Review of Current Problems in Dependent Failure Analysis

Stefan Hirschberg
ABB Atom AB, Västerås, Sweden

ABSTRACT

This paper summarizes experiences from treatment of dependent failures within Probabilistic Safety Assessments (PSAs) and parallel research projects carried out in Nordic countries. Examples of identified dependency related design deficiencies are given, followed by an outline of currently practised approaches to the treatment of different categories of dependencies. Some aspects of Common Cause Failure (CCF) analysis require continued development efforts. Identified problem areas involve choice of extension schemes in the context of CCF-data analysis, impact of defensive measures on estimation of CCF-parameters, and quantification of CCF-contributions in systems with non-standard levels of redundency.

BACKGROUND

Treatment of dependencies constitutes one of the central topics being addressed within current Nordic research projects in the area of Probabilistic Safety Assessment (PSA). In addition, Swedish and Finnish plant-specific PSAs have contributed to a methodological progress and constitute a basis for comparative studies. Such studies have shown to be extremely efficient as a tool for identification of weak points in the approaches applied. The ultimate goal is to improve consistency of the PSAs, eventually resolve matters of concern by reaching consensus (if possible) or by initiation of new research project (if necessary), and consequently reduce modeling and completeness uncertainties associated with treatment of dependencies.

The present paper provides a short summary of problems encountered in the context of dependent failure analysis. The focus is on the Nordic experiences. Common Cause Failures (CCFs), which usually are a subset of intercomponent dependencies, will be covered as a separate topic. Some of the aspects described in this report are covered in more detail in a recent survey concerning Nordic perspective on CCF-treatment (Hirschberg, 1988), in retrospective qualitative analysis of dependencies in Swedish PSAs (Hirschberg and Bengtz, 1987) and in sensitivity studies concerning CCF-contributions (Hirschberg et al, 1989a). The two last mentioned references contain also corresponding studies of human interactions.

TREATMENT OF DEPENDENCIES

Generally, treatment of dependencies is considered as a strong part of the Nordic PSAs. Characteristically, most of the findings in form of identified plant deficiencies, involve unintended dependencies. In several cases the insights have led to introduction of modifications at the plants and,

consequently, to significant safety improvements. Some examples originating from different plants follow below:

1. Some safety systems were connected to the same overcurrent protection switch as non-safety equipment (not qualified for accident environment) inside containment. Short-circuit (resulting from e.g. internal flooding) in the non-safety equipment might disable several safety systems.

2. Two of three water level sensors were fed from the same bus. Loss of this bus in connection with a single failure in the auxiliary feedwater system leads to loss of make-up water.

3. High temperature in only one train of shut-down secondary cooling system results in loss of shut-down cooling system function.

4. Inadvertent switch on of a breaker results in interconnection of two AC-buses and loss of power supply to equipment in several safety systems. The most serious consequence is that only auxiliary feedwater system is available for water make-up to the reactor.

Characteristically, no dependency related design deficiencies have been identified in PSAs for the latest generation of ABB Atom plants. This may be attributed to the basic design principles of four-divisional plants. The main features include complete separation of the redundant trains of the main safety functions and of the corresponding supporting functions, separation of operational and safety equipment from the physical and functional point of view, application of diversity for some critical safety functions (e.g. reactor shut-down, containment isolation), and absence of complicated links, interactions and interconnections between safety related functions (Hirschberg and Tirén, 1988).

The identified deficiencies described above belong to one of the following categories: functional dependencies, shared-equipment dependencies and equipment related Common Cause Initiators (CCIs). In some cases completeness in the treatment of these types of dependencies may be questioned and, in addition, not all discrepancies can be explained by design differences. In fact they originate from different perception of the design, different assumptions, errors in the analyses, or differences in scope, degree of detail and level of ambition. However, from the methodological point of view treatment of these three categories of dependencies does not represent a major problem. The approach used in Nordic countries is based on consequent application of the small event tree/large fault tree techniques, which takes care of functional and shared-equipment dependencies in a rather mechanistic way. Possible problems may originate from computerized Boolean reductions or/and from manual reductions of large logical models. Potential for such errors has been significantly reduced in view of progress made with respect to capacity of computer codes for fault tree analysis. From the point of view of quality assurance (which involves assurance of reasonable completeness) use of efficient computer codes for fault tree handling, as practised in Nordic countries, is also essential (e.g. Hirschberg and Knochenhauer, 1988).

Three types of CCIs are possible: external events, internal events causing severe environmental stresses and internal (equipment related) initiators which may involve functional dependencies not covered by the "generic" transient categories. The first mentioned two types of CCIs are not included in the current Swedish and Finnish base studies, although several analyses concerning e.g. internal flooding, fire, earthquake and air crash have been performed or are in progress for some plants. Also in this context the four-divisional separation constitutes an effective defensive measure against most low probability events with great damage potential. Modeling of external

events requires special techniques and deserves a separate review. Associated uncertainties are usually very large, particularly in the case of seismicanalysis which constitutes the most serious modeling challenge. It should be emphasized that loss of offsite power, sometimes regarded as an external CCI, is a transient covered by the conventional event tree/fault tree approach.

With respect to equipment related internal initiators a thorough well documented plant-specific study of support and control systems which may affect both normally operated systems as well as standby safety systems, is motivated. Examples of such systems include reactor water level measurement, electric power supply, pressurized gas systems and secondary cooling systems. Study of equipment related CCIs is rather straight-forward but time consuming. It ensures the completeness of a PSA, although in some cases a certain overlapping with the standard type of event tree/fault tree approach cannot be excluded.

Apparently, treatment of functional and shared-equipment dependencies, and equipment related CCIs does not represent a serious modeling problem, given a consequent approach. Practical limitations naturally exist in this context but with time, consistency and completeness of the present PSAs will certainly improve. Findings of a recently completed major Swedish research project aiming at comparison of available Swedish PSAs, with due regard to differences in methods, data and assumptions of different PSAs, constitute an important step towards this goal (Carlsson et al, 1988).

More serious modeling problems are usually encountered in the case of physical interactions, human interaction dependencies and residual common cause failures.

Generally, the failures which may be induced by the normal operational environment are part of the conventional analysis. This is due to the fact that:

1. The equipment is assumed to be qualified for such environment.
2. The failure rates used are based on operational experience and are assumed to reflect the actual operational environment.
3. Support functions such as component cooling are covered by the fault tree model and constitute a part of functional or shared-equipment dependencies.
4. Residual common cause failure contributions esssentially include intercomponent physical interaction dependencies not covered by the other approaches.

A documented, systematic and comprehensive study of physical interactions not covered by the points above should be a part of any PSA. This may involve dedicated qualitative or/and quantitative analyses of phenomena of special interest. In some cases physical interactions lead to requirements on operator actions which may be quite demanding. A typical example is back-flush operation identified as an important function for the early generations of ABB Atom's BWRs. Successful mitigation of large and medium LOCAs requires that the emergency core cooling suction pathways are maintained free from debris. Failure to initiate or failure to correctly carry out back-flush operation will lead to loss of core cooling and ultimately to core damage, unless timely recovery actions are taken.

Think-through and walk-through analyses are helpful tools for identification of potentially significant physical interactions. A systematic procedure for structured integration of engineering judgement in such analyses has been developed in one of the Swedish PSAs (Ericsson and Hirschberg, 1984). This

facilitates to examine impact of some environmental factors (grit, humidity, corrosion and other chemical reactions, vibration, temperature and thermal stress, radiation) and gives a rough and quick overview of facility-related events causing severe environmental stresses (fire, energy release through explosion, water hammer, structural failure, flow blockage, leakage, electrical interference; some of these phenomena may belong to CCI-category). The procedure is most efficient for plants with relatively low degree of separation and with substantial operating experience.

Of particular interest are analyses of dynamic effects such as: pipe whips, jets, secondary missiles and pool-dynamic loads, which may follow upon a pipe break within the reactor containment. Studies assessing unavailability contributions from dynamic effects for systems mitigating the consequences of internal pipe breaks are essential, but frequently lacking. In one of the Swedish PSAs dynamic effects contribute significantly to unavailability of pressure relief, emergency core cooling and auxiliary feedwater system, given large or medium LOCA. Analysis of dynamic effects is a relatively complex task which may be facilitated by introduction of "rules of thumb" based on engineering judgement.

Four types of human interaction with some potential for dependencies have been treated in most of the Swedish PSAs:

1) Maintenance and test outages that may increase system unavailability.
2) Manual actuation signals to systems and equipment in case of failure of automatic signals, and local manual actuation of equipment.
3) Manual initiation of safety systems, involving decision and e.g. proper aligment of valves.
4) Misconfiguration of components in redundant trains.

Some simple rules may be applied when modeling human interaction dependencies. Thus, test and maintenance activities should be represented in the fault trees. Simultaneous multiple failures due to maintenance outages are usually covered by CCF-contributions. Manual actuation of redundant components in different trains is treated as a common event. The essential operator actions are modeled either in the event trees or in the fault trees. Operator actions considered as critical for progagation of accident sequences, i.e. operator actions which have impact on functional intersystem dependencies, are in the small event tree/large fault tree approach explicitly represented in event trees. Naturally, failure to observe an indication or to diagnose correctly the nature of the event, is equivalent to no responses being carried out. Systematic misconfiguration of redundant components and systematic calibration errors may be modeled explicitly or the corresponding unavailability contributions may be covered by residual CCF-contributions. Assumed independency between human interactions concerning redundant trains should at least be supported by qualitative arguments (e.g. staggered testing of different subs, automatic restoration of components to original position after test, favourable conditions for recovery) and/or by situation-specific analyses.

Difficulties encountered in treatment of errors of commission, which obviously may introduce complex dependencies, call for further research. Confusion matrix approach has recently been applied in this context in one of the Finnish PSAs (Vuorio and Vaurio, 1987).

TREATMENT OF COMMON CAUSE FAILURES

Identification

The Nordic CCF-data Benchmark Exercise concerning motor-operated valves

(Hirschberg, ed., 1987) has demonstrated that basic CCF-identification can be reasonably performed based on failure reports from the Scandinavian Nuclear Power Reliability Data System and on the Swedish Licensee Event Reports (LERs). The methods used for CCF-identification are straight-forward and require as a minimum information failure decriptions containing failure mode, criticality and time of detection. However, availability of much more detailed background material including data on type of valve, physical location, manufacturers, maintenance policies etc, would decrease the impact of subjective judgement. Use of computers to aid in searching, sorting and generally reorganizing failure reports has been recommended.

The results of identification are directly depedendent on intended scope (e.g. limitation to intrasystem CCFs), on choice of main identification factors (e.g. length of critical time period) and on assumed bounding conditions (e.g. definition and treatment of non-critical failures). Some desirable information is not available when the original failure reports are written; failure cause specification - if it is ever available - is often delayed. The uncertainty concerning the quality of reports originating from the overhaul period is a serious drawback; any improvement of these reports would be most welcome. In addition, when carrying out the screening procedures attention should be given to the types of tests carried out during normal operation and during overhaul, and their capacity of revealing critical failures. Treatment of multiple failure events detected during the overhaul period proved to be one of the most controversial and unresolved issues in the Benchmark Exercise.

Merits of classification systems as a supporting tool for CCF-identification (see e.g. Mosleh et al, 1988) depend on the structure of failure reports. The Swedish and Finnish failure reporting systems concern only components and supply in the first place information about failure modes. The use of classification systems which are cause-oriented is, consequently, of limited value in this case.

Quantification Methods, Data and Uncertainties

Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987) focused on impact of different assumptions involved in data treatment on the estimated CCF-contributions. Of primary interest in this context are such factors as: CCF-definition, use of application- and design-oriented screening, use of extension schemes and weighting of potential CCFs. With few exceptions most of the discrepancies in the estimates of CCF-contributions could be attributed to these factors rather than to the choice of a particular estimation method. These findings are consistent with the results of a parallel CCF Reliability Benchmark Exercise coordinated by Ispra Establishment (Poucet et al, 1987).

Based on the results of Benchmark Exercises the recommended approach to quantification, in applications where in-depth studies of raw data are possible, would employ direct assessment of CCF-contributions. Use of simple parametric methods is still of major interest when good quality single failure probability data (e.g. Swedish Reliability Data Book, Bento et al, 1985) are available. Parametric models are also suitable for checking the impact of modified assumptions and for performance of sensitivity studies, and may represent the only practically available option when the data are lacking or are scarce. As a follow-up to the Nordic CCF-data Benchmark Exercise a survey of various CCF-quantification models has been made, including relations between the parameters (Pörn, 1988).

The impact on PSA-results of different approaches to quantification of CCF-contributions has been studied by means of comprehensive sensitivity analyses (Hirschberg et al, 1989a) and uncertainty analyses (Hirschberg et al, 1989b). The sensitivity studies concern both data and methodological aspects. Examples

of issues addressed involve: impact of lower failure multiplicities, generation of plant-specific CCF-parameters for motor-operated valves using identical assumptions concerning treatment of CCF-data, use of alternative approaches to mapping up and mapping down of impact vectors, comparison of Multiple Greek Letter (MGL) method (Fleming and Kalinowski, 1983) and alpha-factor method (Mosleh and Siu, 1987), systematic misconfigurations of redundant components, impact of practical arrangements of tests of redundant components and of policy applied with respect to identification of CCF-events by testing on the choice of suitable CCF-model, CCF-contributions in systems with non-standard level of redundancy, impact of defensive measures on estimation of CCF-parameters and importance of "state-of-knowledge" dependencies. Below follow some fragmentary examples of insights from these studies. The purpose is to illustrate problems encountered; for a more detailed account we refer to the original references (Hirschberg et al, 1989a, 1989b). It should be noted that the conclusions drawn for Swedish PSAs are not necessarily generally valid.

1. Given a reasonable choice of higher order CCF-parameters the contributions to core damage frequency from lower failure multiplicities are small for plants with high level of redundancy. Use of models which properly take into account all relevant failure multiplicites is, however, recommended.

2. Use of a consistent approach to quantification of CCF-contributions in different PSAs has a strong impact on the results; in one of the analysed cases the total core damage frequency increased by 78 % when the new plant-specific CCF-parameters for motor-operated valves were applied. The results are also sensitive to the choice of schemes for mapping up and mapping down of impact vectors (difference of 21 % in the above mentioned case). A recent survey of available CCF-data (Mankamo, 1989), carried out within one of the Finnish PSAs, clearly illustrates the importance of analysis assumptions and of plant-specific features.

3. The alpha-factor method (Mosleh and Siu, 1987) provides a more correct representation of statistical uncertainties than the MGL-model (Fleming and Kalinowski, 1983). In one of the analysed cases the MGL-based estimates of the mean and 90 % confidence bound for probability of quadruple failure of a set of redundant valves, represent an underestimation by a factor of 3.

4. Application of Multiple-Sequential Failure (MSF) model (Samanta et al, 1985) shows that the impact of postulated systematic misconfiguration of redundant components is small in case of latest generation of Swedish BWRs. For elder plants the impact is more pronounced and becomes quite substantial for dependency factors of the order of 0.1.

5. The practical arrangement of tests of redundant components and policy applied with respect to identification of CCF-events by testing has impact on the choice of suitable CCF-model (Parry, 1984). Use of MGL- and alpha-factor methods is consistent with the origin of Swedish CCF-data, i.e. the presently available Swedish CCF-experience originates almost exclusively from plants where redundant components are tested simultaneously.

6. Presently available methods and data are not adequate for proper modeling of CCF-contributions in systems with non-standard level of redundancy. Of primary interest for ABB Atom's BWRs are pressure relief valves (e.g. 13-out-of-16 failure criterion), control rods, fine motion-drives, scram modules and frequency converters. Incorrect extrapolations of simple parametric methods to such redundancies have been observed in several cases. Application of an extended Common Load (CL) model (Mankamo and Kosonen, 1988) has been recently proposed as a solution of this problem.

The model is defined in terms of subgroup failure probabilities, which means that simple, exact and consistent expressions for different success criteria can be derived. The underlying physical stress-strengh model provides understandable interpretations for the model parameters. Future plans involve detailed data analyses and performance of sensitivity studies based on applications of extended alpha-factor and CL-methods. It must be emphasized that the initial handling of data may in practice have a much stronger impact on the end result than the choice of quantification model.

7. One of the main problems in the current state of CCF-analysis is lack of a systematic approach to reflect inherent defensive measures against CCFs when generating CCF-parameters. Use of partial beta-factor method (Johnston, 1987) has been proposed as a solution of this problem. Some qualitative guidelines have been recently developed for defensive strategies in order to reduce susceptibility to CCFs (Crellin et al, 1988). In Swedish comparative studies (Carlsson et al, 1988) aiming at generation of reference plant models characterized by consistent treatment of central modeling topics (e.g. accident sequence modeling, data, human interactions, dependencies) recommended CCF-parameters have been assigned for different component groups taking into consideration the degree of physical and functional separation at different plants. Future efforts will be directed towards generation of the Swedish CCF-data book, which should reflect these aspects. The intended approach is in line with current NRC-research centered on a cause-coupling-defense methodology (Parry et al, 1989) and will also benefit from the recently formulated procedural framework for CCF-analysis (Mosleh et al, 1988).

8. Current praxis with respect to boundary conditions of CCF-analysis means that residual CCF-contributions are usually limited to intrasystem dependencies. Thus, for practical reasons CCFs are seldom postulated for identical components belonging to different redundant systems. As a consequence of this approach the estimated impact of CCFs on overall level of safety does not fairly reflect advantages of high level of redundancy.

9. The parametric uncertainties associated with CCF-estimates corresponding to high failure multiplicities are large. However, as demonstrated in the Nordic reference study on uncertainty and sensitivity analysis (Hirschberg et al, 1989b) the estimates of the overall uncertainty interval may vary significantly depending on the choice of screening assumptions, quantification methods and probability distributions. Thus, the 90 % confidence bound for a quadruple CCF covers between one and three decades in the analyses carried out by different groups. Notable is also the decisive importance of "state-of-knowledge" dependences, which is not reflected in PSAs limited to point estimates.

CONCLUSIONS

The present review reflects some problems characteristic of dependent failure analyses being carried out in Nordic countries. Treatment of functional and shared-equipment dependencies and equipment related Common Cause Initiators is well-established, although completeness and consistency of analyses can be improved. Some simple rules exist with regard to modeling of physical interactions and human interaction dependencies, but guidance is needed to establish more systematic approaches to e.g. analysis of dynamic effects and errors of commission.

Problem areas, which require continued development efforts have also been pointed out within Common Cause Failure analysis. In this context improvements concerning proper consideration of defensive measures in the process of estimation of CCF-parameters and more credible quantification of

CCF-contributions in systems with non-standard levels of redundancy, are regarded as the most urgent.

REFERENCES

Bento, J.P., ed. (1985). Reliability Data Book for Components in Swedish Nuclear Power Plants. RKS 85-25.

Carlsson, L., Hirschberg, S., Johanson, G., Pörn, K. and Wilson, D. (1988). Can Different PSAs Be Compared and Used in Nationwide Decision Making ? Status of and Experience from the Swedish ASAR-program. OECD/CSNI Workshop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Crellin, G.L., Mott, J.E. and Smith, A.M. (1988). Defensive Strategies for Reducing Susceptibility to Common-Cause Failures. Volume 1: Defensive Strategies. EPRI NP-5777.

Ericsson, G. and Hirschberg, S. (1984). Treatment of Common Cause Failures in Barsebäck 1 Safety Study. Fifth International Meeting on Thermal Nuclear Reactor Safety, Karlsruhe, Federal Republic of Germany, September 9-13, 1984.

Fleming, K.N. and Kalinowski, A.M. (1983). An extension of the Beta Factor Method to Systems with High Levels of Redundancy. PLG-0289.

Hirschberg, S. (1988). Treatment of Comon Cause Failures. The Nordic Perspective. Contribution to the Proceedings of the Advanced Seminar on Common Cause Failure Analysis, Ispra, Italy, November 16-20, 1987.

Hirschberg, S., ed. (1987). NKA-project Risk Analysis (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report, RAS-470(86)14 (ABB Atom Report RPA 86-241).

Hirschberg, S. and Bengtz, M. (1987). Retrospective Analysis of Dependencies and Human Interactions in Swedish PSA Studies. Society of Reliability Engineers Symposium 1987, Helsingør, Denmark, October 5-7, 1987.

Hirschberg, S., Björe, S. and Jacobsson, P. (1989a). Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989.

Hirschberg, S., Jacobsson, P., Pulkkinen, U. and Pörn, K. (1989b). Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989.

Hirschberg, S. and Knochenhauer, M. (1988). SUPER-NET, An Efficient Tool for the Living PSA Concept. OECD/CSNI Workshop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Hirschberg, S. and Tirén, I. (1988). Design-related Defensive Measures against Dependent Failures. ABB Atom's Approach. Contribution to the Proceedings of the Advanced Seminar on Common Cause Failure Analysis, Ispra, Italy, November 16-20, 1987.

Johnston, B.D. (1987). A Structured Procedure for Dependent Failure Analysis (DFA). Reliability Engineering, Vol. 19, pp. 125-136.

Mankamo, T. (1989). Private communication.

Mankamo, T. and Kosonen, M. (1988). Dependent Failure Modeling in Highly Redundant Structures. Society of Reliability Engineers Symposium 1988, Västerås, Sweden, October 10-12, 1988.

Mosleh, A., Fleming, K.N., Parry, G.W., Paula, H.M., Worledge, D.H. and Rasmuson, D.M. (1988). Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Procedural Framework and Examples. NUREG/CR-4780, EPRI NP-5613.

Mosleh, A. and Siu, N.O. (1987). A Multi-parameter Common Cause Failure Model. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Parry, G.W. (1984). Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty. 1984 Annual Meeting of the Society for Risk Analysis, Knoxville, Tenn., September 30 - October 3, 1984.

Parry, G.W., Paula, H.M., Mitchell, D.B., Whitehead, D.W. and Rasmuson, D.M. (1989). A Cause-Coupling-Defense Approach to Common-Cause Failures. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989.

Poucet, A., Amendola, A. and Cacciabue, P.C. (1987). CCF-RBE Common Cause Failure Reliability Benchmark Exercise. Ispra Establishment, EUR 11054 EN.

Pörn, K. (1988). Some Comments on CCF-quantification. The Experience from the Nordic Benchmark. Contribution to the Proceedings of the Advanced Seminar on Common Cause Failure Analysis, Ispra, Italy, November 16-20, 1987.

Samanta, P.K., O'Brien, J.N. and Morrison, H.W. (1985). Multiple-Sequential Failure Model. Evaluation of and Procedures for Human Error Dependency. NUREG/CR-3837.

Vuori, U.M. and Vaurio, J.K. (1987). Advanced Human Reliability Analysis Methodology and Applications. Probabilistic Safety Assessment and Risk Management PSA '87, Zurich, Switzerland, August 30 - September 4, 1987.

ACKNOWLEDGEMENTS

This work has been supported by the Swedish Nuclear Power Inspectorate.