

# Hazard Analysis in Engineering Design

## Introduction

The National Society of Professional Engineers (NSPE) is the society for registered professional engineers which was founded in 1934 and has approximately 60,000 members. NSPE has articulated a Code of Ethics for Engineers that spans the entire range of engineering and is widely accepted by professional engineers. In the preamble to the code, the following statement is made:

“...the services provided by engineers require honesty, impartiality, fairness and equity, and **must be dedicated to the protection of the public health, safety, and welfare.**” (emphasis added)

The NSPE code of ethics lists six fundamental canons. The **FIRST** of those canons is stated as follows:

“Engineers, in the fulfillment of their professional duties, shall ...**hold paramount the safety, health and welfare of the public.**” (emphasis added)

Associated with the first fundamental canon are five rules of practice, two of which are stated as follows:

a. **If engineers' judgment is overruled under circumstances that endanger life or property, they shall notify their employer or client and such other authority as may be appropriate.** (emphasis added)

e. **Engineers having knowledge of any alleged violation of this Code shall report thereon to appropriate professional bodies and, when relevant, also to public authorities, and cooperate with the proper authorities in furnishing such information or assistance as may be required.** (emphasis added)

It is significant that the first duty of an engineer, according to the NSPE, is to be dedicated to the protection of the public health, safety, and welfare. This obligates a design engineer to assess potential failure modes and the resulting hazards to people for every design as part of the engineering design process.

The Accreditation Board for Engineering and Technology (ABET) accredits university engineering and technology programs of all varieties across the United States. ABET [1997] has published a Code of Ethics for Engineers. The **FIRST TWO** of the four Fundamental Principles are -- Engineers uphold and advance the integrity, honor and dignity of the engineering profession by:

- using their knowledge and skill for the **enhancement of human welfare;** (emphasis added)
- being honest and impartial, and **servicing with fidelity the public,** their employers and clients; (emphasis added)

The **FIRST** Fundamental Canon is stated as follows:

1. **Engineers shall hold paramount the safety, health and welfare of the public** in the performance of their professional duties. (emphasis added)

Obviously ABET agrees with NSPE that the first duty of an engineer is to protect public health, safety, and welfare.

ASME International (formerly the American Society of Mechanical Engineers) is the principal professional society for mechanical engineers which was founded in 1880 and has a membership of approximately 125,000 worldwide. ASME International has published a Code of Ethics for Engineers which contains three fundamental principles. The **FIRST** of those fundamental principles is stated as follows:

**“Engineers uphold and advance the integrity, honor and dignity of the engineering profession by ...using their knowledge and skill for the enhancement of human welfare.”** (emphasis added)

The ASME code also lists eight fundamental canons, the **FIRST** of which is stated as follows:

**“Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties.”** (emphasis added)

The ASME code presents the following statements of interpretation for the first fundamental canon:

- a. **Engineers shall recognize that the lives, safety, health and welfare of the general public are dependent upon engineering judgments, decisions and practices incorporated into structures, machines, products, processes and devices.** (emphasis added)
- b. **Engineers shall not approve or seal plans and/or specifications that are not of a design safe to the public health and welfare** and in conformity with accepted engineering standards. (emphasis added)
- c. **Whenever the Engineers' professional judgments are over ruled under circumstances where the safety, health, and welfare of the public are endangered, the Engineers shall inform their clients and/or employers of the possible consequences.** (emphasis added)
  - (1) Engineers shall endeavor to provide data such as published standards, test codes, and quality control procedures that will enable the users to understand safe use during life expectancy associated with the designs, products, or systems for which they are responsible.
  - (2) **Engineers shall conduct reviews of the safety and reliability of the designs, products, or systems for which they are responsible before giving their approval to the plans for the design.** (emphasis added)
  - (3) **Whenever Engineers observe conditions, directly related to their employment, which they believe will endanger public safety or health, they shall inform the proper authority of the situation.** (emphasis added)
- d. **If engineers have knowledge of or reason to believe that another person or firm may be in violation of any of the provisions of these Canons, they shall present such information to the proper authority in writing and shall cooperate with the proper authority in furnishing such further information or assistance as may be required.** (emphasis added)

Obviously ASME International agrees with the NSPE and ABET that the first duty of an engineer is to protect public health, safety, and welfare. The ASME Code of Ethics for Engineers First Fundamental Canon, statements b and c.2 specifically advise engineers to conduct an analysis of the safety of a design, product or system before approving the plans.

In the chemical industry, US government regulations require a process hazard analysis -- OSHA's Process Safety Management standard 29CFR 1910.119, and EPA's Risk Management Program Rule 40 CFR Part 68. Most hazard analysis methodologies presented herein may be used either for product or process design or redesign.

## **The Engineering Design Process**

The engineering design process is part of the overall product or process realization process which takes an idea from conception through implementation to obsolescence. It involves a very detailed cradle to grave analysis. Once a decision has been made to develop a new product or process, the engineering design process to achieve it may be described as follows:

1. Conceptual design/Taguchi systems design [Taguchi et al, 1989] – generate multiple potential solutions. Perform “quick and dirty” initial analyses of each potential solution. Benchmark the potential solutions against a common set of requirements and select the most promising.
2. Detailed design/Taguchi parameter and tolerance design [Taguchi et al, 1989] – perform detailed analyses on the selected solution to determine functionality, geometry, size, fit, finish, tolerances, human interface, safety, etc. Develop all of the models, specifications, drawings and plans necessary for production, distribution, use and disposal.

The conceptual design step is characterized by the generation of multiple potential product or process ideas. These ideas may come from the natural evolution of existing products or processes, benchmarking competing products or processes, market surveys, new knowledge, or the generation of new and different ideas (brainstorming). Each of these ideas undergoes preliminary analysis to create a common basis for comparison. The ideas are then compared against each other (a benchmarking process) and the idea judged to have the highest probability of success is selected for further development. The detailed design process then fleshes out the idea into a workable design and produces all of the information necessary to implement the selected design.

Problems that are solved very early in the design process incur insignificant development cost and provide very large potential revenue gains through simplified production, increased consumer satisfaction, increased market share, and reduced product liability. Problems that are solved late in the design process or after production has begun usually incur substantial development cost and implementation delay.

## **Design for Safety**

Design for Safety [Bralla, 1996, pp. 195-210] is a design methodology that protects the health, safety and welfare of the customer, the public, and the workers who manufacture and distribute the product. It requires that the potential hazards inherent in the manufacture, distribution, use, and disposal of a product be identified in the design phase and mitigated as much as possible. While it may not be possible to remove all hazards from a product (eg. the sharp kitchen knife), the number and severity of the hazards should be minimized and the customer warned about the hazards that remain.

The first step in identifying the hazards associated with any system is to identify all possible ways the system might fail through internal faults, customer use and abuse, and use in challenging environments. Potential failure modes for mechanical components and systems may be listed as follows [after Dieter, 2000, p. 559]:

1. Elastic deformation
2. Brittle fracture
3. Plastic deformation, creep, yielding
4. Ductile failure, buckling, ductile fracture, stress rupture, yielding
5. Fatigue failure: corrosion induced, fretting induced, high-cycle, impact induced, low-cycle, surface, thermal induced, vibration induced
6. Impact/shock induced failure: deformation, fatigue, fracture, fretting, wear
7. Wear: adhesive, abrasive, cavitation, corrosive, deformation induced, erosion, fretting, galling, impact induced, scoring, surface fatigue, surface pitting
8. Thermally induced failure: change of material properties, deformation, thermal shock
9. Bonding failure, delamination
10. Corrosion/chemical attack: galvanic, crevice, hydrogen, intergranular, leaching, oxidation, pitting
11. Combined failure: creep induced buckling and fatigue, thermally induced deformation, etc.
12. Mechanical interface failure: decoupling, interference, seizing, slipping,
13. Biological/environmental attack: animals, decay, insects, people, plants, weather
14. Radiation damage: infrared, microwave, nuclear, ultraviolet (UV)

Potential failure modes for electrical components and systems may be listed as follows:

1. Overvoltage conditions
2. Undervoltage conditions
3. Open circuit failures: what leads to loss of output?
4. Short circuit failures: what happens with the system output is shorted out?
5. Thermal problems: change in material properties, operating temperature, thermal expansion, thermal runaway
6. Mechanical problems: component insertion/removal, vibration
7. Component burnout: how does one failed component affect the system?
8. Supply power problems: fundamental frequency, high frequency noise, RMS and P-P voltage, waveform
9. Time domain signal anomalies: noise, spurious signals, waveform
10. Frequency domain signal anomalies: aliasing, distortion, spectral content

MIL-STD-1629A requires that the following minimum set of system failure modes be considered:

1. Premature operation.
2. Intermittent operation.
3. Failure to operate at a prescribed time.
4. Failure to cease operation at a prescribed time.
5. Loss of output or failure during operation.
6. Degraded output or operational capability.

Once the potential failure modes have been identified, then the hazards associated with them can be determined. The failure modes should be examined from the greatest hazard to the least in an effort to eliminate the failure mode or mitigate the hazard caused by it. The goal of design for safety is to produce a product or process with the minimum potential hazard exposure.

Design for Safety is discussed by the following authors: Atila & Jones [1993, pp. 370-374], Bralla [1996, pp. 195-210], Dieter [2000, pp. 565-567], Lindbeck [1995, pp. 239-246] and Voland [1999, pp. 328-330].

## **Historical Failure and Hazard Information**

Historical information on the performance and problems of existing products and processes is useful to the design engineer. Such information is available in customer service departments and repair facilities as part of their normal activities. It need only be collected and archived for future reference. It may also be collected as part of a market survey. In addition, litigation filed for personal injury and product liability can be scanned for cases involving similar products or processes and the allegations can be examined.

A significant number of similar complaints about a product or process may indicate a problem that should be addressed in the next redesign cycle. By systematically removing potential hazards from a product or process it is made safer and therefore more desirable to the customer, assuming the price does not increase significantly beyond inflation. In addition, the exposure to litigation is reduced, thereby saving additional costs.

## **Intelligent Fast Failure**

Intelligent fast failure [Matson, 1991] is a conceptual design methodology in which potential solutions which are known to be unsuitable or unworkable are compiled by an idea generation process such as brainstorming. These unsuitable potential solutions may be used in conjunction with a list of potentially suitable solutions to define the limits of the design space within which the engineer must work. The intelligent fast failure process may easily incorporate a qualitative analysis of potential failure modes and hazards of the ideas generated. This information may then be used to guide the benchmarking process used to select the design idea that will be developed and implemented. Using this methodology, a design engineer is aware from the outset of potential failure modes and

hazards of each new design and may take steps to minimize the hazards during the design process at little additional cost.

### **Failure Modes and Effects Analysis (FMEA)**

Failure Modes and Effects Analysis is a formal methodology for identifying potential failure modes and their associated hazards which is suitable for detailed engineering design of a product or process. Middendorf [1998, p. 46] [1990, pp. 40-1] describes the steps as follows:

1. Describe the system or process whose failure modes are sought.
2. Identify the ways in which the system or process might fail. These failure modes may be identified by historical data, personal experience, or a process similar to brainstorming.
3. Identify the symptoms of each failure mode that might aid in detection.
4. Determine the effects of each failure mode should it occur – look at property damage and hazard to people.
5. Assess the probability of each failure mode occurring. A qualitative ranking may be used if statistical data is not available – a low ranking means a low probability of occurrence.
6. Assess the risk (probability) of personal injury and property damage for each failure mode. Again, a qualitative ranking may be used in the absence of statistical data.
7. Compute a “danger index” from the numbers assigned in steps 5 & 6 – multiply the probabilities or rankings together.

The FMEA is normally presented as a table. The danger index is a ranking of the risks associated with each design. The failure modes should be examined for possible mitigation through design changes starting with the highest danger index and proceeding to the lowest. It is usually not possible to completely eliminate all failure modes from a consumer product but the hazard to people should be minimized as much as possible. This process should also minimize the exposure of the manufacturer to product liability litigation.

McDermott, et. al, [1996, pp. 35-38] and Dieter [2000, pp. 551-554] propose rating scales for failure severity, probability of occurrence, and probability of detection as shown in tables 1-3. Given ratings in all three categories for each failure mode, a risk priority number (RPN) is computed as follows:

$$\text{RPN} = (\text{failure severity}) \times (\text{probability of occurrence}) \times (\text{probability of detection}) \quad (1)$$

The failure modes should be ranked in descending order by RPN and those at the top of the list should be addressed first. A high RPN indicates a significant risk of system failure and hazard that should be mitigated if possible by redesigning the system to reduce effect severity, reduce the probability of occurrence, and increase the probability of detection. Once changes have been made to the design, the severity, occurrence, detection, and RPN values are recomputed for the affected failure modes.

All potential failure modes cannot be eliminated from all systems, but the goal of the design process should be to minimize RPNs of the system. A minimum RPN should correspond to maximum public safety and minimum exposure to litigation.

<b>Rating</b>	<b>Description</b>	<b>Effect on System or Customer</b>	<b>Potential for Property Damage</b>	<b>Potential Hazard</b>
<b>1</b>	Not noticeable	almost none	almost none	almost none
<b>2</b>	Very minor	noticeable	almost none	almost none
<b>3</b>	Minor	customer annoyed	almost none	almost none
<b>4</b>	Slight	customer annoyed system needs service	almost none	almost none
<b>5</b>	Moderate	customer complains system needs service	minor	slight
<b>6</b>	Significant	customer complains partial system malfunction	moderate	slight
<b>7</b>	Major	customer dissatisfied major system malfunction	significant	minor injury
<b>8</b>	Extreme	system inoperable or unfit for use	major	injury
<b>9</b>	Critical	system inoperable or unfit for use	extreme	serious injury
<b>10</b>	Hazardous	system inoperable or unfit for use	extreme	life threatening injury

<b>Rating</b>	<b>Description</b>	Dieter [2000, p. 552]	McDermott [1996, p. 37]	
		<b>One Occurrence per ? Events</b>	<b>One Occurrence per ? Events</b>	<b>One Occurrence</b>
<b>1</b>	Extremely remote	1,000,000	500,000,000	in 5+ years
<b>2</b>	Highly unlikely	100,000	500,000,000	in 3-5 years
<b>3</b>	Very slight chance	25,000	1,666,667	in 1-3 years
<b>4</b>	Slight chance	2,500	16,667	per year
<b>5</b>	Occasional	500	10,000	in 6 months
<b>6</b>	Moderate	100	333	in 3 months
<b>7</b>	Fairly frequent	25	100	per month
<b>8</b>	High	5	20	per week
<b>9</b>	Very high	3	3	every few days
<b>10</b>	Extremely high	2	3	per day

<b>Rating</b>	<b>In Service</b>	<b>Manufacturing QC</b>
<b>1</b>	Almost certain	100% automatic inspection (SPC) + routine calibration & maintenance
<b>2</b>	Very high	100% automatic inspection (SPC)
<b>3</b>	High	100% SPC ( $C_{pk}$ 1.33)
<b>4</b>	Moderately high	100% SPC
<b>5</b>	Moderate	some SPC plus 100% final inspection
<b>6</b>	Low	100% manual inspection using go/no-go gauges
<b>7</b>	Slight	100% manual inspection in the process
<b>8</b>	Remote	samples inspected, 100% no defects
<b>9</b>	Very remote	samples inspected by acceptable quality level
<b>10</b>	Almost none	no inspection

Failure Modes and Effects Analysis (FMEA) is discussed by the following authors: Christianson & Rohrbach [1986, pp. 175-6], Dieter [2000, pp. 551-554] [1991, pp. 553-555], McDermott, et. al, [1996], Middendorf [1990, pp. 40-2], Middendorf & Englemann [1998, pp. 46], Pugh [1990, pp. 208-210] and Volland [1999, pp. 326-328].

## **Failure Modes, Effects And Criticality Analysis (FMECA)**

The US Department of Defense has published MIL-STD-1629A [1980] which defines the standard procedures for performing a Failure Modes, Effects and Criticality Analysis (FMECA). FMECA is essentially FMEA with the additional step of evaluating the criticality of each failure mode (a process similar to computing the RPN for each failure mode). The DOD recommends that the FMECA be initiated early in the conceptual design process and updated as the design evolves.

In FMECA, each a failure mode is assigned a probability of occurrence. In the absence of probability data, the following levels may be used:

- Level A **Frequent** – the highest probability of occurrence.
- Level B **Reasonably probable**
- Level C **Occasional**
- Level D **Remote**
- Level E **Extremely unlikely** – the lowest probability of occurrence

Each effect is assigned a severity index (ranking) based on MIL-STD-882, which are listed as follows:

- Category I **Catastrophic** – a failure which may cause death or whole system loss.
- Category II **Critical** – a failure which may cause severe injury, major property damage, or major system damage which results in mission loss.
- Category III **Marginal** -- a failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of system availability or mission degradation.
- Category IV **Minor** -- a failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.

At each design review, the failure modes leading to category I and II severities are discussed.

The criticality analysis ranks each potential failure mode identified according to the combined influence of the probability of occurrence and the severity index. The failure modes with the highest criticality rankings should be addressed first to reduce both the probability of occurrence and the severity of the effect.

## **Fault Tree Analysis (FTA)**

Fault Tree Analysis is a graphical flow charting method that connects potential system faults (failures) to expected outcomes (hazards) using a logic diagram. It was originally developed for analyzing electrical systems. Given fault probabilities, the probability of potential outcomes may be determined. A fault tree is essentially a graphical presentation of a Failure Modes and Effects Analysis.

Middendorf [1998, pp. 45-54] [1990, pp. 42-48] states that FTA starts with the identification of potential hazards in the design. Both hazard to people and property damage are considered. Each potential hazard is depicted as the output block in a logic diagram. Next the combination of faults necessary to produce each hazard are determined. This combination of faults is depicted as a logic circuit ending in the potential hazard. Probabilities for the occurrence of each fault may be assigned and the probability of occurrence of the hazard may be determined by combining the fault probabilities according to the logic diagram.

Fault Tree Analysis (FTA) is discussed by the following authors: Christianson & Rohrbach [1986, p. 176], Dieter [2000, pp. 555-557] [1991, pp. 555-558], Middendorf [1990, pp. 42-48], Middendorf & Englemann [1998, pp. 45-54], Pugh [1990, pp. 211-213] and Voland [1999, pp. 323-326].

### **Hazard Analysis and Critical Control Points (HACCP)**

Hazard Analysis and Critical Control Points (HACCP) [USFDA, 2001] was developed by the Pillsbury Company in 1960 to provide quality control for foods produced for the US space program. It was adopted by the US Food and Drug Administration in 1973 and has since been mandated for many types of food processing industries and medical device manufacturers. There are seven principles of HACCP:

1. Conduct hazard analysis. Prepare a list of steps in the manufacturing process where significant hazards occur and identify preventive measures. Data from risk management tools such as Fault Tree Analysis (FTA), Failure Modes Effects Analysis (FMEA), and Failure Modes Effects Criticality Analysis (FMECA) should be used, if available, to identify the hazards in a HACCP system.
2. Identify the critical control points (CCP). A CCP is a step or procedure at which control can be applied and a safety hazard can be prevented, eliminated, or reduced to acceptable levels.
3. Establish critical limits for preventive measures associated with each CCP identified.
4. Establish CCP monitoring requirements. Establish procedures for using monitoring results to adjust the process and maintain control.
5. Establish corrective actions to be taken when a critical limit deviation occurs.
6. Establish procedures for verification that the HACCP system is working correctly.
7. Establish effective record-keeping procedures that document the HACCP system.

HACCP appears to be an extension to FMEA for processes that identifies specific control points in the process where monitoring and corrective action can be done. It is designed to facilitate government regulatory efforts and therefore requires substantial record keeping.

### **Hazard and Operability Study (HAZOP)**

Hazard and Operability Study (HAZOP) [Voland, 1999, pp. 321-322], developed in the UK for chemical plants, is a team-based, systematic, qualitative method for identifying the hazards involved in process industries. The study begins by considering deviations from the desired performance of the process using guide words such as more, less, none, part of, other than, etc. The team then considers the consequences of each deviation by asking questions such as:

- Will someone be harmed? Who? In which way? How severely?
- Will the processes performance be reduced? In which way? How severely? What will be the impact?
- Will costs increase? By how much?
- Will there be any cascading effects where this deviation leads to other deviations? What are they?

Finally, the team develops an action plan to eliminate or minimize the deviations and their consequences.

Hazard and Operability Study (HAZOP) is discussed by the following authors: Kletz [1991] and Voland [1999, pp. 321-322].

## **Hazards Analysis (HAZAN)**

Hazards Analysis (HAZAN) [Voland, 1999, pp. 322-323], developed in the UK for chemical plants, is a systematic probabilistic analysis method for quantifying the importance of hazards involved in process industries that is usually done by one or two people. HAZAN can be summarized in three basic questions:

- How often? (How often will the hazard occur?)
- How big? (What are the consequences of occurrence?)
- So what? (How important is this hazard compared to all the others?)

Once the hazards are identified, efforts are made to eliminate them or at least to reduce the frequency of occurrence beginning with the most important and continuing to the least important. For those hazards that cannot be completely eliminated, efforts are made to minimize the consequences and warn those potentially affected.

HAZAN appears to be very similar to FMEA. The question “How often?” identifies the probability of occurrence. The question “How big?” identifies the severity of the hazard. The probability of detection is not used in HAZAN. The question “So what?” identifies an overall hazard rating, similar to an RPN, that allows the hazards to be ranked and considered in order of importance.

Hazards Analysis (HAZAN) is discussed by the following authors: Kletz [1991] and Voland [1999, pp. 322-323].

## **Root Cause Analysis**

Root Cause Analysis [Lumsdaine, 1995, p. 16] was developed by the Ford Motor Company to handle problems that arose in their business processes. Ford calls it the 8-D Method because they have defined eight steps as follows:

1. Form a team.
2. Define the problem.
3. Handle the current emergency.
4. Find the root causes of the problem/emergency.
5. Test potential corrective actions and devise the best plan of action.
6. Implement the plan of action.
7. Prevent recurrence of the problem/emergency.
8. Congratulate the team for a job well done.

Obviously the task of finding the root cause of a problem is at the heart of this method. Frequently, checklists are developed and used to assist in this task. Management Oversight and Risk Tree (MORT) is a commonly used checklist for evaluating management involvement in a problem. When appropriate checklists are not available, the team must devise their own using idea generation techniques such as brainstorming.

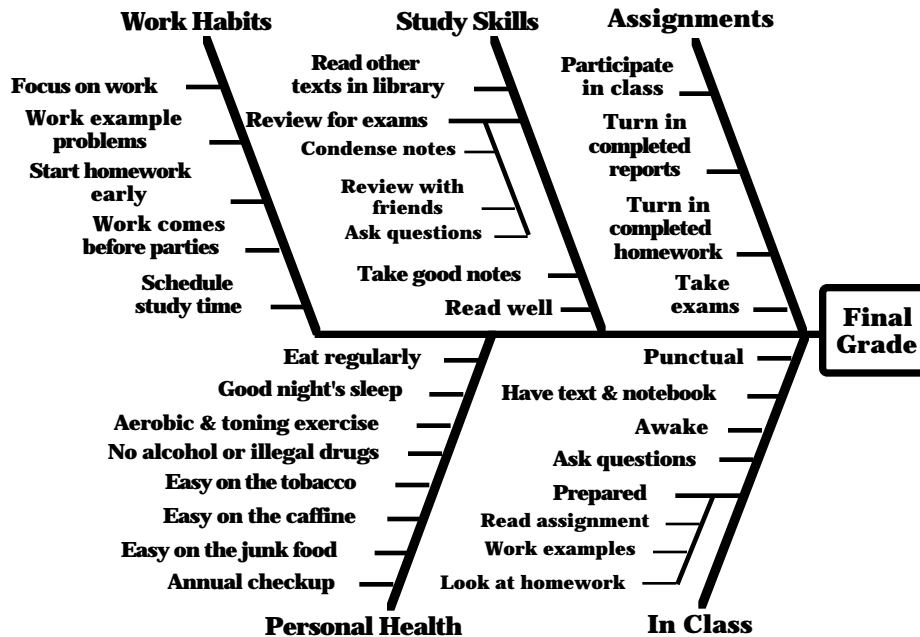
Root Cause Analysis has become a widely accepted tool in quality control circles. It is evident that it can be used to facilitate the process of finding failure modes in the FMEA and FTA methods.

Root Cause Analysis is discussed by the following authors: Lumsdaine [1995, p. 16]

## **Cause and Effect Diagram**

A Cause and Effect Diagram [Ishikawa, 1982], also known as “fishbone” or Ishikawa diagram, is a directed graph connecting potential causes (faults) to an effect (hazard or outcome). It is hierarchical and usually ends up

looking like the skeleton of a fish (hence the name “fishbone” diagram). It is a convenient and useful way to graphically represent a Failure Modes and Effects Analysis, although it is not as quantitative as a fault tree.



**Fig. 2 A Sample Cause and Effect Diagram**

Cause and Effect Diagrams are discussed by the following authors: Dieter [2000, pp. 99-100], Ishikawa [1982], Voland [1999, p. 328].

## **Discussion and Recommendations**

James G. Bralla, a manufacturing consultant, has stated [1996, p. 195] “Safety is a vital issue. From a human standpoint and probably from a cost standpoint as well, it may be the most important consideration of all in product design. Safety during the manufacture, safety during use, and safety after the disposal of the product are all important.”

George Dieter, Dean of Engineering and Professor of Mechanical Engineering at University of Maryland, recommends [1983] that industry engage in more “defensive research” to minimize exposure to litigation. This means that the potential hazards of each product must be identified and an effort made to minimize the risk of injury to the consumer. Every design can be improved and the risk of injury reduced, however, in most cases some hazards cannot be completely eliminated. For those hazards that remain in the product, clearly and simply written warning labels and owner manuals must be written and provided to the consumer.

Juvinall & Marchek recommend [1991] that design engineers make safety an integral part of the product design. As potential hazards are identified, incorporate appropriate safety features into the design. Sometimes this means using an entirely new approach in the product. Provide warning labels and warnings in the user documentation about significant unavoidable hazards that remain in the product.

Shigeo Shingo developed and championed the poke-yoke system [1986] of mistake-proofing the assembly process. It improves safety during manufacturing and product quality by designing the product and assembly process to avoid potential errors, problems and hazards during assembly.

W. Edwards Deming, considered by many to be the father of the modern quality revolution, has stated [1986, p. 396] “I would not participate in any attempt to use cost/benefit analysis for design of product where possible

injury or loss of life is at risk.” Hazards to people should be eliminated where ever possible. Attempting to quantify the cost of injury or death and balance it against potential profits from a consumer product clearly does NOT satisfy the first fundamental canon of the NSPE Code of Ethics for Engineers to hold paramount the safety, health and welfare of the public. Design decisions that affect safety should be made before decisions based on economics.

## **References:**

- Accreditation Board for Engineering and Technology (ABET), 1997, **Code of Ethics for Engineers**, Baltimore, MD, [http://www.abet.org/Code\\_of\\_Ethics\\_of\\_Engineers.htm](http://www.abet.org/Code_of_Ethics_of_Engineers.htm)
- ASME International (American Society of Mechanical Engineers), 1998, **Code of Ethics for Engineers**, New York, NY, (<http://www.asme.org/ame/policies/p15-7.html>)
- Bralla, James G., 1996, **Design for Excellence**, McGraw-Hill, New York. (ISBN 0-07-007138-1)
- Christianson, L. L. and R. P. Rohrbach, 1986, **Design in Agricultural Engineering**, American Society of Agricultural Engineers, St. Joseph, MI. (ISBN 0-916150-80-1)
- Deming, W. Edwards, 1986, **Out of The Crisis**, MIT Center for Advanced Engineering Studies, Cambridge, MA. (ISBN 0-911379-01-0)
- Dieter, George E., 2000, **Engineering Design**, 3<sup>rd</sup> ed., McGraw-Hill, New York. (ISBN 0-07-366136-8)
- Dieter, George E., 1991, **Engineering Design**, 2<sup>nd</sup> ed., McGraw-Hill, New York. (ISBN 0-07-016906-3)
- Dieter, George E., 1983, **Engineering Design**, McGraw-Hill, New York. (ISBN 0-07-016896-2)
- Ertas, Atilla and Jesse C. Jones, 1993, **The Engineering Design Process**, Wiley, New York. (ISBN 0-471-51796-8)
- Ishikawa, K., 1982, **Guide to Quality Control**, Quality Resources, White Plains, NY.
- Juvinall, R. C. & K. M. Marchek, 1991, **Fundamentals of Machine Component Design**, 2<sup>nd</sup> ed., Wiley, New York. (ISBN 0-471-62281-8)
- Kletz, T. A., 1991, **HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards**, 3<sup>rd</sup> ed., Institution of Chemical Engineers, Rugby, Warwickshire, UK.
- Lindbeck, John R., 1995, **Product Design and Manufacture**, Prentice Hall, Upper SaddleRiver, NJ. (ISBN 0-13-034257-2)
- Lumsdaine, Edward & Monika Lumsdaine, 1995, **Creative Problem Solving**, McGraw-Hill, New York. (ISBN 0-07-039091-6)
- Matson, J. V., 1991, **The Art of Innovation: Using Intelligent Fast Failure**, Penn State University, University Park, PA.
- McDermott, R. E., R. J. Mikulak and M. R. Beauregard, 1996, **The Basics of FMEA**, Productivity, Portland, OR. (ISBN 0-527-76320-9)
- Middendorf, W. H. and R. H. Englemann, 1998, **Design of Devices and Systems**, 3<sup>rd</sup> ed., Marcel Dekker, New York. (ISBN 0-8247-9924-0)
- Middendorf, W. H., 1990, **Design of Devices and Systems**, 2<sup>nd</sup> ed., Marcel Dekker, New York. (ISBN 0-8247-8281-1)
- MIL-STD-1629A, 1980, **Military Standard Procedures For Performing A Failure Mode, Effects And Criticality Analysis**, Department of Defense, Washington, DC. (<http://users.compaqnet.be/cn099845/MILSTD1629.htm>)
- National Society of Professional Engineers (NSPE), **Code of Ethics for Engineers**, Alexandria, VA, (<http://www.nspe.org/ethics/eh1-code.asp>)
- Pugh, Stuart, 1990, **Total Design: Integrated Methods for Successful Product Engineering**, Addison-Wesley, Reading, MA. (ISBN 0-201-41639-5)
- Shingo, Shigeo, 1986, **Zero Quality Control: Source Inspection and the Poka-Yoke System**, Productivity Press, Stamford, CT. [ISBN 0-915299-07-0]
- Taguchi, Genichi, Elsayed A. Elsayed & Thomas Hsaing, 1989, **Quality Engineering In Production Systems**, McGraw-Hill, New York. (ISBN 0-07-062830-0)
- US Food and Drug Administration, Center for Devices and Radiological Health, 2001, **Hazard Analysis and Critical Control Points (HACCP) Inspections**, (<http://www.fda.gov/cdrh/gmp/haccp.html>)
- Voland, Gerald, 1999, **Engineering by Design**, Addison Wesley, Reading, MA. [ISBN 0-201-49851-0]