Risk and Fault Tolerance Analysis for Robotics and Manufacturing

D.L. Hamilton, J.R. Cavallaro, and I.D. Walker
Department of Electrical and Computer Engineering
Rice University
Houston, Texas 77251-1892 USA
(713) 527-4020

Abstract

This paper describes a novel method for analyzing, within one framework, several important types of risk associated with robotics and manufacturing applications. We will build on the established technique of Fault Tree Analysis to analyze the risk/benefits of the physical process, and extend the concept to build a dual structure for environmental costs/benefits. In addition, our framework includes the ability to perform financial cost-benefit analyses.

1 Introduction

Various methods for analyzing engineering risk and safety have been established over the years. For example in robotics, the issue of fault tolerance has been an active research area recently [15]. A number of valuable techniques have been developed, including modular fault tolerant environments [1, 6, 12] and the analysis of redundant and safety systems [11, 13, 16, 17].

Use of these techniques would reduce the engineering risk associated with robotics applications. However, there has been little work in analyzing the cost (both financial and environmental) of applying new methods in a given application.

Currently there is a surge of interest in the area of Environmentally Conscious Manufacturing (ECM) [8, 9, 10]. This activity is producing a series of potentially valuable methods [2, 3]. However, progress to date has been somewhat piecemeal and application-specific. Both engineers and managers are often reluctant to accept and adopt new environmentally conscious techniques without some rigorous justification of their systemwide effectiveness.

One difficulty at present is the lack of an accepted method, based on solid scientific principles, which can be applied by engineers and management alike to evaluate the impact of a proposed new ECM strategy. Managers would like an easily understandable "big picture" tool clearly showing the interrelationships between engineering subsystems, with a principles-based numerical capability showing the effects of change [5]. Engineers would appreciate tools which show, qualitatively and quantitatively, how their portion of the system affects, and is affected by the overall system and other subsystems. In addition, financial strategists would like to explicitly include the economic impacts involved in the design or alteration of a process [4]. In particular, a commonly accepted technique which could be used to clearly demonstrate the benefits (or not) of a new ECM strategy to all those parties involved in the decision-making process would be a major step forward.

This paper will describe a new formal model relating the physical process with the engineering, environmental, and financial risks and/or benefits associated with both robotics and manufacturing strategies.

The core of our approach is the use of fault trees to initially model the system. Fault trees provide an excellent method to link the failure modes of complex interdisciplinary systems [14], and have been used successfully recently in robotics [15] to analyze the reliability and fault tolerance capabilities of robots for hazardous environments.

Using the fault tree base, conventional engineering reliability and risk assessments can initially be made for a given process and technology. The next phase of our approach is to augment the basic structure of the fault trees with cost/benefit information. Each node of the fault tree base is augmented with a field giving the environmental cost/benefit related to the subsystem corresponding to that node. A further field, representing financial cost/benefit is then added to the structure at each node. This whole tree 'grows' and 'shrinks' with changes to the engineering system.

This framework is useful in that the structure allows the user to assess the effect of changes in the system on the overall cost of the process. This can be used, for example, to assess the potential cost/benefits of employing environmentally conscious manufacturing strategies. In addition, the method can be used to evaluate the cost/benefit of adopting new technologies, such as fault tolerance strategies in robotics.

0-7803-31-09-5/96/$5.00

1.1 System Analysis

A key issue is the inherent complexity involved in, and the strongly interdisciplinary nature of, most robotics and manufacturing applications. It is not easy for any one person, even those who are experts in part of a process, to appreciate the systemwide effects of changes in a given part of the process. This is true for traditional applications, and becomes even more so in the case when additional environmental considerations are added to the mix.

Consider a typical manufacturing problem where raw materials are selected, mixed, and then heated to produce a final product. Figure 1 shows a basic process flow for this system where an operator interfaces with a control computer that has been programmed to operate the manufacturing equipment. In our first example below, we will apply this structure to an automotive PCV system, including the environmental effects. Environmentally Conscious strategies can be

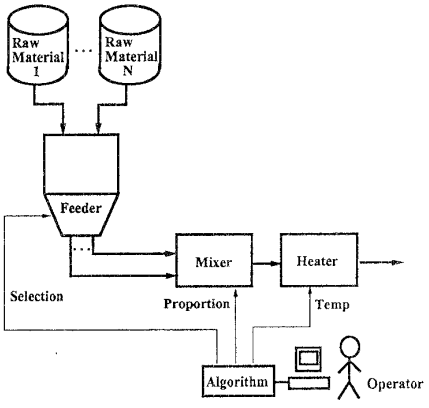

Figure 1: Typical materials processing scenario.

applied to a number of manufacturing processes. In many cases, they may relate to the actual manufacturing of a product. In a broader view, ECM can also be applied to the daily operation of a product or to a decontamination and decommissioning activity.

We now discuss an example relating to the design of a system to control hydrocarbon (HC) emissions from an automobile. In this scenario, the product is motion of the vehicle and the raw materials are gasoline and air. In this regard, the automobile is an ECM system that has been evolving and improving over the last thirty years. The present day automobile has a number of systems that control the emission of hydrocarbon, carbon monoxide, and nitrous oxides. We will concentrate on one example system, the positive crankcase ventilation system (PCV) that seeks to reduce the amount of harmful crankcase HC blow-by gases that are a by-product of normal engine operation. Before emission controls were used, these gases were directly vented to the atmosphere. In current PCV systems, these blow-by gases are recovered and recycled by mixing with fresh air before combustion. A basic mechanical PCV valve is used to control the mixing process. Figure 2 shows a schematic view of the PCV system. In the following, we will analyze

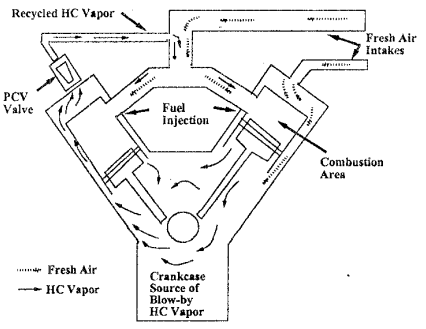

Figure 2: Conceptual automobile PCV process flow.

this current system for reliability, economic cost, and environmental cost. We will discuss the feedback and coupling which exists between these different views of the system and discuss methods by which a proposal for an improved electro-mechanical PCV valve may be evaluated by engineers and managers.

1.1.1 Background: Fault Tree Analysis

We will begin by adopting and extending the existing widely used technique of Fault Tree Analysis (FTA) [14]. FTA is a logical and deductive technique that has been widely applied to analyze reliability and risk in various engineering applications. FTA first logically represents the interrelationships of portions of a system in a graphical fault tree. In a fault tree, a top level system failure is first identified for study. The fault tree is a collection of logical AND and OR gates that relate primary fault events to the top level system failure. FTA also facilitates a numerical evaluation of subsystem effects (typically reliability calculations) on other subsystems and the overall system. Thus FTA provides both qualitative and quantitative information about the system of interest.

One key advantage of FTA is that fault trees allow straightforward graphical and numeric representation of highly complex and interdisciplinary systems, with experts in the various subsystem areas contributing to the subtrees representing those subsystems. Thus those persons with the appropriate expertise contribute to, and have their expertise represented in, the overall model. The possible benefits (or risks) inherent in a system design or implementation can typically be clearly seen and analyzed using

FTA. In the work outlined below, we adopt the fault tree approach, and extend it to explicitly allow the inclusion of both environmental and economic risks and benefits for ECM strategies. Our approach does not assume any underlying type of engineering process, hence our results will be applicable across a wide range of applications.

1.1.2 FITTER-ECM Strategy

The underlying strategy behind our approach builds around the disciplines of Fault Tree analysis [14]. We term our proposed strategy the Framework for Integrated Trees and Teamwork for Emissions Reduction (FITTER) for Environmentally Conscious Manufacturing. This FITTER-ECM approach is shown in Table 1 for the automobile PCV example introduced above. There are four units that comprise FITTER: organizational, economic cost, engineering risk, and environmental cost. These units could be expressed in a tree formation that demonstrates their interrelation (as in Figure 3). We stress the interaction and coupling between the various units for a particular element in a manufacturing system. The FITTER-ECM organizational units are derived from the generic processing system described in Figure 1. In tree formation, the two main branches correspond to the raw materials and the control and equipment portions of the manufacturing process.

The tree for each unit would have the same configuration, with the appropriate element from Table 1 included. The fault tree in Figure 3 shows the structure of the trees with the addition of gates for analysis of the engineering risk. The primary fault events at the leaves of the tree, include faults such as a stuck PCV valve, poor driving style, or worn piston rings. Failure probability information can be added to this tree for a quantitative analysis.

The economic cost column for this system contains information on part costs and operational costs. The top level cost results from combining together the cost of each of the leaves. Most of the costs in this tree are positive expenditures. However, it can be envisioned that through re-cycling, some of the costs may be negative. In this example, there may be a modest negative cost gained by using the recovered crankcase HC vapors as fuel within the engine.

The final column in the FITTER-ECM strategy attempts to capture the environmental costs associated with HC pollution in this particular emission control subsystem. In this example, the various primary events range from harmful environmental costs, such as the HC vapor source of the engine crankcase, through nominal environmental costs, such as the driver and the air consumed, to helpful environmental costs due to re-cycling the HC vapors.

Our FITTER-ECM strategy, (Table 1) which is tailored to specifically couple environmental analysis with the more traditional concerns is a completely new approach for ECM systems. The elegance of FITTER-ECM lies in its simplicity (all four units are built around the anatomy of the physical process). In the next section, we combine the individual analyses to provide an overall effectiveness measure, which could prove valuable for comparison of systems [7].

2 Risk/Cost/Benefit Analysis

In the above section we introduced the tree framework that relates reliability with economic and environmental costs. We now extend the risk/cost/benefit analysis methods to address numerical quantification of overall systems. Here we seek to efficiently analyze a number of "what if" scenarios that cross all units within the framework. Various possibilities in manufacturing systems can be compared in terms of their effectiveness - as defined by the system designers. The goal is to provide feedback between the various units. This will aid engineers and managers in improving all aspects of the system.

The overall effectiveness of a given system is a function of various units that may impact each other. For example, addition of re-cycling capabilities improves the environmental value of a system, but raises the cost for the same basic functionality. The overall effectiveness of a system can be measured using an equation of the form:

$$eff = k_1 v_C + k_2 v_E + k_3 f_t + k_4 p \qquad (1)$$

where:

eff	is the effectiveness rating,
v_C	is the economic value (inverse cost) rating,
v_E	is the environmental value (inverse cost) rating,
f_t	is the fault tolerance rating,
p	is the performance rating, and
k_1, k_2, k_3, k_4	are constants reflecting relative importance of terms.

This general equation can be applied to a variety of systems, with the terms being chosen appropriately for the system being analyzed [7]. For example, the performance might be speed for one system and volume for another. Whatever performance is measured would be mapped to a rating that ranges $[0, 1]$. The remaining three terms also have values in the range $[0, 1]$. Determining the economic and environmental costs at the top level of the tree would simply require summing the costs (some negative) at each level. The cost ranges (determined by the designers) would be mapped to the $[0, 1]$ range to get the economic and environmental value ratings. A term that is not applicable to the given case, such as fault tolerance for the PCV valve example, would have a coefficient of zero. The constants are real numbers ranging in $[0, 10]$ whose sum is ten. These coefficients are chosen to indicate the relative importance of the ratings.

For the PCV valve example, the crankcase source could provide a negative economic cost (positive

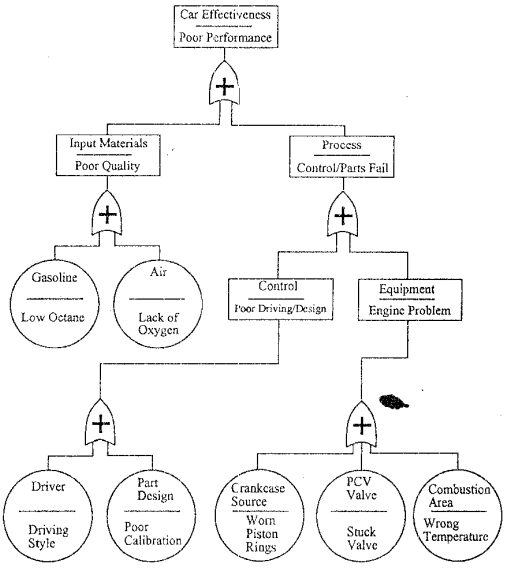

Figure 3: Engineering fault tree unit for PCV valve example.

value), while the remaining elements (except air) increase the cost. Similarly, the only contributors to HC pollution in the environmental cost tree are gasoline, the crankcase source, and perhaps the part design. Re-cycled HC vapors provide a negative contribution via the PCV valve, and the remaining leaves do not affect HC pollution.

The FITTER-ECM framework could be expanded to consider the more complex issue of design optimization for ECM strategies. We believe that the critical mix of disciplinary units in FITTER-ECM will provide an ideal platform with which to analyze such issues. Essentially, design optimization involves simultaneously considering multiple "what-if" situations involved in critical event analyses.

For example, to return to the PCV example, one could consider three alternatives with respect to the emission of hydrocarbon vapors from the engine crankcase. Before the requirement of emission controls, the HC vapors were simply vented to the atmosphere through a draft tube. This resulted in a system with no economic cost, no maintenance or reliability risks, but with high environmental cost. Most current day PCV systems have moderate economic cost, moderate maintenance or reliability risks, and low environmental cost. The FITTER-ECM framework could be expanded to consider a number of "what if" scenarios, such as replacing the mechanical PCV system with a computer controlled self-cleaning electro-mechanical PCV system. The analysis would then study the cost and benefits resulting from higher economic cost, possibly lower reliability risk, and lower environmental cost due to more accurate mixing of the blow-by HC vapors under various engine load conditions.

Finally, we present a waste disposal system example to demonstrate the use of the effectiveness measure. The waste water from a home is sent into a septic tank. Chemicals in the tank break down the solid waste into a more liquid form. The remaining solid mass is deposited at the bottom of the tank, and the liquid flows into a filter bed. The filter bed contains sand through which the liquid waste is filtered. The liquid that exits the filter bed is waste-free water. On occasion, the filter bed may become clogged. When this happens, unprocessed sewage may seep into the ground. In the schematic shown in Figure 4, a second filter bed has been added to compensate for a single filter bed failure (to provide fault tolerance). A sensor system has also been added to provides some fault tolerance at the top level. The filter bed(s) can be manually unclogged if the sensor system indicates that they are full, avoiding seepage of raw sewage into the environment. Table 2 lists the economic, environmental, and risk factors for the waste disposal system, and the fault tree structure is included in Figure 5.

The economic and environmental cost at the top level of the tree is the sum of the costs seen in the leaves. The fault tolerance rating at point X in the tree is 1/2 because one component (filter bed) can fail without resulting in system failure. Since there is only one sensor and one signal, the fault tolerance rating at point Y is 0. The AND gate at the top level indicates

Table 1: Multi-Dimensional Tree Structure.

Organizational Unit	Economic Cost	Engineering Risk	Environmental Cost
Car Effectiveness	Cost of Operation	Poor Performance	HC Pollution
Input Materials	Cost of Materials	Poor Quality	Contained HC Vapor Source
Gasoline	Cost per Gallon	Low Octane	Contained HC Vapor Source
Air	Air Cost - Free	Lack of Oxygen	No HC Vapors
Process	Running Cost	Control/Parts Fail	Probable HC Source
Control	Wages/Design Cost	Poor Driving/Design	Possible HC Source
Driver	Wages per hour	Driving Style	No HC Vapors
Part Design	Design Cost over time	Poor Calibration	Variable w/ Design
Equipment	Hardware Cost	Engine Problem	Probable HC Source
Crankcase Source	Recoverable By-product	Worn Piston Rings	HC Vapor Source
PCV Valve	Part Cost	Stuck Valve	Re-cycle HC Vapors
Combustion Area	Engine Cost per revolution	Wrong Temp	No HC Vapors

Table 2: Waste Disposal System Example.

Organizational Unit	Economic Cost	Engineering Risk	Environmental Cost
T - filter bed 1	Cost of installation (C_1) Cost of maintenance (C_2)	Clogging	Installation impact (E_1) Operational impact (E_2)
U - filter bed 2	Cost of installation (C_1) Cost of maintenance (C_2)	Clogging	Installation impact (E_1) Operational impact (E_2)
V - full tank sensor	Cost of sensor (C_3)	sensor failure	none
W - full tank signal	Cost of signal (C_4)	signal failure	none
X - filtering system failure		$f = 1/2$	
Y - sensor system failure		$f = 0$	
Z - exposure of raw sewage	$C = 2(C_1 + C_2) + C_3 + C_4$	$f_t = 2^{-1}(1/2) + 2^{-2}(1/2 + 0)$	$E = 2(E_1 + E_2)$

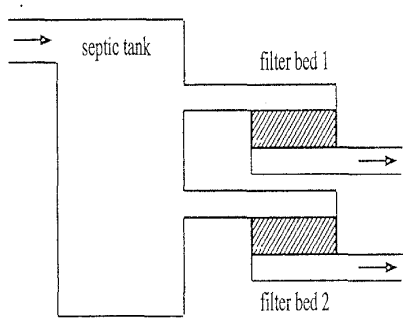

Figure 4: Waste disposal system.

fault tolerance for the top event. Again, since there are two inputs to the AND gate, the fault tolerance level is 1/2. The final fault tolerance rating for the system sums the ratings for the lower levels, multiplied by constant coefficients. These coefficients are chosen to be 2^{-i} for this example, where $i = 1$ at the highest level and decreases by one for each level leading to the leaves. The final effectiveness rating would be determined using the equation presented above, with the constants k_i determined by the design engineers.

3 Conclusions

We have introduced a method for analyzing, within one framework, several important types of risk associated with robotics and manufacturing applications. The approach is based on a tree structure,

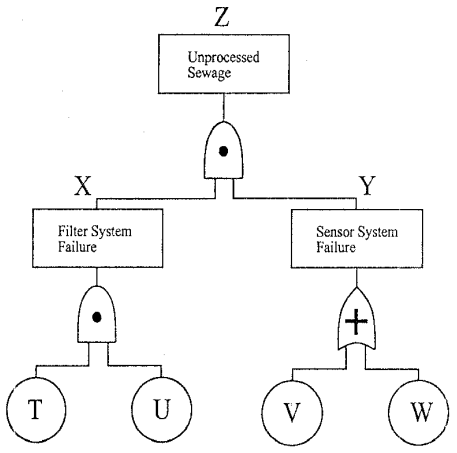

Figure 5: Waste disposal system tree.

which includes a Fault Tree Analysis to analyze the risk/benefits of the physical process. The concept is extended to build a dual structure for environmental costs/benefits. The ideas are demonstrated via some simple examples.

Acknowledgements

This work was supported in part by NASA Graduate Fellowship NGT-70251, in part by the National Science Foundation under grant IRI-9526363, and in part by DOE Sandia National Laboratory Contract #AL-3017.

References

[1] A. Adlemo and S.A. Andreasson. Fault Tolerance Aspects in Computerized Systems. In *Proceedings 7th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pages 1024–1028, Antalya, Turkey, 1994.

[2] S.B. Billatos and V.V. Nevrekar. Challenges and Practical Solutions to Designing for the Environment. In *Design for Manufacturability*, pages 49–64, ASME, DE-Vol. 67, 1994.

[3] W.J. Brady. Environmentally Conscious Products. In *IEEE/CHMT European International Electronics Manufacturing Technology Symposium*, pages 278–279, San Francisco, CA, 1992.

[4] A.C. Butler. A Discussion of Accounting Theory from an Engineering Design and Manufacturing Perspective. In *Design for Manufacturability*, pages 77–87, ASME, DE-Vol. 67, 1994.

[5] E. Callenbach, F. Capra, L. Goldman, R. Lutz, and S. Marburg. *Ecomanagement.* Berrett-Koehler Publishers, 1993.

[6] D.L. Hamilton, M.L. Visinsky, J.K. Bennett, J.R. Cavallaro, and I.D. Walker. Fault Tolerant Algorithms and Architectures in Robotics. In *Proceedings 7th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pages 1034–1036, Antalya, Turkey, 1994.

[7] D.L. Hamilton, I.D. Walker, and J.K. Bennett. Fault Tolerance versus Performance Metrics for Robot Systems. to appear, Proceedings 1996 IEEE International Conference on Robotics and Automation, Minneapolis, MN, April 1996.

[8] M. Hattori, N. Nomura, D. Sommer, and H. Inoue. Fundamentals of Environmentally Conscious Product Design. *International Journal of Environmentally Conscious Design and Manufacturing*, 4(1):3–12, 1995.

[9] P. Johansson. *Cost-Benefit Analysis of Environmental Change.* Cambridge University Press, 1993.

[10] E. Kjeldgaard. Waste Minimization Makes Good Business Sense. *International Journal of Environmentally Conscious Manufacturing*, 1(1):75–84, 1992.

[11] C. Lewis and A.A. Maciejewski. Dexterity Optimization of Kinematically Redundant Manipulators in the Presence of Joint Failures. *Int. Journal of Computers and Electrical Engineering*, 20(3):273–288, 1994.

[12] C. Paredis, A. Au, and P. Khosla. Kinematic Design of Fault Tolerant Manipulators. *Int. Journal of Computers and Electrical Engineering*, 20(3):211–220, 1994.

[13] D. Sreevijayan, S. Tosunoglu, and D. Tesar. Architectures for Fault-Tolerant Mechanical Systems. In *Proceedings 7th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pages 1029–1033, Antalya, Turkey, 1994.

[14] W.E. Vesely, F.F. Goldberg, N.H. Roberts, and D.F. Haasi. *Fault Tree Handbook.* NUREG 0492, Systems and Reliability Research Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C., 1981.

[15] M.L. Visinsky, J.R. Cavallaro, and I.D. Walker. Robotic Fault Detection and Fault Tolerance: a Survey. *Reliability Engineering and System Safety*, 46(4):139–158, 1994.

[16] M.L. Visinsky, J.R. Cavallaro, and I.D. Walker. A Dynamic Fault Tolerance Framework for Remote Robots. *IEEE Transactions on Robotics and Automation*, 11(4):477 – 490, 1995.

[17] T. Wikman, M. Branicky, and W. Newman. Reflex Control for Robot System Preservation, Reliability, and Autonomy. *International Journal of Computers and Electrical Engineering*, 20(5):391–407, 1994.