System Reliability and Risk Assessment: A Quantitative Extension of IDEF Methodologies

Andrew Kusiak, Intelligent Systems Laboratory, Department of Industrial Engineering
Nick Larson, Intelligent Systems Laboratory, Department of Industrial Engineering
The University of Iowa, Iowa City, Iowa 52242-1527

1. Introduction

Evaluating system reliability requires modeling the interaction of resources, information, and material within the system. Such a model must consider quantitative data describing the reliability of each element of the system, as well as logical data describing the relationship between individual components. For example, a manufacturing system may assemble products X, Y, and Z, on machines M1, M2, and M3, respectively, and package the products on a fourth machine, M4. Therefore, three different relationships exist between the components of the system, one for each product. If the reliability of each machine differs, the system reliability will differ depending on the product. Similarly, the reliability of the system as a whole will be affected by the production levels of products X, Y, and Z.

Given the example above, with only three products and four machines, it becomes apparent that determining system reliability requires a significant amount of data and a structured modeling methodology. Furthermore, to obtain an accurate assessment of system reliability, it is necessary to include additional data describing information and material components of the system; such as inspection procedures, assembly specifications, parts, and subassemblies.

System reliability describes the likelihood of success or failure in the operation of a system. Risk assessment is a technique for identifying scenarios that lead to problems in a system, determining the likelihood of each scenario, and the evaluating the consequence of each scenario, i.e., the problem. Although quantitative approaches to risk assessment employ the principles of system reliability, the identification, quantification, and evaluation of risk is a more comprehensive modeling activity. Therefore, risk assessment projects are well suited for the tools developed for process modeling and analysis.

In 1978, the United States Air Force selected SADT (Structured Analysis and Design Technique) as the language to support the Integrated Computer Aided Manufacturing (ICAM) program. SADT activity modeling was adopted by the ICAM program and revised by SofTech, Inc. to develop the ICAM Definition Methodology (IDEF0). Ross (1985) states that "thousands of people from hundreds of organizations working on more than one hundred major projects" proceeded to use the methodology for system definition and design, as well as project management. IDEF0 introduced manufacturing to techniques that were developed for computer system and software engineering applications. Additional IDEF techniques were developed for information analysis (IDEF1), dynamic analysis (IDEF2), and process modeling (IDEF3).

This paper presents procedures for integrating system reliability and risk assessment techniques with IDEF0 and IDEF3 modeling. The paper is motivated by the need to increase the value of IDEF0 and IDEF3 models by incorporating quantitative data, thus, extending model use to applications such as risk assessment. By extending the power of existing IDEF models, process modeling will become more attractive to management and evolve as a powerful tool for reengineering design and manufacturing systems.

2. Definitions of System Reliability and Risk Assessment

Reliability may be defined as the ability of an item (product, system, etc.) to operate under designated operating conditions for a designated period of time or number of cycles (Modarres, 1993). An item's reliability is often measured by the probability it will perform without failure given a set of conditions. The following expression is a probabilistic representation for reliability.

$$R(t) = P(T \geq t | c_1, c_2, \ldots) \tag{1}$$

In (1), t is the period of time for the item's operation, T is the time to failure of the item, $R(t)$ is the reliability of the item, and $c_1, c_2, \ldots$ are the conditions under which the item is operating. The variable t is often referred to as the mission time. In practice, T is a random variable representing the time-to-failure of the item, and $c_1, c_2, \ldots$ are implicitly considered. Furthermore, $f(t)$ may represent the probability density function of the random variable T. The probability that the item fails prior to time t is defined in (2).

$$P(T \leq t) = \int_0^t f(\theta)d\theta = F(t), \qquad \text{for } t \geq 0 \tag{2}$$

Since $F(t)$ denotes the probability the item will fail prior to time t, it is formally the unreliability of the item. Thus, the reliability of the item is determined by (3).

$$R(t) = 1 - F(t) = \int_t^\infty f(\theta)d\theta \tag{3}$$

A system is a collection of entities (i.e., information and material) and resources (i.e., machines and workers)

which interact to perform a set of activities in a given process. Successful completion of the process is dependent upon proper completion of the individual activities in the process. Therefore, it is necessary to model the relationship between various items (entities and resources), as well as the reliability of individual items to assess the reliability of the system. Complex manufacturing systems produce many different products through many different sequences of manufacturing activities. The system reliability is a function of the activities performed and, thus, is product dependent. Therefore, if the production volume of a product exhibiting low system reliability is increased, the reliability of the entire manufacturing system will decrease. At this point, the necessity for evaluating system reliability in a manufacturing setting becomes obvious.

Many of the common techniques for modeling system reliability are difficult to apply to complex manufacturing systems with multiple product types. Therefore, the principles of such tools are more useful when applied to modeling schemes developed for manufacturing systems, such as IDEF0 and IDEF3. Also, the task of evaluating system reliability in a manufacturing setting is more attractive if performed as a component of a risk assessment study.

Risk is a measure of the probability and severity of adverse effects (Lowrance, 1976). Several types of risk associated with project planning and software development have been cited in the literature; see Ang and Gay (1993) and Chittister and Haimes (1993). The following manufacturing risks are generalized from those cited in various engineering disciplines.

1. Requirements risk. The concept of what the product is intended to accomplish is not accurate.
2. Technical risk. The product does not adhere to the requirements set forth by its design.
3. Schedule risk. The product will not be completed by the deadline set forth by production planning.
4. Cost risk. The production cost will overrun its budget.
5. Network risk. The mechanism for linking various production activities will not perform as intended.

Risk assessment is a process that attempts to answer three questions: (1) What can go wrong? (2) What is the likelihood that it will go wrong? (3) What are the consequences? (Kaplan and Garrick, 1981). Based on these questions, (4) is a quantitative definition of risk, where S_i is a scenario of events that leads to a problem, P_i is the likelihood of scenario i, and C_i is the consequence of scenario i.

$$R = \{S_i, P_i, C_i\} \qquad i = 1, 2, ..., n \qquad (4)$$

This section has provided definitions of system reliability and risk assessment. Section 4 discusses techniques for determining system reliability and integrating risk assessment and IDEF models. Section 5 discusses issues related to risk assessment, such as developing quantitative risk models based on IDEF0 and IDEF3.

3. Fundamentals of IDEF0 and IDEF3

IDEF0 was developed for modeling a wide variety of systems which use hardware, software, and people to perform activities (U. S. Air Force, 1981). An IDEF0 model consists of three components, diagrams, text, and a glossary, all cross-referenced to each other. The box and arrow diagrams are the major components of the model. In a diagram, a box represents a function and an arrow represents an interface. A box is assigned an active verb phrase to represent the function. An interface may be an input, an output, a control, or a mechanism, and is assigned a descriptive noun phrase. Inputs (I) enter the box from the left, are transformed by the function, and exit the box to the right as an output (O). A control (C) enters the top of the box and influences or determines the function performed. A mechanism (M) is a tool or resource which performs the function. The interfaces are generally referred to as the ICOMs (see Figure 1).

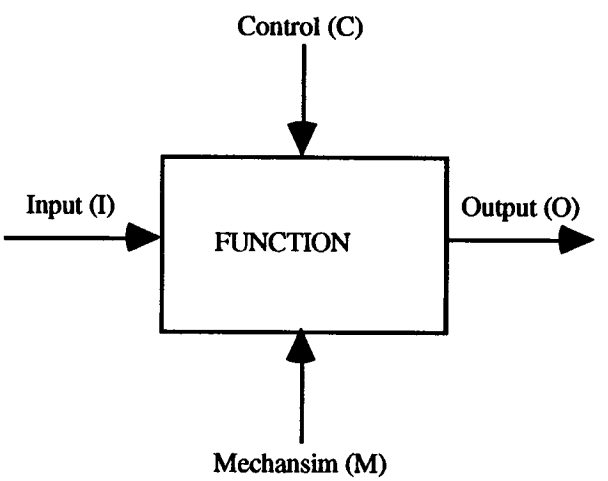

Figure 1. IDEF0 function box and interface arrows

Each diagram has between three and six function boxes placed on a diagonal. The boxes each have a specific node number and are connected by all relevant interfaces. Each box on the diagram may be decomposed into a lower level of detail. This feature restricts the amount of information that may be contained in the model on a single level. The resulting diagrams form a hierarchy of information which is summarized in a node tree.

IDEF0 provides a structured representation of the functions, information, and objects which are interrelated in a manufacturing system. IDEF3 was created specifically to model the sequence of activities performed in a manufacturing system. An IDEF3 model enables an expert

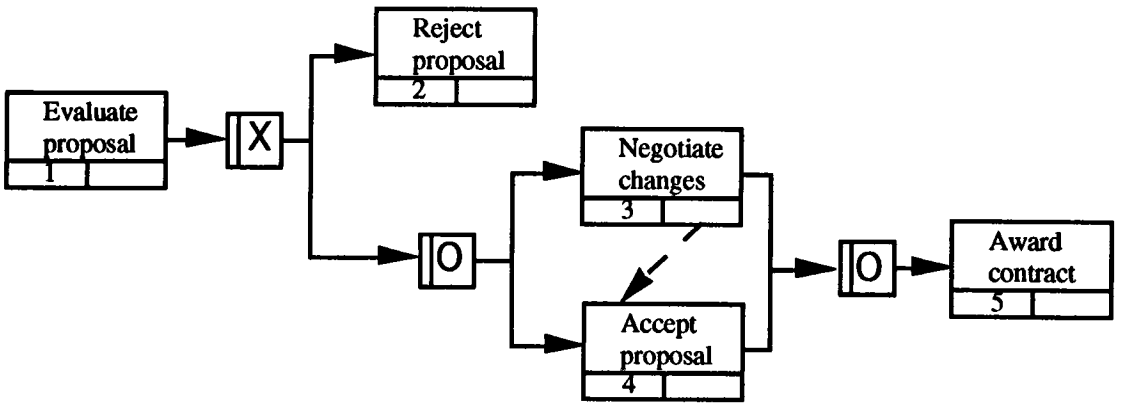

Figure 2. IDEF3 process flow diagram (Mayer et al. 1992)

to communicate the process flow of a system through defining a sequence of activities and the relationships between those activities. There are two basic components of the IDEF3 process description language, the process flow description and the object state transition network description. The two components are cross-referenced to build IDEF3 diagrams (Mayer et al., 1992).

The IDEF3 process flow description is made up of units of behavior (UOBs), links, and junction boxes. A UOB represents a function or activity occurring in the process. For example, *assemble parts, perform inspection,* or *evaluate proposal* are all activities which may be represented as UOBs in a process model. Relationships between UOBs are modeled with three types of links, precedence links, relational links, and object flow links. Precedence links express simple temporal precedence between UOBs. Relational links highlight the existence of a relationship between two or more UOBs, however, no temporal constraint is implied. Object flow links provide a mechanism for capturing object related constraints between UOBs and carry the same temporal semantics as a precedence link. The logic of branching within a process is modeled using junctions. Several classifications are used to define junction boxes. Junctions are classified according to logical semantics as *and* (&), *or* (O), and *exclusive or* (X). Multiple process paths are classified as *fan-in* or *fan-out* corresponding to converging and diverging paths, respectively. The relative timing of process paths that converge or diverge at a junction are classified as *synchronous* or *asynchronous*. An example of an IDEF3 process flow diagram is shown in Figure 2 (Mayer et al., 1992).

4. Integrating System Reliability Techniques and IDEF Models

As stated in section 2, system reliability tools may be quite useful when applied to modeling schemes developed for manufacturing systems, such as IDEF0 and IDEF3. In this section, several system reliability modeling techniques are integrated with IDEF0 and IDEF3. For a detailed discussion of each technique, see Modarres (1993).

4.1 Reliability Block Diagrams

Reliability block diagrams model the effect of component failure on system performance by capturing the physical arrangement of the system. Typical system configurations include series systems, parallel systems, standby redundant systems, shared load systems, complex parallel-series systems, and complex nonparallel-series systems (Modarres, 1993). Additional system configurations may be identified in various applications, however, most manufacturing systems may be accurately described using those listed above. Figure 3 shows reliability block diagrams for series and parallel systems and Figure 4 illustrates complex systems. The reliability of complex systems may be calculated using various analytical methods, however, such methods become computationally intensive as the number of components increases (Shooman, 1990).

The system configurations illustrated in Figures 3 and 4 may also be used to describe IDEF0 and IDEF3 models. Ang and Gay (1993) discuss extensions to IDEF0 models which enable project risk assessment. Several project situations are described which may be generalized to the system configurations described above. The extensions are efficient for including quantitative data in an IDEF0 model, such as a probability of occurrence. However, due to the decomposition principle of IDEF0, it is difficult to identify complex system configurations in the model. The concepts of reliability block diagrams are more easily adapted to IDEF3 models. Consider Figure 2; the five activities in the model are arranged in a complex parallel-series configuration. Unlike IDEF0 models, the number of activities (i.e., functions) in IDEF3 models is not restricted to six per level. Although IDEF3 allows for elaboration on a particular UOB (i.e., activity), the entire process flow may be constructed on a single level. This representation is more suitable for IDEF applications of risk assessment

which are based on the principles of reliability block diagrams.

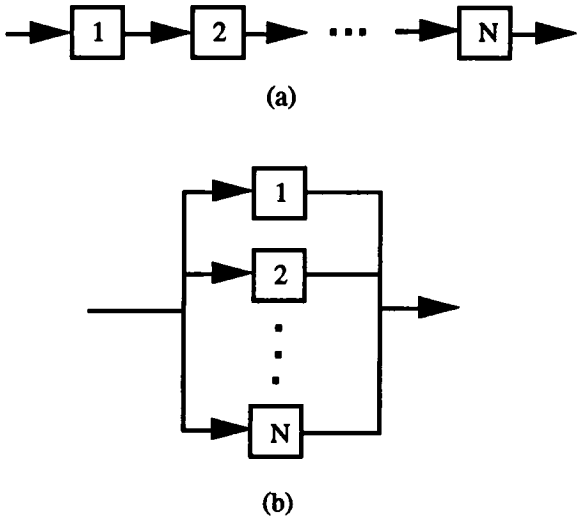

Figure 3. Series (a) and parallel (b) system configurations

In IDEF3, series systems (or the series components of a complex system) are identified by UOBs connected by precedence and/or object flow links. A series of UOBs may not contain a junction of any type, however, a junction box may begin or terminate a series. Furthermore, a UOB is independent if it is not connected to another UOB by a relational link. The reliability of a series of independent UOBs is defined by (5), where $R_S(t)$ is the reliability of the system, the system contains N UOBs, and $R_i(t)$ is the reliability of the ith UOB.

$$R_s(t) = R_1(t) \times R_2(t) \times \ldots \times R_N(t) = \prod_{i=1}^{N} R_i(t) \qquad (5)$$

Parallel systems are defined in IDEF3 using junction boxes. Each UOB immediately following an *and* (&) junction box will be performed in parallel. Therefore, the reliability of the parallel system following an & junction box is determined by (5) as well. However, only one UOB immediately following an *exclusive or* (X) junction box is performed. Thus, the system reliability for parallel UOBs following an X junction box is defined by (6), where the system contains N UOBs, $R_i(t)$ is the reliability of the ith UOB, and P_i is the probability of occurrence of the ith UOB ($P_1+P_2+\ldots+P_N = 1$).

$$R_s(t) = (P_1 \times R_1(t)) + (P_2 \times R_2(t)) + \ldots + (P_N \times R_N(t)) = \sum_{i=1}^{N} (P_i \times R_i(t)) \qquad (6)$$

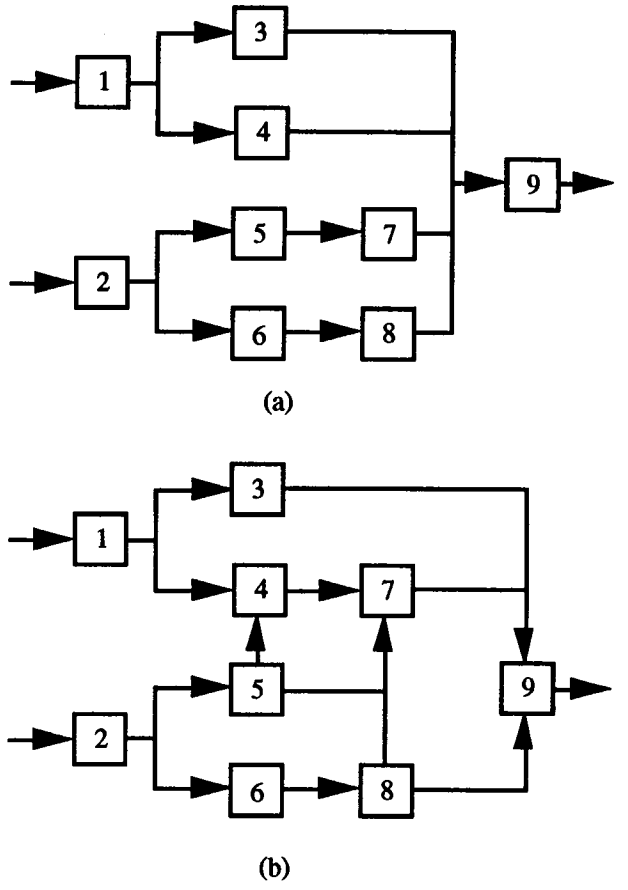

Figure 4. Complex parallel-series (a) and nonparallel-series (b) systems

The system reliability for parallel UOBs following an *or* (O) junction box is more difficult to determine. At least one, and as many as all, of the UOBs following an O junction box may be executed. Unlike the & and X cases, the number of different UOBs performed in parallel is unknown. However, if the system contains N UOBs, $R_i(t)$ is the reliability of the ith UOB, and P_i is the probability of occurrence of the ith UOB ($P_i \leq 1$), a lower bound on the system reliability is given by (7). This describes the worst case, where all UOBs are executed and subject to failure. If the reliability is to be evaluated for a known set of M UOBs in the parallel system ($M < N$), (5) may be used. Figure 5 illustrates parallel system UOBs for &, X, and O junction boxes in IDEF3.

$$R_s(t) = (P_1 \times R_1(t)) \times (P_2 \times R_2(t)) \times \ldots \times (P_N \times R_N(t)) = \prod_{i=1}^{N} (P_i \times R_i(t)) \qquad (7)$$

Two or more UOBs connected by relational links may be considered a single UOB when calculating system reliability in IDEF3 models. In Figure 2, UOBs 3 and 4

are connected by a relational link, implying an interaction with UOB 4 if UOB 3 is executed. In this example, successfully executing UOB 3 will also require successful completion of UOB 4 (i.e., $R_3(t) = R_3(t) \times R_4(t)$). However, UOB 4 does not require execution of UOB 3 and, therefore, is not dependent upon its success. The direction of the relational link determines the reliability of the connected UOBs. In general, if UOB i is connected to UOB $(i + 1)$ with a relational link in the direction of UOB $(i + 1)$, the success or failure of UOB i will determine to success or failure of UOB $(i + 1)$. In IDEF3 applications of system reliability modeling, relational links may be avoided by combining related activities into a single UOB.

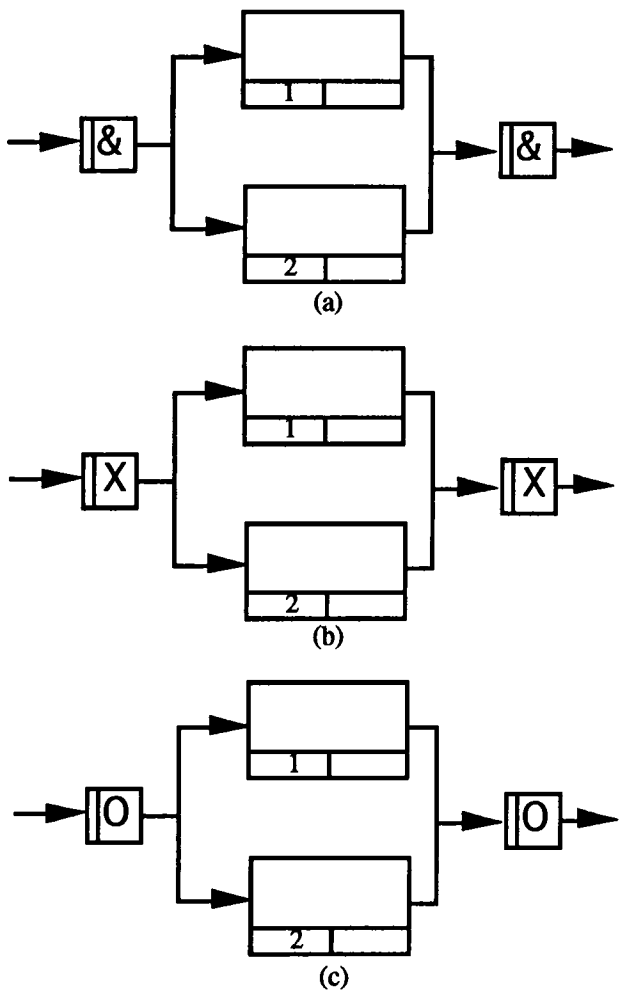

Figure 5. Parallel systems modeled using IDEF3 notation for *and* (a), *exclusive or* (b), and *or* (c) junction boxes

4.2 Path Set and Cut Set Methods

Path set and cut set methods were developed to determine the reliability of complex systems described by reliability block diagrams. However, the principles of these methods are very useful in the analysis of IDEF3 models. A path set is a set of units (i.e., activities, functions, UOBs) that form a connection between input and output when traversed in the direction of the arrows (Modarres, 1993). For each path through an IDEF3 model, a minimal path set will exist containing only the UOBs on the path. Once again, consider Figure 2. There are three minimal path sets in the IDEF3 model; $P_1 = (1, 2)$, $P_2 = (1, 3, 5)$, and $P_3 = (1, 4, 5)$. Each path set represents an event that would successfully accomplish the objective of the system if each of the UOBs on the path execute successfully. Therefore, the union of all m path sets defines the set of all successful completions of the system. The probability of this union represents the reliability of the system, as shown in (8).

$$R_s(t) = \text{Prob}(P_1 \cup P_2 \cup \ldots \cup P_m) \tag{8}$$

Unfortunately, (8) requires that the path sets (P_i) be disjoint and, in practice, this is seldom true. An upper bound on the system reliability may be determined by assuming that the path sets are disjoint, as in (9). However, for reliability values greater than 0.9 for the mission time, as in most practical applications, (9) does not yield a useful bound (Modarres, 1993).

$$R_s(t) \leq \text{Prob}(P_1) + \text{Prob}(P_2) + \ldots + \text{Prob}(P_m) \tag{9}$$

A cut set is a set of units (i.e., activities, functions, UOBs) that interrupt all possible connections between the input and output points in the diagram (Modarres, 1993). In IDEF3 process flow models, the minimal cut set is the smallest set of UOBs which prevent flow from input to output. Failure of all UOBs in the minimum cut set results in system failure. The minimum cut sets in Figure 2 are $C_1 = (1)$, $C_2 = (2, 3, 4)$, and $C_3 = (5)$. If the model has n minimal cut sets and C_i represents the event that all UOBs in the cut set fail prior to the mission time t, the system reliability is obtained from (10). Since the probability that all the UOBs fail in at least one of the cut sets is the probability that the system fails, this value is subtracted from 1 to obtain the reliability of the system.

$$R_s(t) = 1 - \text{Prob}(C_1 \cup C_2 \cup \ldots \cup C_n) \tag{10}$$

As in (8), the union in (10) is not usually disjoint, thus, (11) gives the lower bound for system reliability. Since the probability of failure is used to evaluate the cut sets and, in practice, these values are much lower than reliabilities, the lower bound in (11) is a better representation of system reliability.

$$R_s(t) \geq 1 - [\text{Prob}(C_1) + \text{Prob}(C_2) + \ldots + \text{Prob}(C_n)] \tag{11}$$

The principles of path sets may be adapted to evaluate decision making processes modeled with IDEF3. Each

minimal path set identified in an IDEF3 model corresponds to a set of decisions in the operation of the system. Junction boxes identify points where decisions are made within a system. The decision set corresponding to path set $P_3 = (1, 4, 5)$ is D_3 = {do not reject proposal, accept proposal}. Two decisions are made in the process; one corresponding to each diverging (or fan out) junction box. The first decision is to "not reject the proposal" and the second is to "accept the proposal." Therefore, the reliability of the decision set may be easily determined by calculating the probability of successfully completing all UOBs in the corresponding path set.

Cut sets may be used to expose critical activities in the system. UOBs in the intersection of all or many of the cut sets may be considered critical to the operation of the system. Furthermore, a cut set with a high probability of failure (i.e., there are few UOBs in the cut set and each has a high probability of failure) may be considered a critical group of UOBs.

Applying system reliability techniques to IDEF3 models requires incorporating quantitative data regarding probability of occurrence of UOBs and probability of failure for each UOB. Reliability values for each of the ICOMs in IDEF0 models may be used to obtain probability of failure data for the corresponding UOB of an IDEF3 model. Diverging (or fan-out) junction boxes in IDEF3 may also contain probability of occurrence values for each UOB that immediately follows the junction box.

5. Risk Assessment in IDEF Models

Evaluating risk in IDEF models requires identifying scenarios, determining the likelihood of these scenarios, and estimating the consequences. This set of objectives is often called the "risk triplet." The first two components of the risk triplet are related to the techniques for determining system reliability discussed in Section 4. Path sets may be used to identify scenarios in the system. Each scenario is qualitatively evaluated to identify possible problems that may result. The likelihood of each scenario is determined by the probability of occurrence of the UOBs in the path set.

Determining the consequences of the scenario requires estimating the impact on a set of performance measures. Typical performance measures in manufacturing systems are in-process inventory levels, lead times, set-up times, scrap, rework, and resource utilization. When possible, consequences related to different performance measures should be converted to a single unit of measurement, such as dollar loss.

The total expected risk in the system is calculated by (12), where P_i is the probability of scenario i, and C_i is the consequence, or cost, of the scenario.

$$R = \sum_{i=1}^{n} (P_i \times C_i) \qquad (12)$$

It must be realized that the values for P_i and C_i are based on approximations and assumptions and, thus, possess a high level of uncertainty. Formal methods for treating uncertainty analysis are discussed in the literature (Morgan and Henrion, 1990).

Upon calculating the expected risk in the system, two courses of action may be taken; (1) explore alternative management decisions to avoid risk (i.e., decrease the likelihood of high risk scenarios), and (2) reengineer processes to mitigate the consequences.

IDEF0 and IDEF3 were developed to provide a mechanism for evaluating the performance of complex manufacturing systems. System reliability and risk assessment are applications which provide a useful opportunity for extending the power of these methodologies.

Acknowledgment

This research has been partially supported by grant No. DAAE07-93-C-R080 from the U.S. Army Tank Automotive Command.

References

Ang, C. L. and R. K. L. Gay (1993). "IDEF0 modeling for project risk assessment," *Computers in Industry*, **22**, pp. 31-45.

Chittister, C. and Y. Y. Haimes (1993). "Risk associated with software development: A holistic framework for assessment and management," *IEEE Transactions on Systems, Man, and Cybernetics*, **23**(3), pp. 710-723.

Kaplan, S. and B. J. Garrick (1981). "On the quantitative definition of risk," *Risk Analysis*, **1**(1), 1981.

Lowrance, W. W. (1976). *Of Acceptable Risk*, William Kaufmann, Los Altos, CA.

Mayer, R. J., T. P. Cullinane, P. S. deWitte, W. B. Knappenberger, B. Perakath and M. S. Wells (1992). *Information Integration for Concurrent Engineering (IICE) IDEF3 Process Description Capture Method Report*, Armstrong Laboratory, Wright-Patterson AFB, Ohio 45433, AL-TR-1992-0057.

Modarres, M. (1993). *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York, NY.

Morgan, M. G. and M. Henrion (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge Press, Cambridge, U.K.

Ross, D. T. (1985). "Applications and extensions of SADT," *Computer*, **April**, pp. 25-34.

Shooman, M. L. (1990). *Probabilistic Reliability: An Engineering Approach*, 2nd Ed., Kreiger, Melbourne, FL.

U. S. Air Force (1981). *Integrated Computer Aided Manufacturing (ICAM) Architecture Part II, Volume IV-Functional Modeling Manual (IDEF0)*, Air Force Materials Laboratory, Wright-Patterson AFB, Ohio 45433, AFWAL-tr-81-4023.