INL/CON-10-18284
PREPRINT

Common-Cause Failure Treatment in Event Assessment: Basis for a Proposed New Model

PSAM-10

Dana Kelly
Song-Hua Shen
Gary DeMoss
Kevin Coyne
Don Marksberry

June 2010

Common-Cause Failure Treatment in Event Assessment: Basis for a Proposed New Model

Dana Kelly[a1], Song-Hua Shen[b], Gary DeMoss[b], Kevin Coyne[b], and Don Marksberry[b]

[a]Idaho National Laboratory, Idaho Falls, USA

[b]U.S. Nuclear Regulatory Commission, Washington, DC, USA

Abstract: Event assessment is an application of probabilistic risk assessment in which observed equipment failures and outages are mapped into the risk model to obtain a numerical estimate of the event's risk significance. In this paper, we focus on retrospective assessments to estimate the risk significance of degraded conditions such as equipment failure accompanied by a deficiency in a process such as maintenance practices. In modeling such events, the basic events in the risk model that are associated with observed failures and other off-normal situations are typically configured to be failed, while those associated with observed successes and unchallenged components are assumed capable of failing, typically with their baseline probabilities. This is referred to as the failure memory approach to event assessment. The conditioning of common-cause failure probabilities for the common cause component group associated with the observed component failure is particularly important, as it is insufficient to simply leave these probabilities at their baseline values, and doing so may result in a significant underestimate of risk significance for the event. Past work in this area has focused on the mathematics of the adjustment. In this paper, we review the Basic Parameter Model for common-cause failure, which underlies most current risk modelling, discuss the limitations of this model with respect to event assessment, and introduce a proposed new framework for common-cause failure, which uses a Bayesian network to model underlying causes of failure, and which has the potential to overcome the limitations of the Basic Parameter Model with respect to event assessment.

Keywords: PRA, common-cause failure, event assessment, Bayesian network.

1. INTRODUCTION

Event assessment is an application of probabilistic risk assessment (PRA) in which observed equipment failures and outages are mapped into the risk model to obtain a numerical estimate of the event's risk significance. Such an assessment can be either prospective, as when utilities use PRA as an aid in planning and scheduling equipment maintenance, or retrospective, such as in the Nuclear Regulatory Commission's Significance Determination Process (SDP) and Accident Sequence Precursor (ASP) Program. In this paper, we focus on retrospective assessments intended to estimate the risk significance of degraded conditions, such as equipment failure accompanied by a deficiency in a process such as maintenance practices. In modeling such events, the basic events in the PRA model that are associated with observed failures and other off-normal situations are typically configured to be failed, while those associated with observed successes and unchallenged components are assumed capable of failing, typically with their baseline PRA probabilities. The conditioning of common-cause failure (CCF) probabilities for the common cause component group (CCCG) associated with the observed component failure is particularly important, as it is insufficient to simply leave these CCF probabilities at their baseline PRA model values, and doing so may result in a significant underestimate of risk significance for the event. Past work in this area has focused on the mathematics of the adjustment (1). In this paper, we review the Basic Parameter Model (BPM) for CCF (2), which underlies most current PRA modelling, discuss the limitations of this model with respect to event assessment, and introduce a proposed new framework for CCF, which uses a causal-based Bayesian network to model underlying causes of failure explicitly. Such a model has the potential to overcome the limitations of the BPM with respect to event assessment, but there are implications for further research and development, which we will touch upon in the conclusions.

[1] Dana.Kelly@inl.gov

2. GENERAL EVENT ASSESSMENT PHILOSOPHY

Before turning to the specific issue of CCF, it is helpful to review some principle concepts underlying the use of PRA for event assessment. Most event assessments in the U.S. are done as part of the NRC's SDP, which is intended to evaluate the risk significance of inspection findings that represent a deficiency in licensee performance. Therefore, the analyst is attempting to quantify the risk significance of the deficiency using a PRA model. For example, if the deficiency that led to the observed failure was poor material control, then the retrospective risk assessment is attempting to estimate the risk significance of the equipment failure caused by this deficiency, and the analysis includes a probabilistic treatment of failures that were not actually observed, but could have been, because multiple equipment items could be impacted by the deficiency. Because nuclear plants utilize redundant safety equipment, the risk significance of such a deficiency will often focus on the potential for CCF of this redundant equipment. Thus, a crucial term in the event assessment risk equation is the conditional probability that remaining redundant components could fail, given that one or more such components have failed as a result of the identified performance deficiency. Note that the shared cause of failure at this level is the material control deficiency; the manner in which the deficiency is manifested across components may vary. In other words, two components could fail in the same *mode* due to CCF, with the *shared cause* being the material control deficiency, but the *failure mechanism* at the subcomponent or piece-part level might not be the same. CCF does not require that the failure *mechanism* be identical, only that the *cause* of failure is shared.

In assessing the risk significance of a past event, the analyst fundamentally is attempting to estimate the conditional probability of core damage; the analysis is necessarily counterfactual because the actual event did not lead to core damage. Therefore, the event is not modeled exactly as it transpired as this would lead to a conditional core damage probability of zero. Instead, the analyst accounts for the possibility that equipment that functioned successfully (or was not demanded) in the actual event might, with some probability, fail to function. Thus, parameters such as equipment failure probabilities and human error probabilities are left at their unconditional values or are conditioned as necessary to reflect the salient characteristics of the event. This is referred to as the *failure memory approach* to event assessment (3). The conditioning of CCF basic event probability is particularly important because it is incorrect to simply leave CCF probabilities at their unconditional values, and doing so may result in a significant underestimate of conditional core damage probability for the event.[2]

3. ROLE AND TREATMENT OF CCF IN PRA

CCF is included in the PRA because analysts have long recognized that many factors, such as degraded maintenance practices, which are not modeled explicitly in the PRA, can defeat redundancy and make failures of multiple redundant components more likely than would be the case if these factors were absent (4). These factors often reside in the organization in which the components are embedded, and are not intrinsic properties of the components themselves (5). However, CCF is currently modeled parametrically in PRA, and the CCF parameter values are estimated from a combination of past events, which had a variety of causes (2). Thus, the CCF parameter values are not specific to a single cause, such as poor maintenance practices. The aleatory model used for CCF is a straightforward extension of the binomial model used for failures on demand. In that model the unknown parameter is p, the probability of failure on demand. Note that p is not specific to any particular cause of failure; rather, it is a lumped parameter, encompassing all possible causes of failure. For CCF, the observed random variable is a vector of failure counts, $(n_1, n_2,..., n_m)$, where n_k is the observed number of events in which k components have failed, and m is the number of redundant components in the common-cause component group (CCCG). The aleatory model is the multinomial

[2] If the CCF event represents failure of all the components in the group, then the unconditional value cannot be retained for the case in which one component has failed because we now need the conditional probability that the remaining components in the group fail, given that one has already failed.

distribution, and the unknown parameter is also a vector whose components are usually denoted in PRA as (α_1, α_2,..., α_m). These are the so-called alpha-factors in the parameterization of the BPM used by the NRC, see (2) and (6). Like the analogous parameter p in the binomial distribution, the alpha-factors are lumped parameters, encompassing failure from a variety of causes rather than from any specific cause.

CCF data analysis is focused on estimating parameters in a parametric CCF model, such as alpha factors. These parameter estimates involve ratios of failure counts, such as the maximum likelihood estimate of α_2:

$$\hat{\alpha}_2 = \frac{n_2}{n_1 + n_2} \tag{1}$$

In this equation, and similar equations for other CCF parameters, n_k is the number of actual failures, having the same (typically proximate) cause, occurring within a time window determined by the PRA mission time, involving k components (k = 2 in this example) in a common cause component group (CCCG). Of course, there can be subjectivity in estimating the observed value of n_k, leading to a subjective distribution over the possible observed values (termed an impact vector), or what is used more commonly, an average over this distribution, which leads to fractional counts as the observed value. For more on data uncertainties in CCF parameter estimation, see (7) and (8). Regardless of such complications, n_k is an estimate of the actual failure count. Note, also, that estimates of alpha-factors are not developed for each proximate cause individually; failure counts from multiple proximate causes are combined together in the estimate.

Once alpha-factor estimates are in hand, estimates of the Q_ks in the BPM can be calculated. For the usual assumption of staggered testing, the following equation provides estimates of Q_k (6):

$$\hat{Q}_k^m = \frac{1}{\binom{m-1}{k-1}} \hat{\alpha}_k \hat{Q}_t \tag{2}$$

It's worth emphasizing again that in this equation, and other similar ones based on the BPM, the parameter estimates that appear in the equations are based on counting failures versus modeling causes of failures. Thus, the BPM is a data-driven approach to modelling CCF. As a result, estimates of CCF probabilities are determined only by component type and size (i.e., redundancy level) of the CCCG and causes of failure are lumped together in the parameter estimates. A further item worth noting is that current parametric models of CCF only address CCF within the boundaries of the CCCG. A model based more specifically on causes would not be constrained by the somewhat artificial CCCG boundaries, as a cause such as a procedural deficiency is not limited to redundant components in a CCCG.

3.1 Implications of Current CCF Modeling Approach for Event Assessment

Consider a CCCG consisting of two redundant emergency diesel generators (EDGs). During a surveillance test, one EDG fails to run. The failure mechanism is determined to be a broken exhaust valve insert. An investigation into this event determines that the root cause of failure was degraded maintenance practices. The risk evaluation of this event requires an estimate of the probability that the second EDG, which did not fail during the actual event, could have failed, conditional upon failure of the first EDG, with this failure conditional in turn upon degraded maintenance practices. Put another way, the risk assessment requires an estimate of a probability of failure for the second EDG that is conditioned upon a particular failure cause for the first EDG.

The current approach to modelling CCF, because it is not a causal model, cannot provide the estimate required for an event assessment; it can only provide an approximate answer, using the methods described in (1). One can condition upon the observed failure, and upon whether there is a potential for the cause of failure, which is unspecified in the BPM, to be shared with the redundant EDG.

For example, using the alpha-factor model for CCF, in a CCCG of size two, the unconditional failure probability (Q_g) for the CCCG is given as $\alpha_1^2 Q_t^2 + \alpha_2 Q_t$ (6). When one component fails, and there is potential for shared common cause, the conditional probability for failure of the CCCG becomes $\alpha_1^2 Q_t + \alpha_2 \approx \alpha_2$ (1). If the failure were judged to have no potential for shared common cause the conditional failure probability of the CCCG would be $\alpha_1 Q_t$ (1). Again, these are CCCG failure probabilities, conditional upon an observed failure; they are not, however, conditional upon the actual observed cause of the failure, which was degraded maintenance. Thus, because the CCF parameter estimates are not specific to a single cause, such as poor maintenance practices, these results are approximate answers to the question being posed by the event assessment. As a result, the conditional CCF probability, which is a function of the baseline CCF parameter values, may be either conservative or nonconservative, depending on the specific situation being modeled. However, while some causal factors, such as degraded maintenance practices in the example above, have the potential to cross system boundaries, the state of the practice in PRA does not include intersystem CCF, only CCF within a redundant group of components in a single system. From this perspective, the conditional CCF probability could be nonconservative.

4. PROPOSED CAUSAL FAILURE MODEL

To directly address the question being asked in event assessment, one needs a model that links equipment failures to their causes in a probabilistic fashion, allowing the analyst to estimate conditional probabilities of failure, given a particular cause such as degraded maintenance. A *Bayesian network* is one such model. A Bayesian network is a type of probabilistic graphical model, first developed by Judea Pearl as a model for probabilistic reasoning by intelligent systems (9). Specifically, a Bayesian network is a directed acyclic graph (DAG), in which nodes in the graph represent events of interest, and the edges connecting the nodes represent the directional influence of one event upon another. There are no loops in the graph, as an event cannot influence its own occurrence. For theoretical details on Bayesian networks see (10) and (11). For a more practical treatment, including applications, see (12) and (13). For more general types of probabilistic graphical models, including Bayesian networks, (14) is an excellent recent text.

Let us return now to our earlier example, in which an EDG failed as a result of a broken exhaust valve insert, with the root cause of the broken insert being degraded maintenance practices. The Bayesian network shown in Figure 1 represents this situation.[3] Failure of the EDG is a probabilistic event, which can be caused by any number of failure mechanisms, including a broken exhaust valve insert. Given that the exhaust valve insert has failed, the EDG will fail with probability one. The probability that the exhaust valve insert fails is influenced by the licensee's maintenance practices and other organizational factors. Overall, the network representation allows the joint probability of all three events to be factored into a series of conditional probabilities: P(EDG fails|broken exhaust valve insert) × P(broken exhaust valve insert|degraded maintenance) × P(degraded maintenance). The network can also be used to calculate the probability that the EDG fails, given that maintenance is degraded, which is the type of question that event assessment needs to be able to answer.

[3] The usual convention with Bayesian networks is for the child node to be at the bottom of the network and the parent to be at the top, so that inference is performed upwards in the network. We have chosen to reverse this visual convention here so that the networks more closely resemble fault trees, which are perhaps a more familiar model to most PRA analysts.

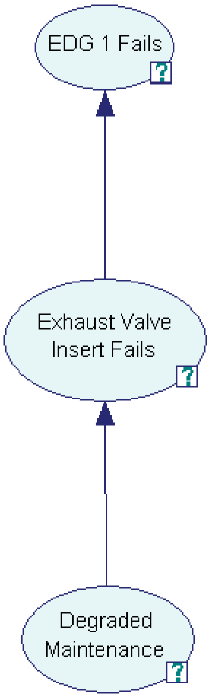

Figure 1 Bayesian network representing influence of root cause (degraded maintenance) on failure mechanism (failure of exhaust valve insert) and observed failure of EDG 1

Of course, in reality there are many failure mechanisms for an EDG, and multiple causes for these mechanisms. Some of the causes may be specific to one mechanism, or even specific to one EDG, while others can affect multiple EDGs via several different failure mechanisms. Figure 2 shows a slight extension to the very simple Bayesian network in Figure 1, which begins to represent the more general situation. In this model the failure of the exhaust valve insert is shown as a mechanism peculiar to EDG 1, perhaps because of a design difference. Other failure mechanisms are common to both EDGs. At the root cause level, there are causes peculiar to EDG 1, which impact the exhaust valve insert, and others, which can impact both EDGs via their influences on various failure mechanisms. Degraded maintenance practices, for example, can increase the probability of EDG 1 failing because of a broken exhaust valve insert, while at the same time increasing the probability of EDG 2 failing via some other mechanism that is not shared with EDG 1. This is a graphical illustration of the earlier point that CCF does not require identical failure mechanisms, only a shared failure cause.

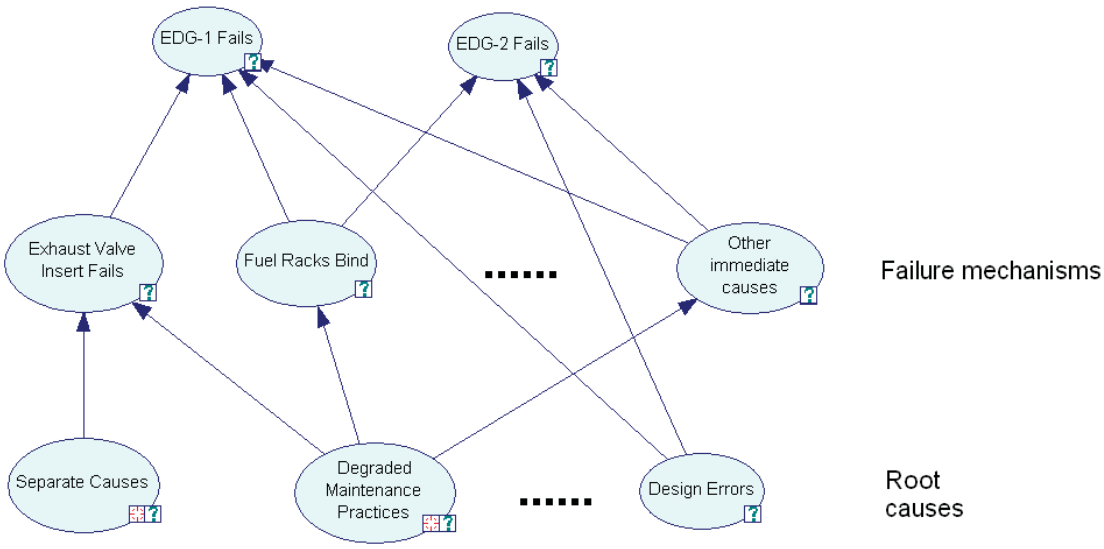

Figure 2 Bayesian network representing more general situation of multiple failure mechanisms and causes in a CCCG of two EDGs

It is easy to imagine the potential complexity of such a network in general, and so, as in all modeling, simplifying assumptions have to be made in order for the model to be tractable. We now turn to a simplification based on modeling proximate causes of failure only, rather than root causes and failure mechanisms.

4.1 Bayesian Network Based on Proximate Causes of Failure

The CCF data collection, classification, and coding project at the Idaho National Laboratory, sponsored by the U.S. NRC, makes use of proximate failure causes rather than root causes (15). These proximate causes are listed in Figure 3. Information is collected during this process that could potentially be used to estimate, with uncertainty of course, the probability of each proximate cause, and the conditional probability of component failure, given a particular proximate cause. So as a starting point for future development, one could begin with a Bayesian network that includes the proximate causes shown in Figure 3, but which excludes failure mechanisms and root causes in order to simplify the modeling. An example of such a network for an emergency power system (EPS) supplied by two EDGs is shown in Figure 4.

To further simplify the modeling, we will assume that each EDG can exist in one of two states: working and failed, and that each cause can be either present or absent. In general, it is straightforward to model multiple states in a Bayesian network, but we have chosen to simplify the network for the sake of illustration. To quantify the network, we need proximate cause probabilities and conditional probabilities of EDG failure, given each combination of proximate causes. With nine proximate causes, each of which can be present or absent, the conditional probability table for each EDG would have 2^9 entries. This illustrates a practical problem with discrete Bayesian networks: the size of the conditional probability table for a node in the network grows exponentially with the number of parents of that node. There have been various approaches developed for simplifying the structure of the conditional probability table, the most popular being the noisy-OR model and generalized linear models, see (11) and (14). We will use the noisy-OR model, in which each proximate cause is assumed to act independently of the others. With this model, we only have to specify the conditional probability of EDG failure for each proximate cause separately, making the complexity of the network linear in the number of parents.

Specifying the probabilities for each of the proximate causes, which are the parent nodes in the network, is perhaps feasible using the information collected by the CCF data project at INL, although in reality such estimates may need to rely upon additional information, such as might be available in a licensee's corrective action program database. It is feasible, however, to use the information in the INL CCF database to make ballpark estimates of the probability of EDG failure, conditional upon a particular proximate cause. Both sets of probability estimates are shown in Table 1. In this table, "other causes" represents those causes not modelled explicitly in the network, or what might loosely be termed "random" failures. This category is referred to as "leakage" in the noisy-OR model. We would like to caution that numbers, both those in Table 1 and elsewhere in this paper, are for illustration only; the values in Table 1 have not been derived rigorously from any underlying database.

Table 1 Illustrative probabilities to be used in Bayesian network example shown in Figure 4

Proximate cause	**Probability**	**P(EDG failure|cause)**
State of other component	1.3E-3	1.1E-3
Internal to component	1.5E-2	3.7E-3
Design error	5.9E-3	4.4E-3
Ambient environmental stress	5.1E-3	2.2E-3
Accidental action	1.4E-3	1.7E-3
Inadequate procedure	4.0E-3	3.3E-3
Design/construction error	6.3E-3	1.8E-3
Failure to follow procedure	3.5E-3	2.6E-3
Manufacturing error	4.9E-3	1.8E-3
Other causes	0.95	4.9E-3

FAILURE CAUSE

- Design/Construction/Manufacture
  - Design Error
  - Manufacturing Error
  - Installation/Construction Error
  - Design Modification Error
- Operational/Human Error
  - Accidental Action
  - Inadequate/Incorrect Procedure
  - Failure to Follow Procedure
  - Inadquate Training
  - Inadequate Maintenance
- External Environment
  - Fire/Smoke
  - Humidity/Moisture
  - High/Low Temperature
  - Electromagnetic Field
  - Radiation
  - Bio-organisms
  - Contamination/Dust/Dirt
  - Acts of Nature
    - Wind
    - Flood
    - Lightning
    - Snow/Ice
- Internal to Component
  - Normal Wear
  - Internal Environment
  - Early Failure
- State of Other Component
  - Supporting System
  - Inter-connection
- Unknown
- Other

Design/Construction/Installation/Manufacture Inadequacy. This category encompasses actions and decisions taken during design, manufacture, or installation of components both before and after the plant is operational.

Operational/Human Error (Plant Staff Error). Represents causes related to errors of omission and commission on the part of plant staff. An example is a failure to follow the correct procedure. This category includes accidental actions and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. It also includes ambiguity, incompleteness, or errors in procedures for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test, and calibration procedures.

External Environment. Represents causes related to a harsh external environment that is not within component design specifications. Specific mechanisms include electromagnetic interference, fire/ smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperatures, and acts of nature.

Internal to Component. This is associated with the malfunctioning of something internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the internal environment of a component. Specific mechanisms include erosion/ corrosion, vibration, internal contamination, fatigue, and wear-out/end of life.

State of Other Component. The component is functionally unavailable because a supporting component or system fails. For example, an air supply line to a valve breaks or a fuse in a control circuit blows. CCF events exclude those events that have dependencies that would reasonably be expected to be modeled in an individual plant examination or PRA.

Unknown. The category used when the cause of the component state cannot be identified.

Other. The category used when the cause cannot be attributed to any of the previous cause categories. This category is most frequently used for cases of set point drift.

Figure 3 Proximate causes and their descriptions

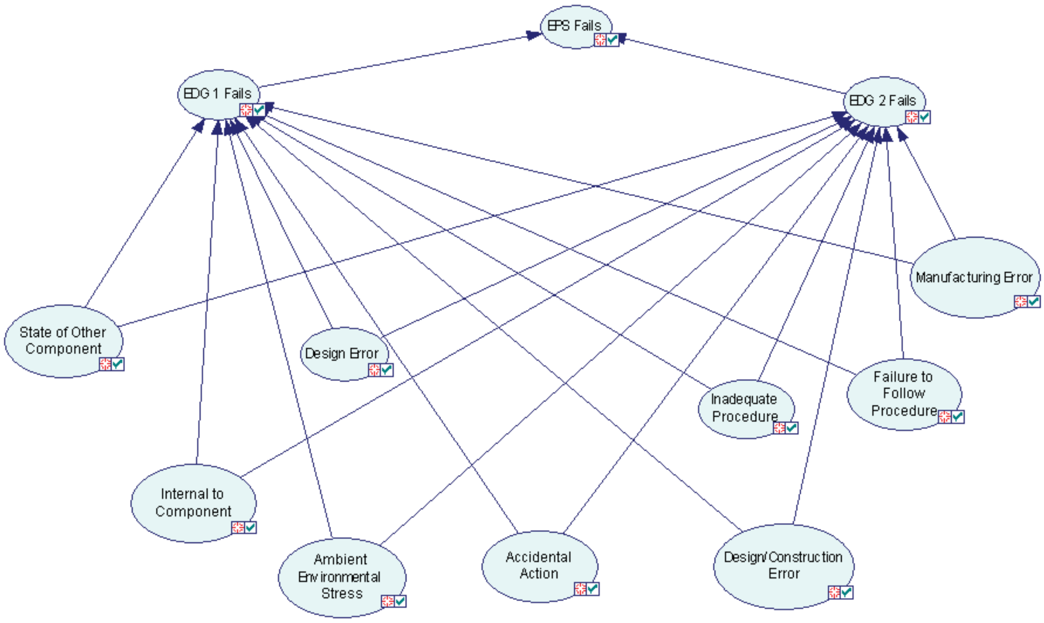

Figure 4 Bayesian network for two EDGs, showing influences of proximate causes

4.2 Illustrative Calculations for Event Assessment

The freely available GeNIe software package (16) was used for all of the following calculations using the probabilities in Table 1 with the Bayesian network shown in Figure 4. The nominal probability of failure for each EDG is 5.1E-3, which is the analog of Q_t in the BPM. If all of the explicit proximate causes are instantiated as absent in the network, and the network is updated, each EDG's conditional failure probability becomes 4.9E-3, the leakage probability for the noisy-OR gate. This is loosely analogous to Q_1 in the BPM, and represents "independent" failure of the EDG, which in this case is failure due to causes that are not modeled explicitly. Note that failure of EDG 2 in this network is conditionally independent of EDG 1, given the states of the proximate causes shown in the network; EDG 1 and EDG 2 are directionally separated, or *d-separated,* under this condition (10), (11), (12). Thus, once the probability of each EDG is updated to reflect the states of the proximate causes in the network, the resulting probabilities can be multiplied together to give the probability of EPS failure. In the "independent" case this probability is $(4.9E\text{-}3)^2 = 2.4E\text{-}5$

For event assessment, we can use the network to condition upon observed failures and causes. In the following examples, we will assume that EDG 1 has failed. It is straightforward to update the failure probability of EDG 2 to reflect the available observations and evidence as to causes. For example, if we can demonstrate that none of the proximate causes are present, then the conditional failure probability of EDG 2 becomes 4.9E-3, the "`independent" failure probability (Q_1) in the BPM. If EDG 1 failed and all of the proximate causes were present, the conditional failure probability of EDG 2 would become 0.03, which is equivalent to α_2, and represents failure caused by one of the present proximate causes in the noisy-OR model we are employing.

In between these two extremes are situations where one or more causes are present, or causes are present with some probability ("soft evidence" in the terminology of Bayesian networks). Table 2 shows the probability that EDG 2 fails, conditional upon the failure of EDG 1 and the presence of the indicated proximate cause. Soft evidence can be incorporated by inputting the probability that a particular proximate cause is present.

Table 2 Conditional probabilities of failure for EDG 2, given failure of EDG 1 and presence of indicated proximate cause

Proximate cause	P(EDG 2|EDG 1, proximate cause)
State of other component	6.2E-3
Internal to component	8.7E-3
Design error	9.5E-3
Ambient environmental stress	7.3E-3
Accidental action	6.8E-3
Inadequate procedure	8.4E-3
Design/construction error	6.9E-3
Failure to follow procedure	7.7E-3
Manufacturing error	6.9E-3

Recall that with the current approach to CCF modeling, which is based on the BPM, the conditional probability of failure of EDG 2 (using the alpha-factor parameterization) will be either α_2 or $\alpha_1 Q_t$., 0.03 or 4.9E-3, respectively, using the values in our illustrative example. Thus, a Bayesian network model, even a simple one that only models proximate causes, can provide more precise estimates of desired conditional probabilities for event assessment, as well as estimates that are conditional upon specific causes.

A Bayesian network can also be used to provide probabilistic insights into likely causes of failure. Using the values in Table 1, if EDG 1 fails, the most likely proximate cause is found to be "internal to component," with a conditional probability of 0.03. Thus, such models (although not the simple one used here as an example) have the potential to provide engineering insights into factors that can threaten designed-in redundancy. For too long, PRA has been telling engineers that CCF is important, but has not been able to tell them how to focus efforts at reducing CCF potential, because the CCF models are not causally based. Causal-based models such as Bayesian networks have the potential to help focus such efforts by providing engineers with cause-specific quantitative results.

5. SUMMARY

We have illustrated how the current CCF modeling approach, which is based on the BPM, is not able to directly answer the main question of interest for event assessment, namely what is the conditional probability of failure of remaining equipment, given observed equipment failures and associated causes? The current CCF modeling approach also cannot provide cause-specific quantitative insights to engineers to help them focus their efforts at reducing CCF. Furthermore, the current approach is constrained by the sometimes artificial boundaries of the CCCGs, and thus cannot model CCF of diverse equipment, or CCF across system boundaries, even though there are certainly causes of failure that do not respect such boundaries.

Causal-based modeling via Bayesian networks has the potential to overcome these limitations. However, such modeling raises several issues that will need further research and development before these models could be used as a part of common PRA practice. First, effort needs to be put into developing a rational hierarchy of failure mechanisms and causes to include in the model. This hierarchy would in turn drive data-collection efforts to support quantification of the model. The perspective provided by the list of proximate causes in Figure 3 is quite component-centered, and would perhaps need to be augmented with a more human-centered set of causes, more in line with the performance deficiencies typically observed in a plant or facility. Second, Bayesian network models have implications for PRA parameter estimation beyond CCF, and these implications may need to be explored. Lastly, there may also need to be changes to conventional PRA modeling using event trees and fault trees, with events in the event trees and fault trees perhaps being linked to a Bayesian network, a concept that has been explored in work done by the University of Maryland, via so-called hybrid causal logic model, in (17), (18), and (19).

Acknowledgements

The authors would like to acknowledge Prof. Ali Mosleh of the University of Maryland for pressing the viewpoint that CCF is often a reflection of issues outside the boundaries of the components affected, and for advocating the use of causal-based models in PRA. Even those of us (and there do not seem to be many) who have not studied formally with Ali, are nonetheless his students. We would also like to thank Dr. Nathan Siu of the NRC Office of Nuclear Regulatory Research for his time and support over many years.

A discussion of root cause analysis with Paul Bonnett of the NRC Office of Nuclear Reactor Regulation catalyzed the idea that perhaps the time has come for causal models, such as Bayesian networks.

References

1. Rasmuson, Dale M. and Kelly, Dana L., "Common-Cause Failure Analysis in Event Assessment," 2008, *Journal of Risk and Reliability*, Vol. 222, pp. 521-532.
2. Mosleh, A., et al., *Procedures for Treating Common-Cause Failures in Safety and Reliability Studies.* Washington, DC : U. S. Nuclear Regulatory Commission, 1988. NUREG/CR-4780.
3. Hulsmans, M., et al. , "Development of Guidelines for PSA-Based Event Analysis (PSAEA) in an International Project," Brussels, 2001. OECD/NEA/CSNI/WGOE+WGRISK workshop on Precursor Analysis.
4. American Nuclear Society and The Institute of Electrical and Electronics Engineers, *PRA Procedures Guide.* American Nuclear Society and The Institute of Electrical and Electronics Engineers. Washington, DC : U. S. Nuclear Regulatory Commission, 1983. NUREG/CR-2300.
5. Galan, S. F., Mosleh, A. and Izquierdo, J. M., Incorporating Organizational Factors into Probabilistic Safety Assessment of Nuclear Power Plants through Canonical Probabilistic Models," 2007, *Reliability Engineering and System Safety*, Vol. 92, pp. 1131-1138.
6. Mosleh, A., Rasmuson, D. M. and Marshall, F. M., *Guidelines on Modeling Common-Cause Failures in Risk Assessment.* Washington, DC : U. S. Nuclear Regulatory Commission, 1998. NUREG/CR-5485.
7. Siu, N. , "A Monte Carlo Method for Multiple Parameter Estimation in the Presence of Uncertain Data," 1990, *Reliability Engineering and System Safety*, Vol. 28, pp. 59-98.
8. Siu, Nathan O. and Kelly, Dana L., "Bayesian Parameter Estimation in Probabilistic Risk Assessment," 1998, *Reliability Engineering and System Safety*, pp. 89-116.
9. Pearl, J., *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference.* San Francisco : Morgan Kaufmann, 1988.
10. Pearl, Judea, *Causality: Models, Reasoning, and Inference.* Second Edition. Cambridge University Press, 2009.
11. Neapolitan, Richard E., *Learning Bayesian Networks.* Upper Saddle River, NJ : Prentice Hall, 2004.

12. Kjaerulff, Uffe and Madsen, Anders., *Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis.* Springer, 2008.
13. Pourret, Olivier, Naim, Patrick and Marcot, Bruce, *Bayesian Networks: A Practical Guide to Applications.* Wiley, 2008.
14. Koller, Daphne and Friedman, Nir, *Probabilistic Graphical Models: Principles and Techniques.* Cambridge, MA : MIT Press, 2009.
15. Wierman, T. E., Rasmuson, D. M. and Mosleh, A., *Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding.* Washington, DC : U. S. Nuclear Regulatory Commission, 2007. NUREG/CR-6268, Rev. 1.
16. Decisions Systems Laboratory, GeNIe. 2010. http://genie.sis.pitt.edu.
17. Groen, F. and Mosleh, A., "An Algorithm for the Quantification of Hybrid Causal Logic Models," New Orleans, 2006. Eigth International Conference on Probabilistic Safety Assessment and Management.
18. Mosleh, A., et al., "An Integrated Framework for Identification, Classification, and Assessment of Aviation System Hazards," Berlin, 2004 Seventh International Conference on Probabilistic Safety Assessment and Management.
19. Wang, C. and Mosleh, A., *Procedures for Qualitative and Quantitative Analysis of Risk Models Based on Hybrid Causal Logic Methodology.* Centre for Risk and Reliability, University of Maryland. College Park, 2005. Technical report.