k) = \frac{p(y_1,...,y_m,\phi_1,...,\phi_k|\theta_1,...,\theta_n)p(\theta_1,...,\theta_n)}{\int_{\theta_1}\cdots\int_{\theta_n} p(y_1,...,y_m,\phi_1,...,\phi_k|\theta_1,...,\theta_n)p(\theta_1,...,\theta_n)d\theta_1...d\theta_n}. \tag{4}$$

The conditional distribution of certain Θ_i given the observations, or the posterior distribution, is the conditional marginal distribution

$$p(\theta_i|y_1,...,y_m,\phi_1,...,\phi_k) = \int_{\theta_1}\cdots\int_{\theta_{i-1}}\int_{\theta_{i+1}}\cdots\int_{\theta_n} p(\theta_1,...,\theta_n|y_1,...,y_m,\phi_1,...,\phi_k)d\theta_1...d\theta_{i-1}d\theta_{i+1}...d\theta_n. \tag{5}$$

2.2 Bayesian networks

In practical applications the main task usually is to update the distribution of certain parameter Θ_i, when the values of the observable variables become known. In other words, we have to determine the conditional marginal distribution of the parameter Θ_i, given the observations **y**. To do this, we have to model the overall uncertainty by postulating the joint distribution of the all random variables of the model, i.e., the joint distribution of random vector $\Omega = (\Theta_1,...,\Theta_n,Y_1,...,Y_m,\Phi_1,...,\Phi_k)$, or

$$\begin{aligned} &p(\theta_1,...,\theta_n,y_1,...,y_m,\phi_1,...,\phi_k) = \\ &p(\theta_1)\cdot p(\theta_2|\theta_1)\cdot p(\theta_3|\theta_1,\theta_2)\cdot ...\cdot p(\phi_k|\theta_1,...,\theta_n,y_1,...,y_m,\phi_1,...,\phi_{k-1}), \end{aligned} \tag{6}$$

in which we have assumed that the appropriate conditional distributions are available. [4] The form of the joint distribution in equation (6) is determined by the dependencies between variables. Often we may assume a hierarchical dependency structure among the variables, which simplifies the model. For example, we may assume a model with $k = n$ and $m = n+1$, conditional independence of parameter Θ_i, given Θ_{i-1}, conditional independence of parameter Φ_i, given Θ_i, and conditional independence of the variables Y_i, given parameters Φ_{i-1} and Φ_i. All the conditional independence lead to following joint distribution:

$$\begin{aligned} &p(\theta_1,...,\theta_n,y_1,...,y_m,\phi_1,...,\phi_k) = \\ &p(\theta_1)\cdot p(\phi_1|\theta_1)\cdot p(y_1|\phi_1)\cdot p(y_2|\phi_1)\cdot \prod_{i=2}^{n}\left[p(\theta_i|\theta_{i-1})\cdot p(\phi_i|\theta_i)\cdot p(y_i|\phi_i)\cdot p(y_{i+1}|\phi_i)\right]. \end{aligned} \tag{7}$$

The joint distribution models described in formulas (6) and (7) consist of networks of conditional dependencies between random variables. Such networks are often called Bayesian networks. A Bayesian model, which can be represented as a directed acyclic graph, in which nodes correspond to random variables and directed arcs between the nodes describe the statistical dependence and possibly missing arcs between the nodes describes the statistical independence between the random variables, is a Bayesian network. As an example the graphical representation of the hierarchical model described by equation (7) is depicted as a Bayesian network in Figure 1.

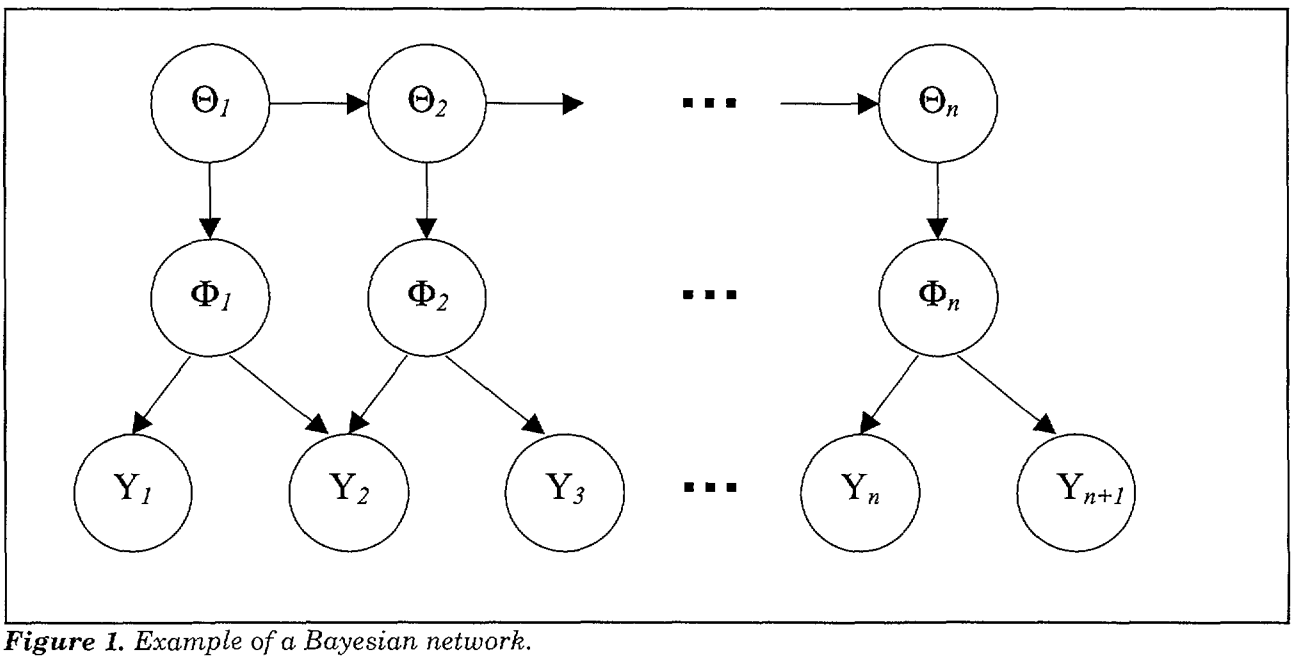

Figure 1. *Example of a Bayesian network.*

The joint distribution of the all random variables in equations (6) and (7) is also the numerator in equation (3), and the conditional marginal distribution of the parameter Θ_i can be determined combining the equations (4) and (5) to the following form:

$$p(\theta_i|y_1,...,y_m,\phi_1,...,\phi_k) =$$

$$\int_{\theta_1}\cdots\int_{\theta_{i-1}}\int_{\theta_{i+1}}\cdots\int_{\theta_n}\frac{1}{C}\cdot\left[p(y_1,...,y_m,\phi_1,...,\phi_k|\theta_1,...,\theta_n)\,p(\theta_1,...,\theta_n)\right]d\theta_1...d\theta_{i-1}d\theta_{i+1}...d\theta_n, \tag{8}$$

where the constant C stands for the normative denominator and can be solved from equation:

$$C=\int_{\theta_1}\cdots\int_{\theta_n}p(y_1,...,y_m,\phi_1,...,\phi_k|\theta_1,...,\theta_n)\,p(\theta_1,...,\theta_n)d\theta_1...d\theta_n. \tag{9}$$

In Bayesian models, where we are interested in the relationships of a large number of variables, Bayesian network becomes an appropriate representation. A Bayesian network is a graphical model that efficiently encodes the joint probability distribution for a large set of variables. Determining the conditional posterior distributions for the parameters of interest is usually not a simple task in Bayesian networks. To obtain an analytic result for the conditional posterior distribution the denominator of the Bayes formula, which normalises the conditional posterior distribution to unity, must be evaluated. A proportional result for the posterior distribution can be obtained without solving the denominator, but the integral for the numerator has only one dimension less. For analytic result, or at least for a good approximation of the result, the integrals have to be determined a way or another. For simple models the integrals can be evaluated using conventional numerical techniques, but in most applications the Bayesian network contain tens and hundreds of parameters and the analytic evaluation of the integrals by conventional numerical techniques is impossible. The evaluation of the distributions in large networks must be carried out with other means such as Monte Carlo simulation, as in our calculations below.

3 RELIABILITY ESTIMATION OF SOFTWARE-BASED SYSTEM

3.1 Combining evidence

The main sources of reliability evidence in the case of safety critical systems considered in this report are depicted in Figure 2. [1] Part of the evidence may be directly measurable statistical evidence, such as the evidence obtained through operational experience and testing. Part of the evidence may be qualitative characterisation of the system such as the design features and the development process of the system. The qualitative characterisation of the design features and the development process follows certain quality assurance and quality control principles, which are based on applicable standards. The more strict standards the characterisations fulfil the more reliable the system is believed to be. Later on in the text the evidence based on qualitative characterisation is considered as *soft evidence*, while evidence obtained from operational experience and testing is considered as *hard evidence*. The division of evidence as hard and soft evidence is always somewhat a fuzzy procedure, since even the evidence from testing and operational experience usually include some qualitative characterisations. The exploitation of soft evidence in the reliability analysis of software-based system requires extensive use of expert judgement and therefore

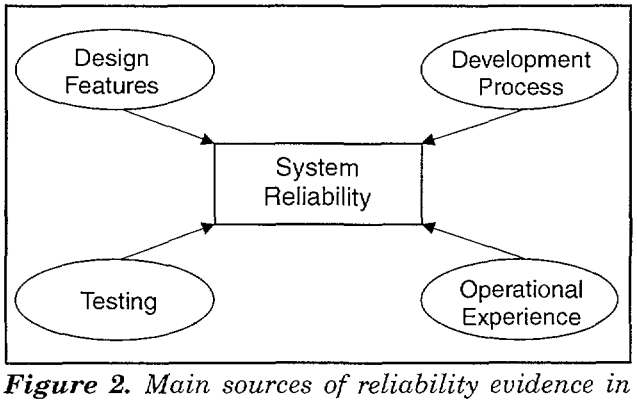

Figure 2. *Main sources of reliability evidence in the case of safety critical system.*

in this work the main interest is focused to the utilisation of hard evidence.

The software-based systems considered in this work are automation systems containing identical platforms with identical applications. The same methodology used in this work could be extended for systems with disparate platforms or applications, but the difference between different systems should be taken into consideration in the modelling.

In the models the reliability of software-based systems is modelled as a failure probability parameter, which reflects the probability that the automation system fails to operate correctly when demanded. Information for the estimation of the failure probability parameter can be obtained from the various sources of hard and soft evidence. To obtain the best possible estimate for the failure probability parameter of the target system all evidence should to be combined.

In this report this combining is carried out using Bayesian networks. The principle idea in our estimation method is to build a prior estimate for the failure probability parameter of software-based system using the soft and hard evidence obtained from the system development process, pre-testing and evaluating system design features while system is produced, but before it is deployed. The prior estimation is then updated to a posterior estimate using the hard evidence obtained from testing after the system is deployed and from operational experience while the system is operational. The difference between disparate evidence sources can be taken care in the structural modelling of the Bayesian network model.

To analyse the applicability of Bayesian networks to the reliability estimation of software-based systems we build Bayesian network models for safety critical systems representing on a general level very typical and common situations in

Table I. Different system and operational profile configurations.

Model 1	Evidence from one system with one operational profile
Model 2	Evidence from one system with two operational profiles
Model 3	Evidence from one system with multiple operational profiles
Model 4	Evidence from several systems something in common with multiple operational profiles

practice. The different models are distinguished by the evidence, which is collected from identical systems functioning in different operational profiles. The system and operational profile configurations under consideration are shown in Table I. After the Bayesian network models are built, we run several simulations to evaluate the failure probability parameters in the models and to study the feasibility of Bayesian networks in the reliability estimation. The modelling and simulations are carried out using the WinBUGS program, and so all the Bayesian networks presented below are depicted in the WinBUGS format. For closer review about the WinBUGS program, see Spiegelhalter et al. [5].

3.2 Failure probability and logit-transformation

For a system with hard evidence the failure probability may assume two different definitions as the failure probability can be seen as a number of failures on a defined number of demands or as a number of failures on a defined time period. For the defined number of demands n with the constant failure probability p the random number of failures Y has a binomial distribution defined as:

$$f(y|p,n)=\frac{n!}{y!(n-y)!}p^{y}(1-p)^{n-y};y=0,\ldots,n. \quad (10)$$

Respectively, for a defined time period the random number of failures follows a Poisson distribution. Because of the on demand nature of the safety critical automation system, we use the binomial representation in our models, but for Poisson representation the models would be similar.

To obtain an estimate for the random failure probability P, we need a prior estimation. The most appropriate choice for the distribution of P with binomial distributed Y would be the beta distribution. Since binomial and beta distributions form a conjugate prior distribution pair, the parameters P and Y could be sampled directly from the conditional posterior distribution and no reject-accept method would be necessary. However, we want to be able to combine different distributions flexibly together, and this can be conveniently carried out for example using the properties of normal distributions. Normal distribution is defined in the interval $(-\infty,\infty)$, and since the failure probability P in the binomial distribution is bounded between zero and one, the failure probability P needs to be transformed to extend over the entire real axis. This can be carried out using the following transformation:

$$\Theta=\ln\left(\frac{P}{1-P}\right), \quad (11)$$

and, if Θ is defined, P can be solved from:

$$P=\frac{e^{\Theta}}{1+e^{\Theta}}. \quad (12)$$

The transformation introduced in equation (11) is the *logit-transformation* of the parameter P. In practice, the assumption that the logit-transformed failure probability Θ is normally distributed also enables us to easily express the uncertainty about the parameter simply by altering the value of the variance in the normal distribution.

3.3 Bayesian network models

3.3.1 Model 1

The Bayesian Network shown in Figure 3 describes a system, for which the observed number of failures Y is binomial distributed with parameters N and P. Parameter N describes the number

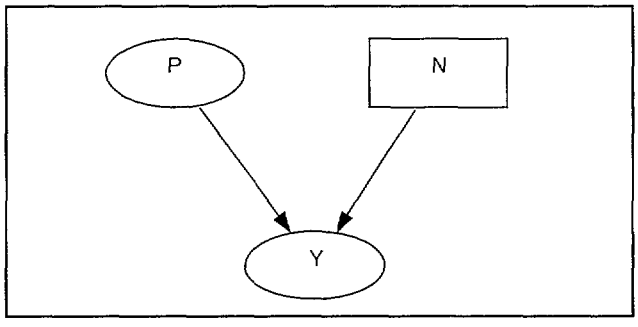

Figure 3. *Bayesian network for one test cycle.*

of demands in the single test cycle and parameter P is the random failure probability parameter. This model can be further extended to represent a system with several test cycles using the same operational profile and in Figure 4 this is shown for three separate test cycles. Since all the test cycles with identical operational profiles form a binomial distribution with P as a parameter, the information can be gathered to one large test cycle and the network shown in Figure 4 can be simplified back to the network shown in Figure 3 simply by summing the data using following formulas:

$$Y = \sum_i Y_i,$$
$$N = \sum_i N_i. \qquad (13)$$

To increase the flexibility of the model depicted in Figure 3, we include the logit-transformed P parameter named Theta into the network, and the network becomes as shown in Figure 5. The Bayesian network represented as model 1 can be used in the reliability estimation of a software-based system attached with binomial distributed hard evidence under unchanged operational profile.

3.3.2 Model 2

The hard evidence obtained for the reliability estimation of software-based systems is usually obtained from both, testing and operational experience. If the testing has been carried out under the same operational profile as the operational experience, equation (13) can be applied and the Bayesian network becomes the same as the Bayesian network in Figure 5. Often this is not the case, and the system is tested with a different operational profile under different operational environment. Since the errors in the software are triggered only when certain input occurs, the different operational profiles provide different failure probabilities for the same system. However, the failure probability from testing gives us some information about the failure probability of the same system functioning in a different operational profile. The evidence provided by testing is very valuable and we should make a good use of it by taking into account the difference in the operational profiles when building the model.

The problem of different operational profiles is solved by first connecting the binomial distributed evidence from different operational profiles to separate failure probability parameters, and then the logit-transformed failure probability parameters are connected to equal each other. The difference in the operational profile of the two failure probability parameters is carried to the model by adding a normal distributed random term Omega' to the logit-transformed failure probability parameter obtained from testing. The parameters of the normally distributed random term correspond to our belief of the difference between the two operational profiles. The Bayesian network representing the case is illustrated in Figure 6, where the parameters connected to the evidence obtained from the testing are illustrated by parameter names with apostrophes.

The fundamental idea behind the parameters Mu' and Sigma', which define the normal distributed random parameter Omega' in Figure 6, is based on the input space of the target system. As mentioned earlier in the text, it is not reasonable to test the target system with all possible inputs it

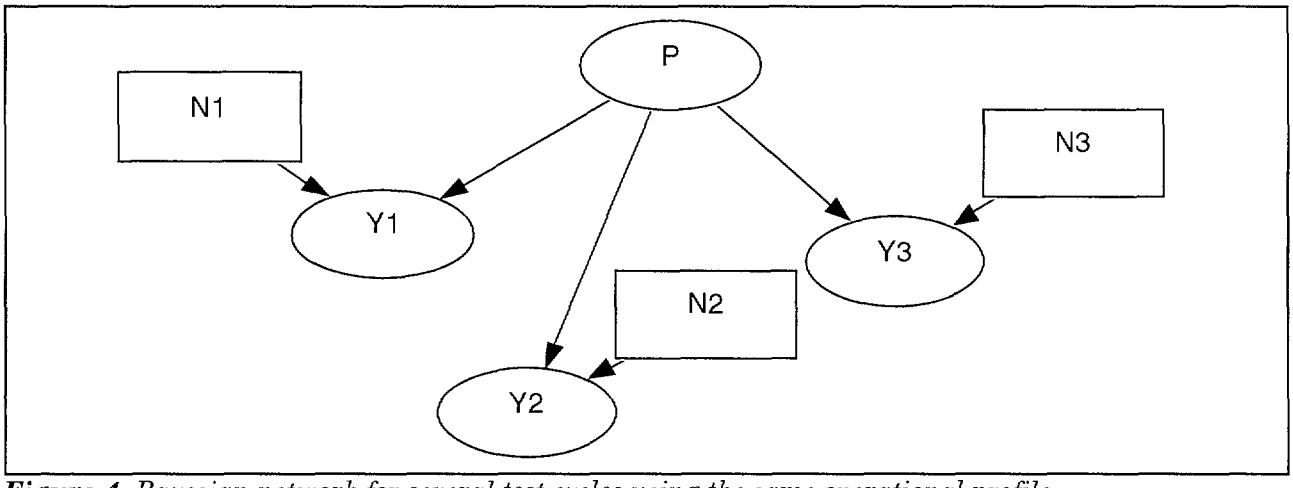

Figure 4. *Bayesian network for several test cycles using the same operational profile.*

might have, since the number of possible inputs would extend to enormous scales and the testing would take a huge amount of time. Because the test includes only a certain amount of inputs from certain areas of the whole input space, we can fix the two parameters to express our belief about the quality of the test. The magnitude of parameter Sigma' and the magnitude and sign of parameter Mu' are determined from how well the inputs of the test cover the whole input space of the target system and whether the probability of different inputs has been taken into account when choosing the inputs of the test.

For example, if the sign of parameter Mu' is negative it is believed that the test inputs are somewhat 'easier' than the inputs in the operational experience, and the significance of the test evidence applied to the reliability estimation of the target system is downgraded. If the sign of parameter Mu' is positive, the situation becomes opposite. In case the normal distributed random parameter Omega' has zero mean with zero variance the evidence obtained from testing and operational experience coincide, and model 1 can be applied.

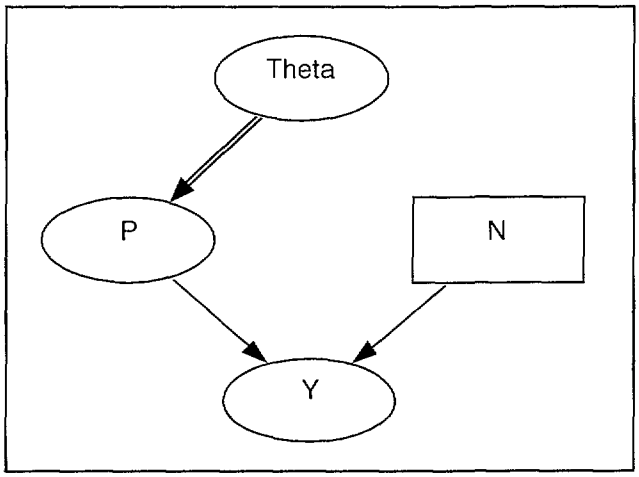

Figure 5. *Model 1.*

3.3.3 Model 3

The Bayesian network represented in Figure 6 can be generalised for the case of combining evidence from multiple operational profiles for the same system. This generalisation is depicted in Figure 7.

The different operational profiles are represented in the figure with overlays. The multiple operational profiles may be introduced to the model, besides from the sources described in model 2, but also from the testing and operational experience evidence of different power plants using the same software-base system under different operational and environmental conditions. The differences between the original operational profile, obtained for the operational experience of the target system, and the other operational profiles

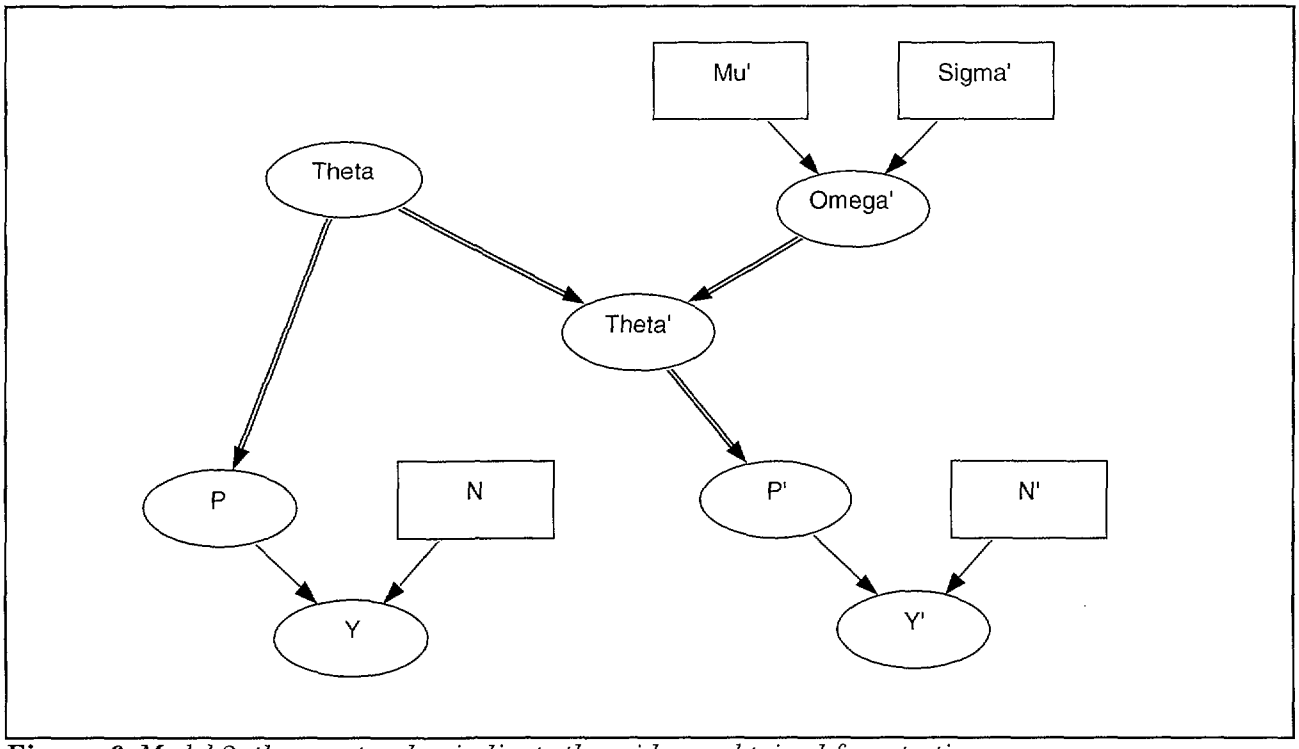

Figure 6. *Model 2, the apostrophes indicate the evidence obtained from testing*

are introduced to the model by adding a normal distributed random term Omega'[i] to each Theta'[i] parameter, which are the logit-transformed P'[i] parameters. The addition is similar to the procedure done in model 2 for the logit-transformed failure parameter Theta' obtained from testing.

3.3.4 Model 4

In some cases we may have several different systems with something intentionally common. This can be the case when making a reliability estimation of a software-based system using information from the previous versions of the system. The new version of the system can be just the old version but with known faults removed, or it can be an extension of the old system.

In the case of a new system version the reliability estimation for the system can be carried out using model 3 depicted in Figure 7. However, making the estimate with model 3 would not be very wise, since the reliability estimation for the system would have to be carried out separately after each version update and the information obtained from the earlier system versions would be lost. Instead, it is more rational to model each system version using model 3 and combine the system versions to a chain of systems, as it is done in Figure 8 for a model of two version updates.

The assumed enhancement or deterioration between different system versions has been implemented to the model by the same procedure as with the different operation profiles of single system in models 2 and 3. This means that the difference is introduced to the model by adding a normally distributed random variable Omega to the logit-transformed failure probability parameter Theta of each new system version. Models, such as illustrated in Figure 8, enable reliability estimations that can be expanded over the entire lifespan of the software-based system, and thus making the continuous reliability estimation more feasible. The reliability estimation model for a system with multiple versions is shown here only as an interesting extension, and there are no calculations concerning the model in this report.

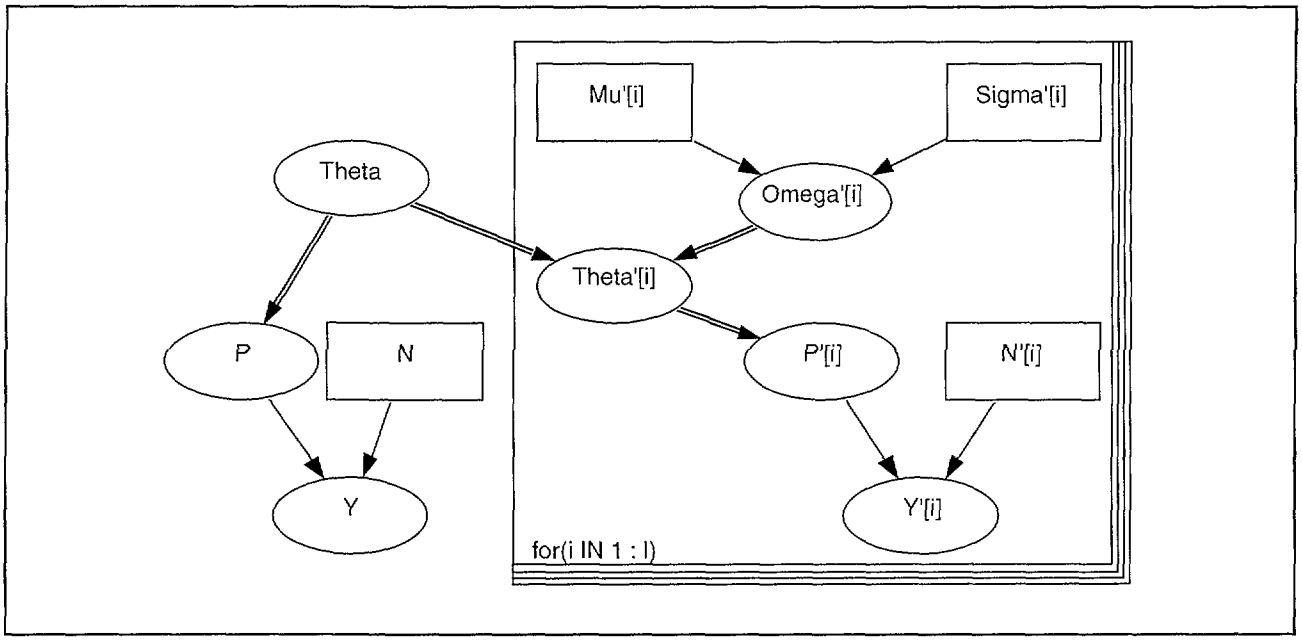

Figure 7. *Model 3.*

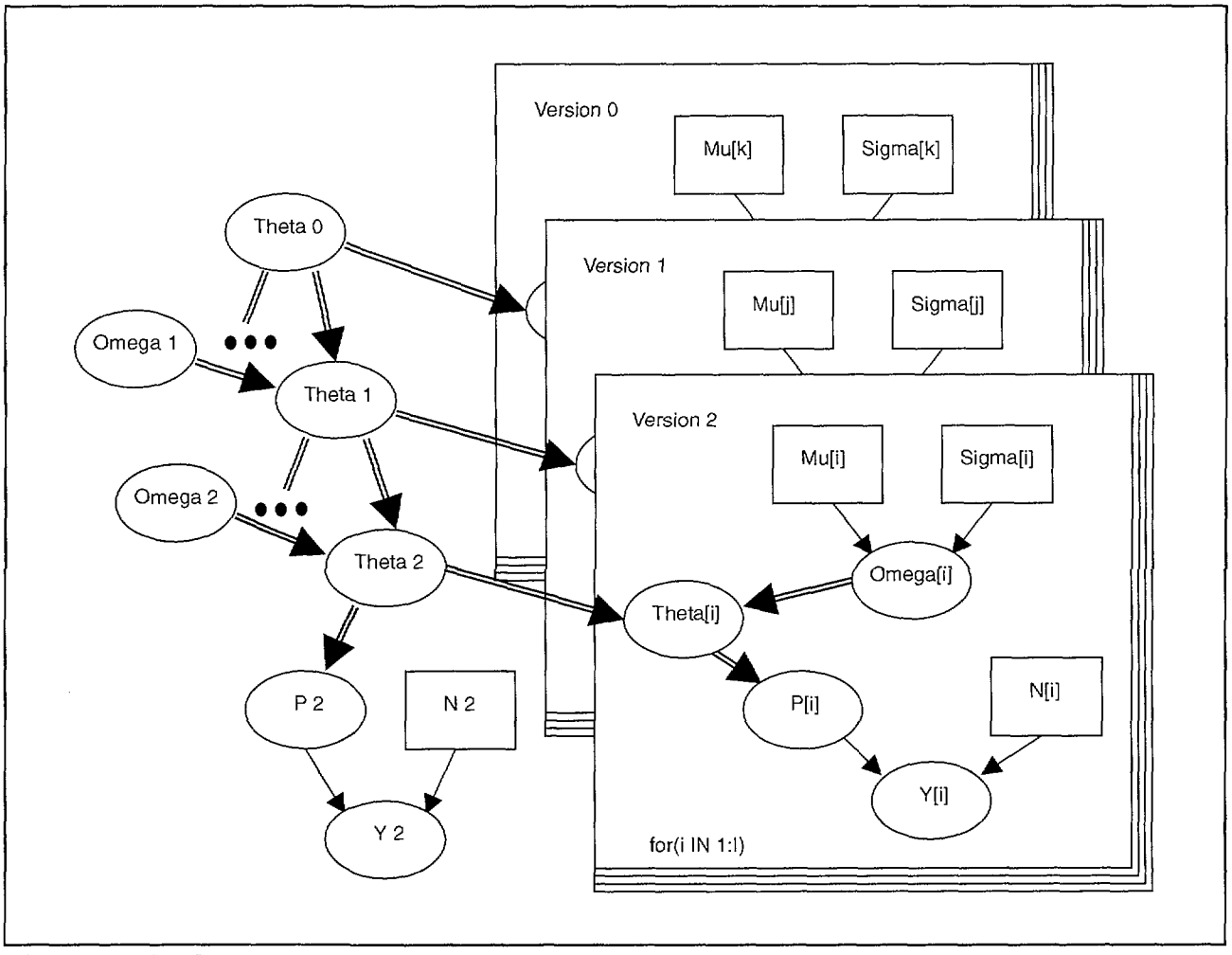

Figure 8. *Model 4.*

4 NUMERICAL EXAMPLES

4.1 Prior distribution of the failure parameter

In the previous chapter we mentioned that the prior estimation of failure probability parameter is built using the information obtained from the system development process, pre-testing and evaluating system design features. In the models the prior estimation is usually given as a prior distribution, which should express the assessor's a priori knowledge on the failure probability parameter, as well as possible. The selection of the prior distribution is one of the most important issues of Bayesian statistical inference. If only little is known about the failure parameter, then the prior distribution should be flat. On the other hand, if the most weight is given to the sample, then so called non-informative prior distributions should be applied, see Box & Tiao [6] for details.

In the case of Bernoulli or binomial sampling, which is the basic setting in this work, it would be convenient to use a beta-prior distribution, where the parameters can be interpreted to reflect the assessor's prior belief about the reliability of the system. In beta-prior distribution $B(p|\alpha,\beta)$, the parameters can be selected so that α is the number of failures on $\alpha + \beta$ number of demands, for details see Korhonen et al. [7]. However with the transformed normal distributed prior distribution, which is used in our approach, the interpretation between the distribution parameter and number of failures on certain number of demands is not as straightforward. Therefore, the characteristics of the transformed normal distributed prior should be considered in detail.

In the text below we use parameters named by the models in chapter 3. The relationships between different parameters are considered here only for the most basic case, but the same relationships can be generalised to the other repetitive parts in the models.

While the data in the analysis is increased, the influence of the prior distribution is decreased. This can be seen from Figure 9, where the 90 percentile posterior distribution values have been sampled for model 1 with a variety of different prior distributions. The prior distributions in the figure are separated by the prior variance value of parameter Theta, and the simulations for the posterior distributions are run with increased number of faultless data, i.e. N increases while Y remains zero. The same figure in logarithmic scale of P is presented in Figure 10.

Besides the prior variance value of parameter Theta, the prior mean value of Theta has also an influence to the posterior distribution of parameter P. The corresponding graphs of 9 and 10 are shown in Figures 11 and 12 for the different prior mean values of Theta. From Figures 11 and 12 similar conclusions about the decreasing importance of the prior mean value of Theta to the

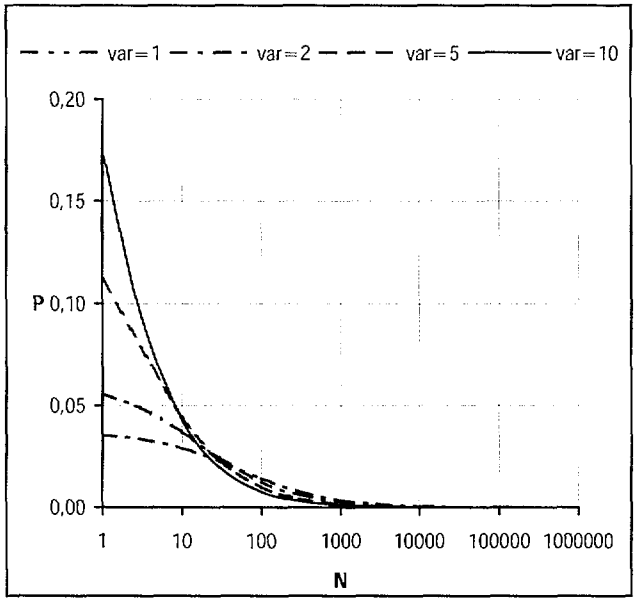

Figure 9. *Sampled 90 percentile posterior distribution values for P. Prior mean value for* Theta *is* $\mu = -4{,}595$.

posterior distribution of P can be made for the increasing number of faultless data. In fact the influence of the prior mean seems to be even smaller than the influence of the prior variance for large quantities of data, since the curves in Figure 12 converge more stronger than the curves in Figure 10 for large N.

With beta-prior distribution a similar 90 percentile posterior distribution for the parameter P can be obtained. An example of such calculation is shown in Korhonen et al. [7]. This gives us a reason to believe that there is a certain relation between the prior parameters of beta distribution and the prior parameters of transformed normal distribution. Defining such relation would be a great advantage in the determination of the prior parameters of the transformed normal distribution from the basis of the evidence obtained from the qualitative characterisation and pre-testing.

From Figures 9–12 it can be approximately estimated how many tests need to be run for a single system functioning in one operational environment to achieve certain reliability. The curves in the figures indicate that a better system reliability is achieved for a smaller amount of faultless data if the prior mean is small and the prior variance is large. In fact, a prior reliability estimation of small prior mean and large prior variance may reduce the amount of data needed to achieve a certain reliability level for the system to a fraction of the data that would be needed if the prior estimate had a large prior mean with small prior variance. However, to achieve a system reliability of less than one failure in one hundred thousand demands a huge number of tests need to be run, no matter how favourable the prior estimation is. To reduce this big number of tests needed for the high reliability estimation of the system it is rational to use the evidence obtained from other operational profiles.

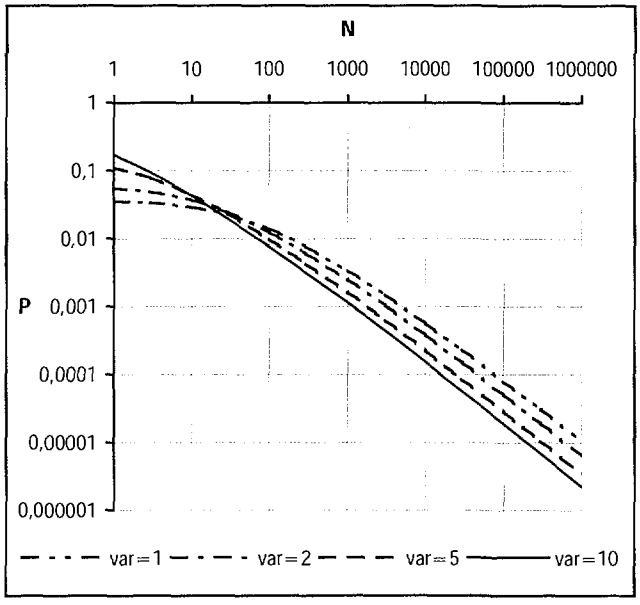

Figure 10. *Sampled 90 percentile posterior distribution values for P on logarithmic scale. Prior mean value for* Theta *is* $\mu = -4{,}595$.

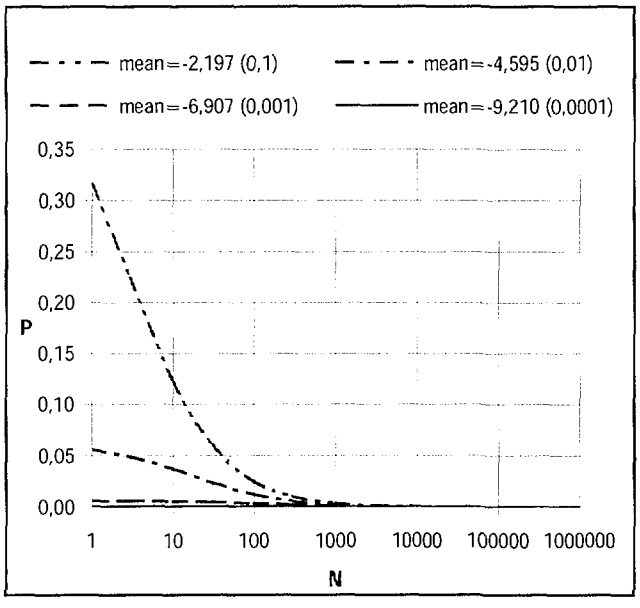

Figure 11. *Sampled 90 percentile posterior distribution values for P. Prior variance value for* Theta *is* $\sigma^2 = 2$.

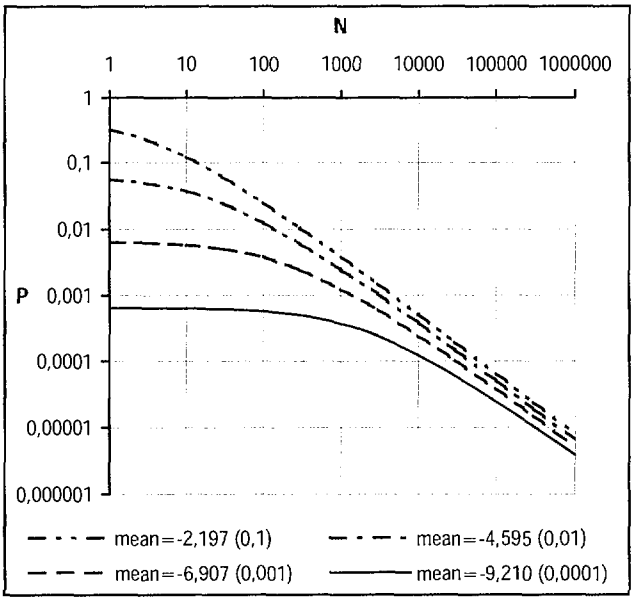

Figure 12. *Sampled 90 percentile posterior distribution values for P on logarithmic scale. Prior variance value for* Theta *is* $\sigma^2 = 2$.

4.2 Combining evidence from two operational profiles

The interesting question, when combining evidence for a same system running in two different operational profiles, is how much the evidence coming from the other operational profile can compensate the lack of operational experience obtained from different operational profile. This question is clarified in following simulations, which are carried out using model 2 with different values of parameters Mu' and Sigma'.

It was shown in the previous paragraph that to achieve the system failure probability of 10^{-5} per demand, which is the required failure probability of the reactor scram [8], the number of tests needed for a single system operating in one operational profile extends to several hundred thousand test cases. The number of tests can be reduced if we use redundant independent systems and the functionality of one system is enough to secure the functionality of the whole safety operation. However, the independence of software-based systems may not be proven as easily as it can be proven for analogue systems. The dilemma concerning the independence of software-based systems is not considered in this work or in the simulation below, and so the reader should take this fact into account when reading the results of the calculations.

In the case of two redundant independent systems the required system failure probability drops down from $1 \cdot 10^{-5}$ to approximately $3 \cdot 10^{-3}$ failures per demand. The magnitude of test cases needed for the reliability estimation of such systems is approximately 1000, which is the number of test cases we use as a base number for the calculations below.

In the calculations the 97,5 percentile comparison value is first calculated for the system with 1000 faultless test cases obtained from the operational experience, i.e. the parameter N having value 1000 and the parameter Y having value 0. The number of test cases N is then decreased and by increasing the number of faultless tests obtained from the other operational profile, i.e. decreasing N and increasing the parameter N' with the parameters Y and Y' remaining 0, the corresponding equilibrium with the comparison value is determined. The same calculation is carried out for different values of Mu' and Sigma'. The result for three different Mu' values with the Sigma' value of one is shown in Figure 13 and the corresponding result for three different Sigma' values with the Mu' value of zero is shown in Figure 14. The reader should notice that because of the WinBUGS language the parameter Sigma' is the inverse value of the variance of the normal distributed parameter Omega'. The prior values for the parameter Theta in all the simulations were $\mu = -4{,}595$ and $\sigma^2 = 1{,}0$.

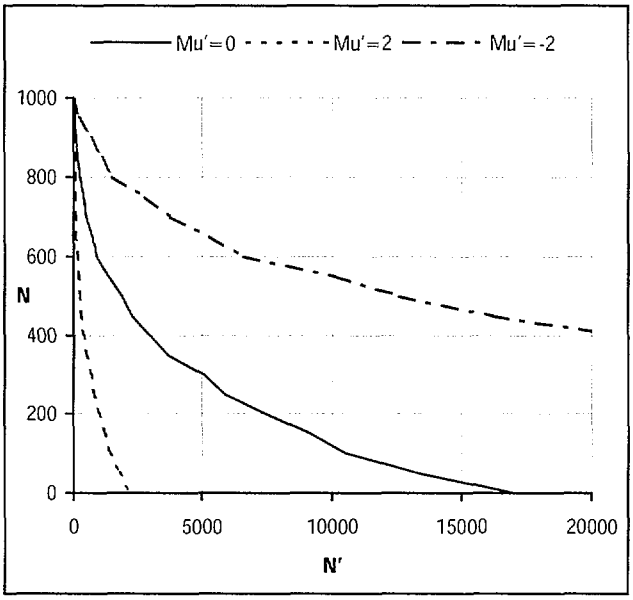

Figure 13. *Relation between the evidence obtained from operational experience* N *and the evidence obtained from other operational profile* N'.

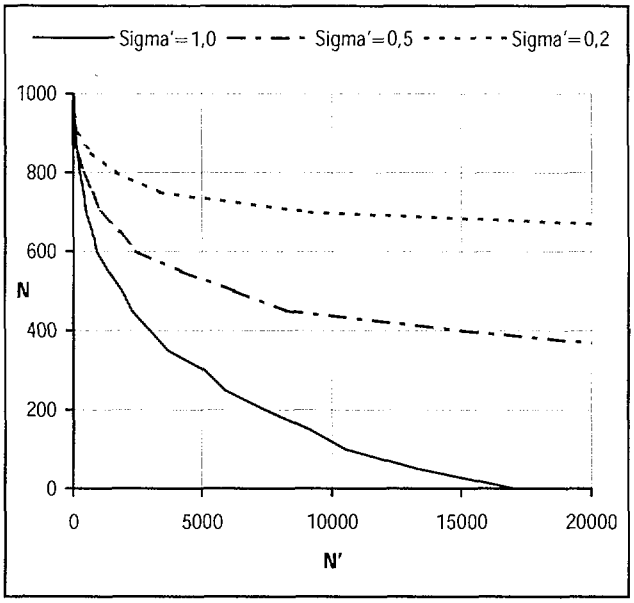

Figure 14. *Relation between the evidence obtained from operational experience* N *and the evidence obtained from other operational profile* N'.

The results confirm our former beliefs about the meaning of the parameters Mu' and Sigma', which were explained in chapter 3. With the negative value of Mu' the inputs of the other operational profile are believed to be somewhat less rigorous than the inputs of the operational experience, and so the amount of test cases needed from the other operational profile to compensate the lack of operational experience is larger. With the positive values of Mu' the situation is opposite and the amount of test cases needed from the other operational profile is smaller. The situation is illustrated in detail in Figure 13, where the solid line denotes the reference line, the upper dashed line denotes the negative value of Mu' and the lower dashed line denotes the positive value of Mu'. With the parameter Sigma' the situation is more straightforward. The magnitude of parameter Sigma' reflects how accurately the parameter Mu' can be determined, which means how well the rigorous of the inputs of the other operational profile can be evaluated. As the parameter Sigma' decreases, i.e. the variance of the parameter Omega' increases, the amount of test cases needed from the other operational profile to compensate the lack of operational experience is increased. The situation is shown in detail in Figure 14.

4.3 Combining evidence from multiple operational profiles

A similar estimation about the ability to compensate the lack of operational experience as done above for the evidence obtained from one other operational profile can be done for the evidence obtained from several operational profiles. In such estimation, the interesting question is what kind of an influence does the increasing number of other operational profiles have to the compensation of the operational experience. To estimate such an influence, simulations with model 3 are done with constant parameters Mu' and Sigma' and with increasing number of operational profiles.

The calculations are carried out using the same method as it was done in the calculations for two different operational profiles above. For the parameter Mu' having value zero and the parameter Sigma' having value one, the number of other operational profiles is extended from one to two and five, and corresponding equilibrium with the comparison value, i.e. N having value 1000 and N' having value zero, is determined. The results of the calculations are shown in Figure 15. From the figure it can be seen that while the evidence coming from the other operational profiles is divided with a larger number of operation profiles having similar parameter values, the number of test cases needed from the other operational profiles to compensate the lack of operational experience becomes smaller. However it is reasonable to ask if the evidence obtained from the other operational profiles can ever fully compensate the operational experience of the system, and therefore can the curves in Figure 15 cross the straight line drawn between the axes values of one thousand.

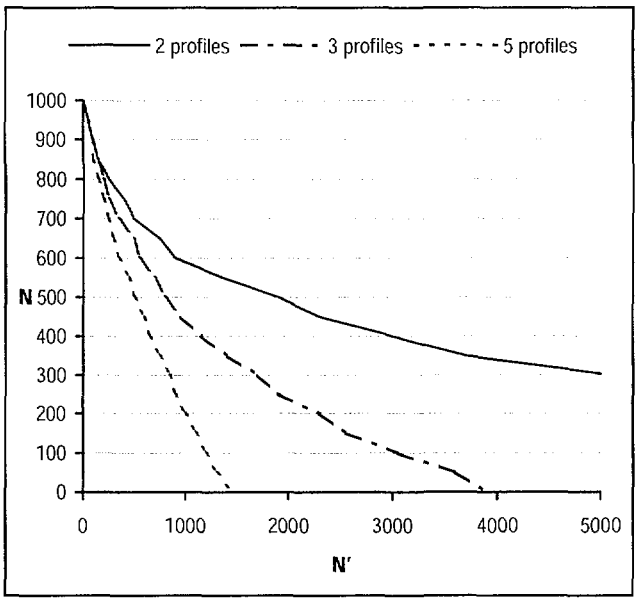

Figure 15. *Relation between the evidence obtained from operational experience N and the evidence obtained from other operational profiles N'.*

5 CONCLUSIONS

Based on this study we are able to conclude that the Bayesian network modelling provide a flexible and compatible tool for combining different evidence from various sources together. The models built using Bayesian networks are always subjective views, encoded as probabilistic statements, of the modeller's comprehension about the system and the different operational environments of the system. The transparency in the Bayesian network modelling, however, ensures that all parameters and their prior estimations in the model are in sight, and therefore are open for discussion and suggestions to improve the model can be made. On the other hand, the influence of subjective evidence introduced to the models for example by the qualitative characterisations of the system is decreased, as more data is included to the models.

In the simulations the influence of prior estimations was determined and some notation about the interpretation of different prior values were made. The dependencies between different parameters, and between different parameters and data were clarified. The ability to compensate the evidence from one source with the evidence from other sources was determined for the few different cases. Overall, the simulation results indicate that Bayesian networks provide an efficient and consistent way of applying Bayesian inference, and therefore probability calculus, to the complex reliability estimation models.

Characteristic of the reliability estimation of safety critical systems is high reliability requirements with only little statistical evidence available. This dilemma cannot be solved explicitly with any statistical method, and therefore the best way to compensate the lack of statistical evidence is to apply all possible evidence to the estimation. This means that the evidence from other similar systems and the evidence from qualitative characterisations of the system should also be included to the estimation. Based on the experience of this report the Bayesian networks provide an efficient way of combining all kind of evidence together, and thus generating a method for estimating the reliability of software-based systems.

REFERENCES

[1] Littlewood B, Fenton N E & Neil M, *Applying Bayesian Belief Networks to Systems Dependability Assessment*, In: 4th Safety Critical Systems Symposium, 1996, Leeds. Proceedings of the conference, Springer Verlag, 1996: pp.71–93.

[2] Fenton N E, Littlewood B, Neil M, Strigini L & Wright D, *Bayesian Belief Network Model for the Safety Assessment of Nuclear Computer-based Systems*, In: DeVa ESPRIT Long Term Research Project No. 20072—2nd Year Report, City University, London, 1997: pp.1–28.

[3] Gelman A, Carlin J B, Stern H S & Rubin D B, *Bayesian Data Analysis*, Chapman & Hall, London, 1995: pp.1–526.

[4] Pulkkinen U & Holmberg J, *A Method for Using Expert Judgement in PSA*, Finnish Centre for Radiation and Nuclear Safety, Helsinki, 1997: 1-32.

[5] Spiegelhalter D, Thomas A, Best N & Gilks W, *BUGS 0.5 Bayesian Inference Using Gibbs Sampling Manual (version ii)*, MRC Biostatistic Unit, Cambridge, 1996: pp.1–59.

[6] Box G & Tiao G, *Bayesian Inference in Statistical Analysis*, Addison-Wesley Publishing Company, Reading, 1972: pp.1–588.

[7] Korhonen J, Pulkkinen U & Haapanen P, *Statistical Reliability Assessment of Software-Based Systems*, Finnish Centre for Radiation and Nuclear Safety, Helsinki, 1997: pp.1-31.

[8] Guide YVL 2.8, *Probabilistic Safety Analyses (PSA)*, Finnish Centre for Radiation and Nuclear Safety, Helsinki, 1997: pp.1–10.

STUK-YTO-TR-reports

STUK-YTO-TR 180 Ansaranta T, Ala-Heikkilä J, Aarnio P (TKK). Comparison of radionuclide data analysis results of the CTBTO/IDC and the Finnish NDC.

STUK-YTO-TR 179 Orantie K, Kuosa H, Häkkä-Rönnholm E (VTT). Ydinvoimalaitoksen suojarakennuksen pinnoitteita koskevat vaatimukset.

STUK-YTO-TR 178 Helminen A (VTT). Reliability estimation of safety-critical software-based systems using Bayesian networks.

STUK-YTO-TR 177 Honkamaa T (ed.). Spent fuel encapsulation and verification. Safeguards workshop in Helsinki, Finland, 19–20 December 2000. Phase II interim report on Task FIN C1184 of the Finnish Support Programme to IAEA Safeguards.

STUK-YTO-TR 176 Saario T, Mäkelä K, Laitinen T, Bojinoff M (VTT). Susceptibility of copper to general and pitting corrosion in saline groundwater.

STUK-YTO-TR 175 Tiitta A, Hautamäki J (VTT), Turunen A (STUK), Arlt R, Arenas Carrasco J, Esmailpour-Kazerouni K (IAEA), Schwalbach P (Euratom). Spent BWR fuel characterisation combining a fork detector with gamma spectrometry. Raport on Task JNT A 1071 FIN of the Support Programme to the IAEA Safeguards.

STUK-YTO-TR 174 Smartt H, Martinez R, Caskey S (Sandia National Laboratories), Honkamaa T, Ilander T, Pöllänen R (STUK), Jeremica N, Ford G (Nokia). Secure transfer of surveillance data over Internet using Virtual Private Network technology. Field trial between STUK and IAEA. Interim report on Task FIN A929 of the Finnish Support Program to IAEA Safeguards.

STUK-YTO-TR 173 Hautamäki J, Tiitta A (VTT). Spent fuel verification options for final repository safeguards in Finland. A study on verification methods, their feasibility and safety aspects.

STUK-YTO-TR 172 Pulkkinen U, Simola K (VTT). An expert panel approach to support risk-informed decision making.

STUK-YTO-TR 171 Haapanen P, Korhonen J, Pulkkinen U (VTT). Licensing process for safety-critical software-based systems

STUK-YTO-TR 170 Tanskanen A (VTT). Assessment of the neutron and gamma sources of the spent BWR fuel. Interim report on Task FIN JNT A 1071 of the Finnish support programme to IAEA Safeguards.

STUK-YTO-TR 169 Kattilakoski E, Suolanen V (VTT). Groundwater flow analysis and dose rate estimates from releases to wells at a coastal site.

STUK-YTO-TR 168 Mankamo T (Avaplan Oy), Marttila J, Reponen H. Experiences from the LNPP-P&DSA review. Lessons learned from RBMK safety studies.

STUK-YTO-TR 167 Anttila M (VTT). Integrated Safeguards proposal for Finland. Final report on Task FIN C 1264 of the Finnish support programme to IAEA Safeguards.

STUK-YTO-TR 166 Rossi J (VTT). Significance of the results from probabilistic safety assessment at level 2 for off-site consequences.

Complete list of STUK-YTO-TR-reports is available from STUK.

STUK's website: http://www.stuk.fi/