Reliability Analysis Based on Multilevel Flow Models

Jan Eric Larsson, Fredrik Dahlstrand, Bengt Öhman, Jan Tuszynski

GoalArt, Tunavägen 39C, 223 63 Lund, Sweden
E-mail: info@goalart.com, URL: www.goalart.com

Abstract

System reliability and availability can be calculated using a multilevel flow model to describe the causal dependencies of the target system. Compared to established techniques, this allows for a method, which is less error prone, more efficient, and allows for multiple fault situations. The largest practical advantage of the method is that it is much easier to construct an MFM model of a system than to perform a reliability analysis by block diagrams or fault trees. The method allows on-line reliability analysis in real-time.

INTRODUCTION

Availability analysis, reliability analysis, and other related methods provide a way of estimating the availability, reliability, etc., of a process, that is, to give a measure on the probability that the process or its subsystems will actually work and not be broken or unavailable at some time or time interval in the future. This gives a general feeling for how "safe" and "trustworthy" a process is.

These methods pose two practical problems, however. First, good values of component reliabilities are needed as inputs to the calculations. Secondly, the work effort going from process knowledge, via causal mapping of some kind, to the probability calculations can be very large.

This paper presents a new method for calculation of availability or reliability. It uses *multilevel flow models* (MFM) as the basis for the causal analysis. In this way, much of the work effort needed is circumvented. The effort is instead to build an MFM model of the process. Since MFM models are useful for other algorithms too, work costs can be further reduced.

The developed method even allows calculation of reliability on-line, so that the results can be used as high-level sensors during process operation.

SYSTEM RELIABILITY ANALYSIS

System reliability analysis is the area in reliability engineering concerned with computing system reliability characteristics from the reliability characteristics of single components. A target system, for example an industrial process, is composed of a large number of components (items of physical equipment), which form subsystems. Subsystems form new, larger subsystems, and eventually the entire target system. Each component and subsystem can have one or several functions to fulfill, and these functions achieve the goals of the target system, (in other literature, however, the term function is often used to mean a combination of both function and goal).

Reliability analysis is performed so that single components and/or subsystems are assigned a measure describing the probability that the item is in working order and able to fulfill its functions and goals. Through use of a description of causal dependencies between components and subsystems, it is possible to calculate the conditional probabilities that top-level functions and goals are fulfilled.

Reliability analysis can be used both to analyze the general safety properties of the target system during the design phase, and on-line to analyze the effects of failure of redundant systems.

Several different probability measures are possible to use:

- *Reliability* is the probability that the system has experienced no failure at some specified time in the future, while *unreliability* is the opposite probability, that is, 1 – reliability.
- *Availability* is the probability that a system failure does not exist at a certain time in the future, while *unavailability* is 1 – availability. The difference between this and reliability is that a measure of failure, downtime, and repair is included, while reliability assumes no failure at all.
- *Rate of failure* is the expected number of failures per time unit at a time t. The expected number of failures during a time interval is given by the integral over time of the rate of failure.
- *Failure rate* is the probability of failure at time t, given no failures before t.

Most of these measures are based on probabilities and are treated in a similar way in the reliability calculations. It is often trivial to change one measure for another in a specific method. For more on these measures, see for example Fussell (1975).

REPRESENTATION OF SYSTEM CAUSALITY

In order to calculate top-level reliability from the reliability measures of single components and subsystem, the causality between parts of the system must be known and described. Two different methods have been used regularly for this:

- Reliability block diagrams
- Fault trees

Both these representations allow the calculations of *minimal cut sets*, that is, the failure combinations, which will cause the system to fail. These in turn can be represented as a (large) matrix, and the calculations can be performed as a vector and matrix multiplication.

The main drawbacks with these representations are:

- Reliability block diagrams and fault trees describe failure causality but have no direct relationship to the structure of the target system. Thus, they have to be built from scratch, and cannot be synthesized from other descriptions of the system.
- Reliability block diagrams and fault trees potentially cover a very large number of minimal cut sets. A fault tree composed of some 20 logic gates can represent millions of system failure modes. All these failure modes should be taken into consideration when building the block diagrams or fault trees, or errors may occur in the representation.
- The result of a reliability analysis cannot relate back to the causal path taken by failures in the physical process.
- The methods assume that only one minimal cut set (that is, root cause fault) occurs at a certain time, and that the input probabilities of each component are independent.

For the reasons above, a system for reliability analysis based on these "classical" techniques cannot be complete and there is no guarantee that it will have a correct description of the target system's causality. In fact, the probability is overwhelming that there will be errors in the description. Finally, there is always a risk that the independence assumptions made are not valid, and then the results are not necessarily valid. For more on calculation of reliability measures using fault trees, see for example Inoue and Henley (1975).

All these drawbacks can be solved, though, with the introduction of multilevel flow models as the representation of system causality.

MULTILEVEL FLOW MODELS

Multilevel flow models (MFM) are graphical models of goals and functions of technical systems. The goals describe the purposes of a system or subsystem, and the functions describe the capabilities of the system in terms of flows of mass, energy, and information. MFM also describes the relations between the goals and the functions that achieve those goals, and between functions and the subgoals, which provide conditions for these functions. MFM was invented by Morten Lind at the Technical University of Denmark, see Lind (1990 a). Several new algorithms and implementations were contributed by Jan Eric Larsson at Lund Institute of Technology, see Larsson (1992, 1994, 1996, 2002).

MFM provides a good basis for diagnostic algorithms. The work of Larsson (1996) describes three algorithms based on MFM: measurement validation, alarm analysis, and fault diagnosis. Other algorithms have been developed later, such as fuzzy alarm analysis, see Dahlstrand (1998),

Dahlstrand (2000), Larsson and Dahlstrand (1998), failure mode analysis, see Öhman (1999, 2001), and sensor fault detection, see Öhman (2001, 2002).

AN EXAMPLE OF AN MFM MODEL

MFM has been thoroughly explained in Lind (1990 a) and Larsson (1992, 1996). Here a small example will be given, to show the basics of MFM modeling. We will use a part of the main circulation system of a nuclear power plant. A much simplified process graph, from an example in the master's project Ingström (1998), is shown in Figure 1.

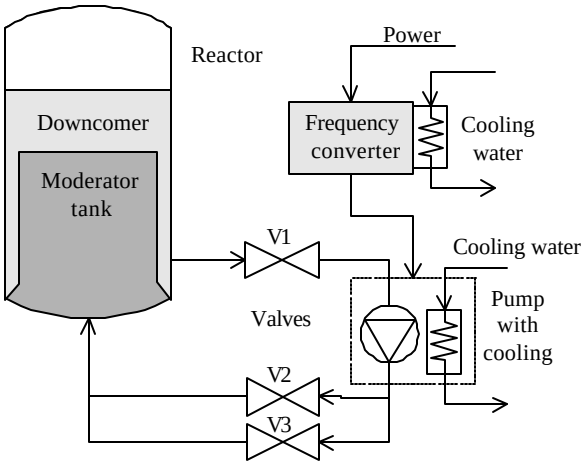

Figure 1. A process graph of the main recirculation system of a nuclear power plant.

In this system, reactor tank water flows from the downcomer, via the valve V1, to the pump. After the pump, the water flows through the two parallel valves V2 and V3, back to the moderator tank. The pump is cooled by water. There is also a need for a frequency converter for the power to the pump, since the pump is frequency-controlled. Finally, the frequency converter must also be cooled. The purpose of the main water circulation is to control (moderate) the flow of neutrons in the reactor, and to cool it at the same time.

The goals of this simple system are: "maintain desired water flow through the moderator tank," "cool the pump," "provide electrical energy with the correct frequency," and "cool the frequency transformer."

The functions of the system are, among others, the downcomer's ability to provide water, the pump's ability to transport water, and the heat exchanger's ability to transport heat. An MFM model of this system is shown in Figure 2.

In the MFM model, there are four flows. The flow network M1 describes the water flow from the downcomer to the moderator tank. The network E1 describes the transport of thermal energy from the pump to the cooling water. The network E2 describes the flow of electrical energy from the supply, via the frequency transformer, to the pump. Finally, the network E3 describes the

flow of thermal energy from the frequency transformer to the cooling water. Thus, M1 is a model of a mass flow, and E1 to E3 are models of energy flows. In the network M1 the functions are, from left to right: 1) a source of water, realized by the downcomer; 2) a transport, realized by the valve V1; 3) a balance, realized by the pipe between V1 and the pump; 4) another transport, realized by the pump; 5) another balance, realized by the forking pipe between the pump and the two parallel valves V2 and V3; 6) two transports, realized by the valves V2 and V3; 7) a balance, realized by the pipe sections between V2 and V3, and the moderator tank; 8) a transport, realized by the pipe that runs into the moderator tank; and finally, 9) a sink, realized by the moderator tank. The networks E1 to E3 contain energy flow functions describing the flows of electrical and thermal energy.

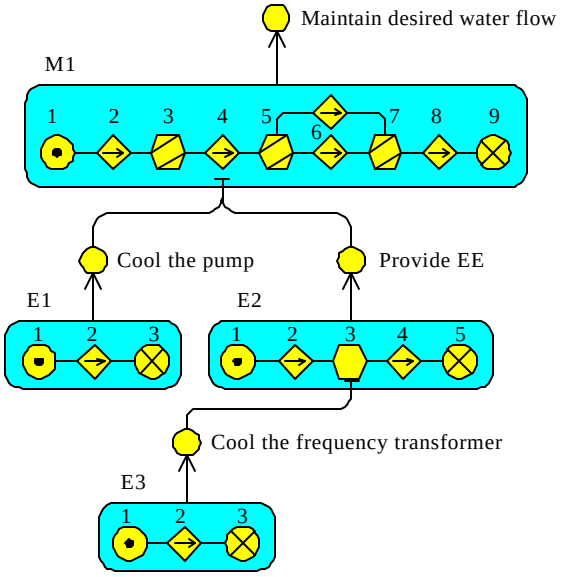

Figure 2. An MFM model of the main recirculation system.

It should be noted that MFM describes how different flows enable each other. In the simple example in Figure 2, it can be seen that the cooling water flow E3 is necessary for the proper function of the frequency converter, and that the cooling water flow E1 and the electrical flow E2 are needed to keep the main water flow operating.

PROPAGATION OF PROBABILITY MEASURES IN MFM

MFM can be used to calculate reliability measures for all goals and functions of a system. An MFM model could easily be turned into a matrix describing causality, as is usual when using fault trees, but the calculations can be performed directly in the MFM model data structures.

The steps of the algorithm are as follows:

- Some of the functions are input nodes. These receive pre-calculated reliability values depending on the state of the corresponding components. If the functions are not available in

the current state, they receive the reliability (or availability) zero. Unconnected functions receive a default reliability of unity.

- Each network receives a reliability value, which is the product of the reliabilities of the functions it comprises.

$$R(N) = \Pi\ R(F_i)$$

- Each goal receives a reliability value, which is the product of the connected network and manager.

$$R(G) = R(N) * R(M)$$

If there is no manager, then R(M) = 1.

- Each redundancy goal receives a reliability value, which is the probability that at least one of needed number of connected networks is working. Redundancy goals were introduced in Ingström (1998).

$$R(GR) = 1 - \Pi\ (1 - R(N_i)$$

Similar calculations apply for "n of m."

- Each condition receives a reliability value, which is equal to that of the goal it is connected to.
- Each function with conditions, receives a reliability value, which is the product of its input reliability and the product of the reliabilities of the connected conditions.

$$R(F) = R(F_{in})\ \Pi\ R(C_i)$$

When these calculations have been propagated through the MFM model, each MFM object, and thereby each function and goal, will have a known reliability, including all top-level goals. It is also straightforward to add new calculation rules if new MFM concepts are introduced.

The algorithm recognizes loops in the means-end dimension, that is, where there are circular dependencies. In such cases, the loops are broken and the calculations amended afterwards to a safe value.

ADVANTAGES OF THE METHOD

Using MFM as a basis for reliability has a number of clear advantages:

- MFM models describe physical flows of mass, energy, and information, and relate directly to physical parts of the target system.
- MFM models are easily built, and mean something to the designers and operators.

- The calculations of reliability propagate in a fixed graph of limited size, giving a linear or sub-linear complexity.

In short, when building a fault tree for a system with N inputs, in the order of 2^N possibilities must considered, while for an MFM model, some 5*N objects must be selected. In practice, the number N may be in the order of 100 to 10 000. This allows a complete and well-verified MFM description, which cannot be achieved with the other methods.

Another advantage of the method is that it can handle multiple fault situations without complications.

AN INPUT RELIABILITY ESTIMATOR

So far, all methods use independent failure probabilities as inputs to each component or function. This means that these probabilities must be known in advance. The normal assumption is that the data to be used are design data from manufacturers, etc. This disallows the use of data that can be estimated during operation of the target system.

The *input reliability estimator* is based on MFM and can estimate reliability and availability during plant operation. The method works as follows:

- Conditional reliability or availability is estimated for each component connected to an MFM function. This can be done with several standard methods. For example, availability is simply working time divided by total time for a certain time interval. However, such estimates provide information on the conditional probabilities only (where a failure can be cause by a root failure in a connected component), not the independent probability for each component.
- By using alarm analysis based on MFM and considering primary failures only, the statistics will find the independent failure probabilities and be able to discard the conditional components in the statistics.

In this way, the input reliability estimator can be used to gather the basic reliability information during operation of the target system. It should be noted though, that this demands that enough failures happen before the statistics will be reliable. For unusual failures, the only solution is to use a priori known design information.

OTHER ALGORITHMS BASED ON MFM

Over the years, Larsson and his research group have developed several algorithms based on MFM and related to process safety analysis. The algorithms are:

Failure Mode Analysis
This algorithm calculates future consequences of actions, given a process state and one or several proposed faults or actions. In this way, it is an on-line planning support tool.

Verification of Redundancy
This algorithm checks whether redundant subsystems rely on common support systems. If so, true redundancy may be compromised and the process design is faulty.

Verification of Safety Classification
This algorithm checks whether classified subsystems rely on non-classified support systems. If so, safety may be compromised.

All the algorithms above use the same MFM model, that is, the MFM model is the "knowledge database" for the algorithms. This has some obvious advantages:

- A single modeling effort will provide the database needed for a whole set of different diagnostic tasks.
- The same MFM model can be used throughout the life cycle of the process, for different design and supervision tasks.

RELATED WORK

The main contributions to MFM have been made by Morten Lind and his group. Lind (1990 a, 1994) describes the basics of MFM, while Lind (1990 b) contains an early suggestion for a diagnostic system. Lind has also treated real-time diagnosis, Lind (1990 c), and design of operator interfaces, Lind (1989).

MFM has also been used in nuclear safety research, De et al. (1982) and Businaro et al. (1985), in operator interfaces for fault diagnosis, Duncan and Prætorius (1989), for constructing COGSYS diagnostic systems, Sassen (1993), for fault diagnosis in process industry, Walseth (1993), and in intelligent man-machine systems for nuclear plants, Monta et al. (1991).

Larsson has used MFM in monitoring and diagnosis for intensive-care units, Larsson and Hayes-Roth (1998), Larsson, et al. (1997 a, b).

MFM is the main basis for the startup company GoalArt, which works with diagnostics for various branches of industry, for example nuclear power generation, see Larsson (2000).

MFM can be compared to other modeling and diagnosis methodologies, such as rule-based expert systems, fuzzy logic, qualitative physics based on Reiter's algorithm, Hamscher et al. (1992), Reiter (1987), Greiner et al. (1989), classical statistical methods, methods from control theory, Frank (1996), and neural networks. In comparison to expert systems and fuzzy logic, MFM imposes a deep model structure of means and ends, as opposed to a shallow rule-based representation. It differs from qualitative physics in that it explicitly represents goals and

functions, avoids general logic, and is computationally more efficient, while qualitative physics has been geared towards diagnosis of electrical circuits, a task which MFM is not very well adapted for. MFM differs from statistical and control theory methods in that it uses discrete and more abstract representations, and thus is useful on a higher level of decision and diagnosis. For example, control theory methods are usually aimed at fault detection on control loop level, while MFM is aimed at diagnostic reasoning on a plant-wide level. Finally, MFM differs strongly from neural networks in that it explicitly represents human knowledge using linguistic concepts, and that the model construction relies almost completely on available human knowledge and not on automatic generalization of test cases.

CONCLUSIONS

MFM provides a good basis for reliability analysis for industrial processes. Among its advantages are an explicit description of goals and functions and a relatively easy knowledge engineering task. Using MFM solves the problems hampering older methods based on using reliability block diagrams, fault trees, and similar representations. Finally, the methods allows for reliability calculations on-line in real-time.

ACKNOWLEDGEMENTS

The authors would like to thank Morten Lind, who invented MFM and have supported our efforts from the beginning. We would also like to thank the staff at GoalArt, Antonio Calzada, David Sjölander, and Anu Uus for providing a inspiration, help, and a nice mental environment in our daily lives.

REFERENCES

Businaro, T., A. Di Lorenzo, G. B. Meo, M. I. Rabbani, and E. Rubino, "An Application of MFM Method for Nuclear Plant State Identification," Proceedings of the Halden Programmer's Group Meeting on Computerized Man-Machine Communication, Gothenburg, 1985.

Dahlstrand, F., "Alarm Analysis with Fuzzy Logic and Multilevel Flow Models", Proceedings of the 18th Annual International Conference of the British Computer Society Special Group on Expert Systems, ES98, Cambridge, England, pp.173–188, 1998.

Dahlstrand, F., *Methods for Alarm Reduction with Multilevel Flow Models of Industrial Processes*, Licentiate thesis, Department of Information Technology, Lund University, Lund, Sweden, 2000.

De, M. K., J. A. Rumancik, A. J. Impink, and J. R. Easter, "A Functional Design Approach to PWR Safety," Proceedings of the International Meeting on Thermal Nuclear Reactor Safety, Chicago, Illinois, 1982.

Duncan, K. D. and N. Prætorius, "Flow Displays Representing Complex Plant for Diagnosis and Process Control," Proceedings of the 2nd European Meeting on Cognitive Science Approaches to Process Control, Siena, 1989.

Frank, P. M., "Analytical and Qualitative Model-Based Fault Diagnosis ? A Survey and Some New Results," *European Journal of Control,* vol. 2, pp. 6–28, 1996.

Fussell, J. B., "A Review of Fault Tree Analysis with Emphasis on Limitations," Proceedings of the 6th Triennial World Congress of the International Federation of Automatic Control, Pittsburgh, Pennsylvania, 1975.

Greiner, R., B. A. Smith, and R. W. Wilkerson, "A Correction to the Algorithm in Reiter's Theory of Diagnosis," *Artificial Intelligence,* vol. 41, pp. 79–88, 1989.

Hamscher, W., L. Console, and J. de Kleer, (Eds.), *Readings in Model-Based Diagnosis,* Morgan Kaufmann, San Mateo, California, 1992.

Ingström, D., "MFM Modeling and Alarm Analysis of the Barsebäck Nuclear Power Plant," Master's thesis, Department of Information Technology, Lund Institute of Technology, Lund, 1998.

Inoue, K. and E. J. Henley, "Computer-Aided Reliability and Safety Analysis of Complex Systems," Proceedings of the 6th Triennial World Congress of the International Federation of Automatic Control, Pittsburgh, Pennsylvania, 1975.

Larsson, J. E., *Knowledge-Based Methods for Control Systems,* Doctor's thesis, TFRT–1040, Department of Automatic Control, Lund Institute of Technology, Lund, 1992.

Larsson, J. E., "Diagnostic Reasoning Strategies for Means-End Models," *Automatica,* vol. 30, no. 5, pp. 775–787, 1994.

Larsson, J. E., "Diagnosis Based on Explicit Means-End Models," *Artificial Intelligence,* vol. 80, no. 1, pp. 29–93, 1996.

Larsson, J. E., "Avoiding Human Error," Proceedings of the International Conference on Control and Instrumentation in Nuclear Installations, Bristol, England, 2000.

Larsson, J. E., "Diagnostic Reasoning Based on Means-End Models: Experiences and Future Prospects," *Knowledge-Based Systems,* vol. 15, no. 1-2, pp. 103-110, 2002.

Larsson, J. E. and F. Dahlstrand, "New Algorithms for MFM Alarm Analysis," invited paper, Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, San Diego, California, 1998.

Larsson, J. E. and B. Hayes-Roth, "Guardian: An Intelligent Autonomous Agent for Medical Monitoring and Diagnosis," *IEEE Intelligent Systems,* vol. 13, no. 1, pp. 58–64, 1998.

Larsson, J. E., B. Hayes-Roth, and D. M. Gaba, "Goals and Functions of the Human Body: An MFM Model for Fault Diagnosis," *IEEE Transactions on Systems, Man, and Cybernetics,* vol. 27, no. 6, pp. 758–765, 1997 a.

Larsson, J. E., B. Hayes-Roth, D. M. Gaba, and B. E. Smith, "Evaluation of a Medical Diagnosis System Using Simulator Test Scenarios," *Artificial Intelligence in Medicine,* vol. 11, pp. 119–140, 1997 b.

Lind, M., "Human-Machine Interface for Diagnosis Based on Multilevel Flow Modeling," Proceedings of the 2nd European Meeting on Cognitive Science Approaches to Process Control, Siena, 1989.

Lind, M., "Representing Goals and Functions of Complex Systems — An Introduction to Multilevel Flow Modeling," Technical report, 90–D–38, Institute of Automatic Control Systems, Technical University of Denmark, Lyngby, 1990 a.

Lind, M., "Abstractions Version 1.0 — Descriptions of Classes and Their Use," Technical report, 90–D–380, Institute of Automatic Control Systems, Technical University of Denmark, Lyngby, 1990 b.

Lind, M., "An Architecture for Real-Time MFM Diagnosis," Technical report, Institute of Automatic Control Systems, Technical University of Denmark, Lyngby, 1990 c.

Lind, M., "Modeling Goals and Functions of Complex Industrial Plants," *Applied Artificial Intelligence*, vol. 8, no. 2, pp. 259–283, 1994.

Monta, K., J, Takizawa, Y. Hattori, T. Hayashi, N. Sato, J. Itoh, A. Sakuma, and E. Yoshikawa, "An Intelligent Man-Machine System for BWR Nuclear Power Plants," Proceedings of AI91 — Frontiers in Innovative Computing for the Nuclear Industry, Jackson, Wyoming, 1991.

Öhman, B., "Failure Mode Analysis Using Multilevel Flow Models," Proceedings of the 5th European Control Conference, Karlsruhe, Germany, 1999.

Öhman, B., *Real-Time Diagnosis of Industrial Processes Using Multilevel Flow Models*, Licentiate thesis, Department of Information Technology, Lund University, Lund, Sweden, 2001.

Öhman, B., "Discrete Sensor Validation with Multilevel Flow Models," *IEEE Intelligent Systems*, vol. 17, no. 3, pp. 55-61, 2002.

Reiter, R., "A Theory of Diagnosis from First Principles," *Artificial Intelligence*, vol. 32, pp. 732–737, 1987.

Sassen, J. M. A., *Design Issues of Human Operator Support Systems*, Doctor's thesis, Faculty of Mechanical Engineering and Marine Technology, Laboratory for Measurement and Control, Delft University of Technology, Delft, 1993.

Walseth, J. Å., Diagnostic Reasoning in Continuous Systems, Doctor's thesis, ITK-rapport 1993: 164–W, Division of Engineering Cybernetics, Norwegian Institute of Technology, Trondheim, 1993.