

# 1.0 Introduction

The California PATH (Partners for Advanced Transit Highway) project is a collaborative effort between industry, academia, and the public sector to develop more efficient transportation systems. The California PATH project was established in 1986 by the California Department of Transportation and the Institute of Transportation Studies at the University of California, Berkeley to investigate the applicability of advanced highway automation, communication and roadway electrification technologies.

The goal of PATH is to increase the capacity of the most frequented highways thus decreasing traffic congestion, air pollution, accident rates and fuel consumption. Current research is being done to develop an IVHS (Intelligent Vehicle Highway System) which will improve traffic conditions on highways. Critical to a successful IVHS is safety; a safe automated system relies on the use of sensors to conduct such varied tasks as longitudinal control, lateral control, and maneuvering techniques. The reliability of these sensors is crucial to successful operation of the IVHS to ensure a safe environment for human beings.

In the IVHS vehicles are to travel in a platoon, a group of one or more cars, with approximately a one meter separation between cars. In order to achieve close vehicle proximity and high speeds it is necessary to remove control from the human and hand it over to computer controller systems such as AVCS (Advanced Vehicle Control Systems). The rate of travel of a platoon is determined by various conditions including the presence of another platoon, the detection of an approaching object, and road conditions. AVCS is a multi-faceted research area including Safety Warning Devices, Active Sensing Devices, and the Automated Highway System (AHS). The Automated Highway System component controls the longitudinal motion, lateral motion, acceleration, and deceleration of all the vehicles.

## 1.1 Project Objective

The longitudinal motion controller in the AHS controls maneuvers such as platoon merging and splitting. The sonar and radar sensors are components of the longitudinal motion controller which provide information about the vehicle separation distance between cars or approaching objects. There are certain external conditions which alter the sensor's performance. Research has been conducted exploring environmental conditions (e.g. rain, fog, snow) effects on the sensors. The current focus is on analyzing the sensor systems and determining all possible failure modes using Fault Tree Analysis. Knowledge of all possible failure modes and their characteristics can assist in anticipating future failures. Thus, hazardous situations on the highway can be averted. The safety of the Intelligent Vehicle Highway System as a whole will be improved.

# 2.0 Hazard Characterization

## 2.1 Safety Concerns

It is necessary that the Intelligent Vehicle Highway System be at least as safe as the current highway system. Ordinary traffic casualties are 90% associated with some kind of human error (Hitchcock, A., 1992), but in IVHS humans will no longer be in control of their own vehicles. In the IVHS environment where there is such a dependency on sensor performance, a sensor component failure can lead to catastrophic situations. It has been hypothesized that in the IVHS the number of accidents will decrease and the number of vehicles involved with accidents will decrease, but the mean number of vehicles involved in an individual accident will increase. Similarly, the number of fatal accidents will decrease

and the number of fatalities will decrease, but the mean number of fatalities per fatal accident will increase (Hitchcock, A., 1992).

## 2.2 Hazard Characterization

Hitchcock has done extensive research in the area of hazard characterization and has defined a hazard as a precursor to a condition in which one further failure could lead to a catastrophe. A catastrophe is a high speed collision between platoons where multiple deaths and injuries are likely. In Hitchcock's exhaustive set of hazards that can lead up to catastrophes, he presented the following situations.

A collision is likely to occur:

a) when all platoons involved are under control, automated or manual; in this case vehicles were too close before a final control failure

**Hazard 1:** A platoon is separated from one ahead of it, or from a stationary object in its path, by less than platoon spacing.

**Hazard 2:** A vehicle, not under system control is at an unmeasured or unknown distance in front of a platoon.

(b) when one platoon is not under control; this will happen if automatic control is switched off before the driver is ready, or not switched on when the driver lets go

**Hazard 3:** A vehicle is released to manual control before the driver has given a positive indication that he/she accepts it.

**Hazard 4:** a vehicle is released to manual control at less than manual spacing from the vehicle ahead of it; or at such a relative speed that manual spacing will be realized in less than 2 seconds, or while the brakes are being applied.

(c) when the final failure is a failure to brake or to communicate that brakes should be applied

**Hazard 5:** a vehicle under automatic control is in such a condition that if instructed from the infrastructure to brake, it will not do so.

## 3.0 Longitudinal Motion Controller

### 3.1 Sensor Function

The sonar and radar sensors are components of the longitudinal distance controller which controls the distance between vehicles in the platoon. The sensors, mounted on the grill, measure the distance from a vehicle or an approaching object. Both sensors use the same underlying physical principal to measure the separation distance. They emit a signal which is reflected by a target (target refers to either object or vehicle) within the sensor range; the reflected signal, or echo, is then received by the sensor. The time for the signal to travel to the target and return as an echo is recorded. Then the known velocity of the pulse propagation is used to convert the output to distance by a data acquisition system.

### 3.2 Sensor Behavior

Radar and sonar sensors are susceptible to the external conditions under which they operate; conditions such as rain, fog, and humidity have a certain effect on sensor output. The research done by Bellm includes a series of experiments conducted on the longitudinal controllers in sub-optimal environments. Bellm quantitatively characterized the effects of the environment on sensor output (Table 1). This information facilitates sensor failure prediction because the symptoms of the failure are known.

	<b>Radar Sensor Output</b>	<b>Sonar Sensor Output</b>
<b>Power Line</b>	constant 2.20m	constant -0.85m
<b>Data Line</b>	constant 4.25m	constant 2.20m
<b>Dirt</b>	mean: 1.5m<<2.5m	constant 0m
<b>Fog</b>	not significantly affected	variance increased by factor of 4
<b>Rain</b>	variance increased by factor of 4	variance increased by factor of 4
		mean increased by 10%
<b>Plastic</b>	variance increased by 20%	constant 0m
<b>Vibration</b>	variance increased by 20%	not significantly affected

**Table 1: Characterization of Sonar and Radar Behavior (Bellm, R, 1995)**

## 4.0 Failure Analysis

### 4.1 Motivation for Failure Analysis

There are several qualitative and quantitative methods established for exploring failure modes and the reasons for which they occur. Fault Tree Analysis provides both the benefits of a qualitative and quantitative analysis through a graphical tool that focuses on a failed state and provides a method for determining the causes of the failed state. After completion of the fault tree, Boolean Algebra can be used to determine the minimum number of component fault combinations that will lead to sensor failure.

### 4.2 Fault Tree Analysis

The Fault Tree Analysis Method (Vesely, W.E et al, 1981) focuses on failure because a failed state is generally easier to characterize than is a successful state. The basic elements of the Fault Tree method depict the logical interrelationships of basic events that lead to the undesired event (failed state) of the fault tree. There are entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. Gates show the relationships of events needed for the occurrence of a "higher" event (outputs to the gate). Gate symbols denote the relationship between the input events and the output event.

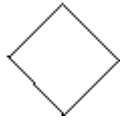
The component fault categories are classified as primary, secondary, and command. A primary fault is any fault of a component that occurs in an environment for which the component is qualified (e.g. defect). A secondary fault is a fault of a component that occurs in an environment for which it has not been qualified. A command fault is a fault where there is proper operation of a component but at the wrong time or in the wrong place. Fault Tree Symbols and their descriptions are illustrated in Figure 1.

The Fault Tree is complete when all possible occurring events have been exhausted and all the branches terminate with either a basic event or an undeveloped event. Boolean algebra can then be used to quantitatively determine the smallest combination of component failures which lead to system failure.

#### **Primary Events:**



Basic Event: A basic initiating fault requiring no further development.



Undeveloped Event: An event which is not further developed

because it is of insufficient consequences

or because information is unavailable.

### Intermediate Event Symbols:



Intermediate Event: A fault event that occurs because of one or more antecedent causes acting through logic gates



Transfer in/out: indicates that the tree is either developed further on

another page or is the continuation of a tree from a

previous page.

### Gate Symbols:



OR: Output fault occurs if at least one of the input faults occurs



AND: Output fault occurs if all of the input faults occur

Figure 1: Basic Fault Tree Symbols (Vesely, W.E, et al, 1981)

## 5.0 Results

Failure analysis was performed on the longitudinal motion controller to predict faults that could later lead to catastrophic failure. Fault Tree Analyses were conducted on sonar and radar sensors. The faults predicted dealt with component failure and operation in sub optimal conditions that could possibly lead to system failure. The results from the fault tree analyses (Figures 2-8 in Appendix) can be used to anticipate further failure and most importantly, hazards. The component faults derived from the trees can be considered symptoms for types failures that lead to specific hazards.

### 5.1 Fault Tree Analysis of Radar Sensor

For the radar sensor the failed state is described as "Radar Sensor output is not close to the true distance." The next step was to determine how to further expand on this failure. Three separate events, connected by the logic gate "OR" re-express the failure.: primary fault (defect), secondary fault, and

command fault.

The primary fault is defined as a defect internal to the sensor, most likely occurring with the electrical components. The resulting outcome of any electrical component failure is a sensor output equal to the maximum or minimum of that sensor.

The command fault has been defined for this purpose as either a power failure or a data line failure of the longitudinal motion controller. For a data line failure the observable characteristic of the output is approximately constant at 4.25m and for a power failure the output is around 2.2m.

The secondary fault can be re-expressed by two events connected by the logic "OR" gate. "Radar Sensor Failure due to environmental clutter" and "Radar Sensor Failure due to range limitations" further describe the intermediate event. "Radar Sensor Failure due to range limitations" is shown as an undeveloped event, where causes of failure cannot be determined due to lack of information of sensor characteristics or observations. The intermediate event of "Radar Sensor Failure due to environmental clutter" can be described by two intermediate events and an undeveloped event. The RSF due to corrosive effects is an attempt to describe the sensor performance near the ocean or any environment where corrosive agents are in the air and can possibly affect the integrity of the electrical components and lead to degradation. This event cannot be described further and is therefore considered an undeveloped event.

The weather and rugged road conditions describe the intermediate event of environmental clutter. They are connected by the logic "OR" gate. In terms of weather conditions, rain, snow and humidity have shown to have adverse affects on sensor performance. Rain can be affect the sensor output in two ways, internally the moisture can cause a power failure and externally the sensor signal can be attenuated by the water drops. Both of these intermediate events can be characterized by basic observations. The moisture can be predicted by a constant output of 2.2m and the attenuation can be predicted by an increase of variance by a factor of four. Snow is the cause of similar results. The moisture from the snow can again internally affect the electrical components and the same prediction can be made (output of 2.2m). The snow can also reflect the sensor signal in which case the basic observation is that the output mean between 1.5m and 2.5m. The humidity in the highway environment may cause internal damage to the sensor in the same manner that the moisture from the rain and snow cause damage.

The road conditions describing radar sensor failure are road clutter, rugged road conditions, and road course. The three events are connected by the logical "OR" gate. The course failure refers to an event on the highway that results in a loss of communication between cars in a platoon, such as a round bend or a pothole in the road where the sensor signal emitted is not aimed at the car ahead of it. The rugged road conditions can result in a vehicle vibration in which case, the observed characteristic in the sensor output would be an increase in variance by 20%. The road clutter can be further described as "Radar Sensor Failure due to debris covering the sensor" and "Radar Sensor Failure due to debris from the road environment." The two intermediate events are linked by the logical "OR" gate. The debris covering the sensor has an observable effect on the sensor output; the sensor mean is between 1.5m and 2.5m. The debris from the road can have any effect on the sensor output and cannot be clearly described and for this reason it has been left as an undeveloped event.

## **5.2 Fault Tree Analysis of Sonar Sensor**

The sonar sensor fault tree analysis is quite similar. The undesired top event is "Sonar Sensor Failure: the output is not close to the true distance." The three intermediate events, primary (defect), secondary,

and command fault further describe the top fault and are logically connected by the "OR" gate.

The primary fault is defined as a defect internal to the sensor, most likely occurring with the electrical components. The resulting outcome of any electrical component failure is a sensor output equal to the maximum or minimum of that sensor.

The secondary fault is associated with a proper operation of a component but in environments for which it was not designed for. The two intermediate events are connected by the logical "OR" gate. Sonar Sensor Failure due to the environment or due to range limitations describe two circumstances for which the sensor was not designed for. The observable characteristic of range limitation for the sonar sensor is a default value of 15m when out of range. Similar to the radar sensor, the environmental fault can be further described by weather conditions, road conditions, and corrosive effects. These events are connected by the logical "OR" gate. Corrosive effects again refers to the affects of the electrical components of the sensor in an atmospheric environment where corrosive agents are present. However, further information about the effect on the output of the sensor and thus, this remains an undeveloped event. The weather and road conditions can be defined more completely.

The weather conditions affecting the sonar sensor are rain, snow, humidity, and fog. The moisture in the rain can possibly short out the electrical component in which case the sensor output would be show outliers at +2m. Water drops from the rain can also serve to attenuate the signal and the variance in the output would increase by a factor of four and the mean would increase by 10%. Snow has a similar effect. The moisture can affect the sensor internally in which case the output would show outliers at 2m. The snow covering the sensor would result in a constant output of 0m. Humidity and fog have the same affect that the moisture has, it may damage the sensor internally and result in an output with outliers at 2m.

The road conditions which affect the sonar sensor performance are road clutter and course condition. The road clutter can be either debris covering the sensor or debris from the highway environment. The debris covering the sensor would result in a constant output of 0m while the characteristics for the sensor signal hitting random debris from the highway environment cannot be determined. The course can cause Sonar Sensor Failure in that a loss of communication would render the output as not the true distance. However, an observable characteristic is not noticed and hence it remains an undeveloped event.

### **5.3 Linking Faults with Hazards**

The completed fault tree provides important information about sensor failure. The faults leading up to the failure have been identified and their correlation to hazards can now be examined. There is not an established method to complete this, however, the fault tree analysis provided a methodical way of thinking that can be similarly applied to each fault.

An example of the flow chart method is shown in Figure 11. The first event in the flow chart is the fault: "Radar Sensor Signal Attenuated by Rain Drops", the following event is a result from this fault, "Radar Sensor Performance Inhibited", the observable symptom from this fault is, "Radar Sensor Output Increases". As a result of these events the Longitudinal Controller will receive information that is not close to the true measurements which leads to three possible situations, vehicle accelerating too quickly, decelerating too quickly, or not responding quick enough. Resultingly, the vehicle may be either too close, too far, or at an unknown distance from the vehicle ahead of it. These scenarios point to three possible hazards: 1, 2 and 4.

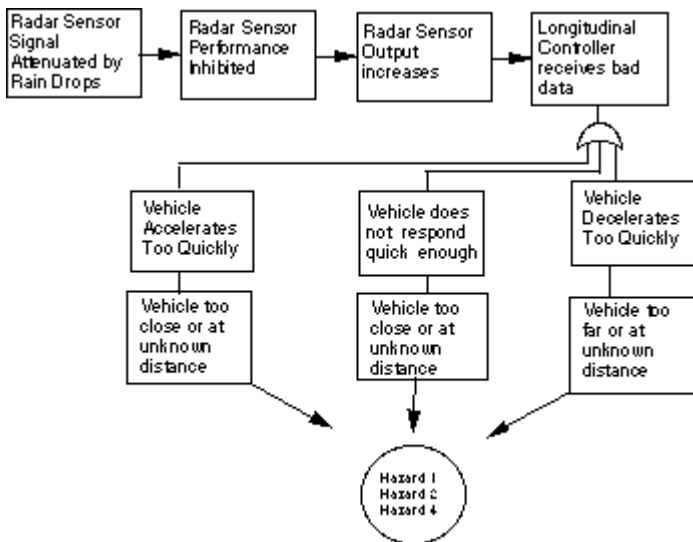


Figure 11: Radar Sensor Hazard Flow Chart

The same procedure was employed for all the component faults and Tables 2 & 3 illustrate the results.

	Radar Sensor Output	Sonar Sensor Output
<b>Power Line</b>	constant 2.20m	constant -0.85m
<b>Data Line</b>	constant 4.25m	constant 2.20m
<b>Dirt</b>	mean: 1.5m < x < 2.5m	constant 0m
<b>Fog</b>	not significantly affected	variance increased by factor of 4
<b>Rain</b>	variance increased by factor of 4	variance increased by factor of 4 mean increased by 10%
<b>Plastic</b>	variance increased by 20%	constant 0m
<b>Vibration</b>	variance increased by 20%	not significantly affected

Table 2: Linking Radar Sensor Faults with Hazards

Faults for Sonar Sensor	Possible Hazards			
Power Line Down	1	2		4
Data Line Down	1	2		4
Debris Covering Sensor	1	2		4
Debris on Road	1	2		4
Rugged Road Conditions			3	
Course Limitations	1	2		4
Electrical Component Shortage	1	2		4
Attenuation from water drops	1	2		4
Snow reflects sensor signal	1	2		4
Electrical Component failures	1	2		4
Moisture affect performance	1	2		4

Table 3: Linking Sonar Sensor Faults with Hazards

## 6.0 Discussion/Conclusion

Through Fault Tree Analysis the component faults that lead up to system failure can be qualitatively predicted. The symptoms of these failures were distinguished by previous research done. The fault characteristics provide useful insight as to what happens with the controller if a failure occurs. This information can be used to predict which hazards are imminent. The results gathered from the Fault Tree Analyses show that the hazard definitions are far too broad to provide useful information in failure

analysis. Future work may include redefining the set of existing hazards to allow for use in failure analysis.

Unfortunately, the trees could not be analyzed quantitatively using Boolean algebra because of the number of undeveloped events and the lack of data corresponding to those events. The Fault Trees developed for the radar and sonar sensors are very limited and exclusive in nature, however, they serve as a springboard to other applications.

One application that the information from the trees can provide is in alerting the supervisory controller that a sensor failure has occurred. Future developments may allow the controller to discard the output that the radar and sonar sensors have provided and rely on other sensory information to make the decisions for the next move.

## **7.0 Acknowledgments**

I would like to thank Laura Darby, Sheila Humphreys, and Lisa Bailey for coordinating the Summer Undergraduate Program in Engineering Research at Berkeley (SUPERB). This wonderful opportunity allowed me to work in a very supportive research environment, the Berkeley Expert Systems Technology Laboratory. Additional thanks to Professor Agogino for her guidance, direction, and provision of three outstanding mentors: Kai Goebel, Brad Cammon, and Jorge Barreto. I cannot thank them enough for their time, dedication, and most importantly patience. I'd like to thank all the members of the BEST lab (Bala Chidambaram, Andy Dong, Rob Stanard, Anil Varma, and David Yu) for showing me how nurturing a research group can be.

## **8.0 References**

Barton, David, et al. Radar Evaluation Handbook. ANRO Engineering, INC, 1991.

Bellm, David W. "Characterization of the Sonar and Radar Distance Sensing Devices Under Sub-Optimal Operating Conditions for the California Partners for Advanced Transit and Highways." Report for Master's Thesis at UC Berkeley, 1995.

Hitchcock, A. "Method of Analysis of IVHS Safety." PATH Research Report

UCB-ITS-PRR-92-14, 1992, pgs. 17-19.

Leonard, J, Hugh, F. Directed Sonar Sensing for Mobile Robot Navigation. Kluwer Academic Publishers, 1992.

Vesely, W. E, et al. Fault Tree Handbook. U.S. Nuclear Regulatory Commission, 1981

pgs. IV-1 -V-3.

## **9.0 Appendix**

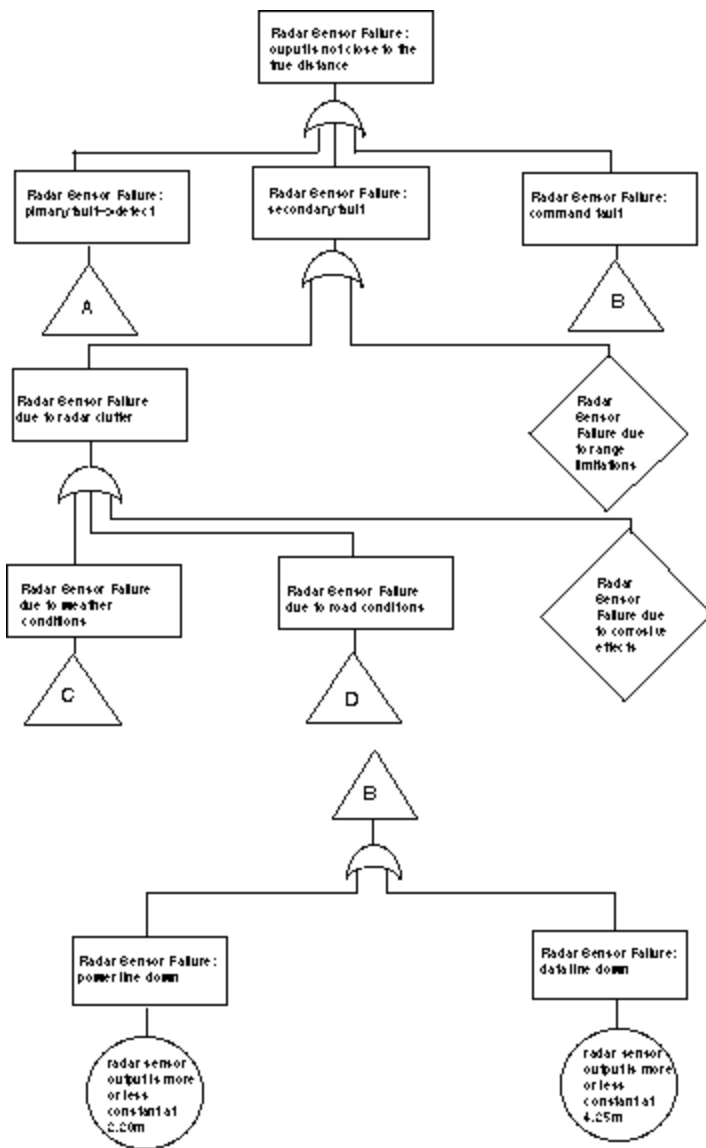
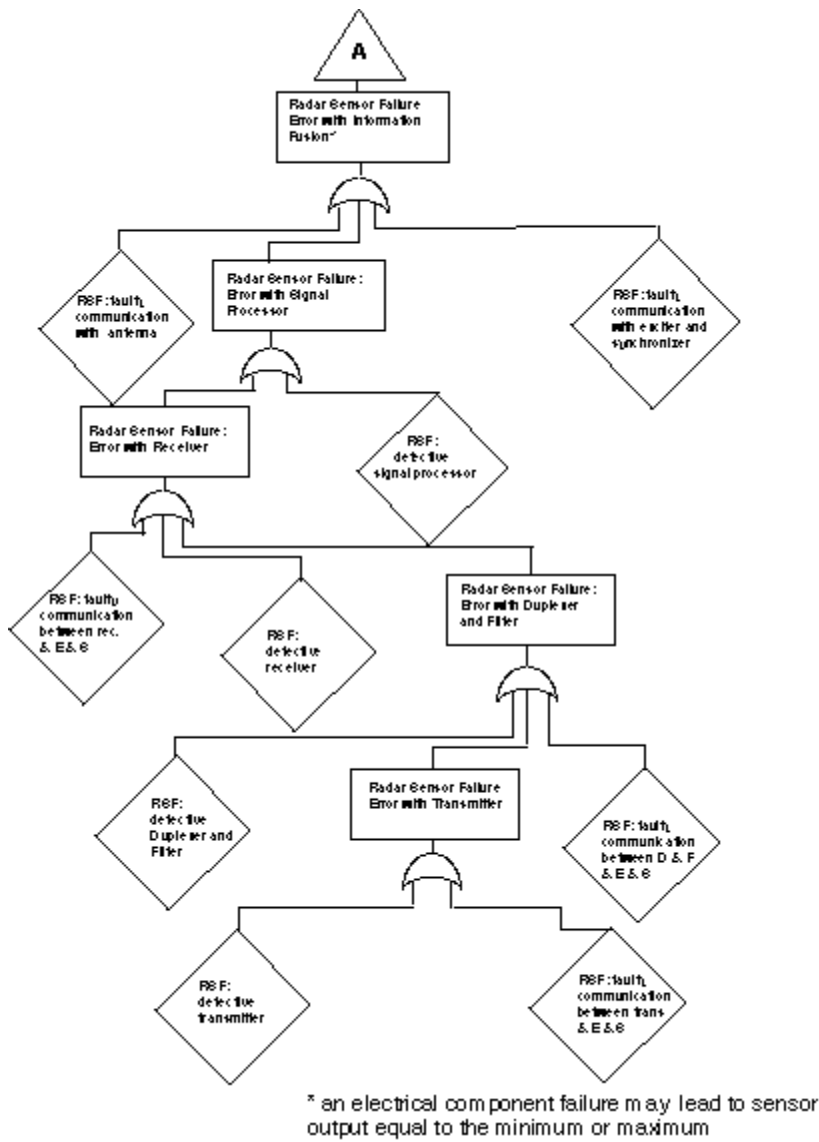


Figure 2: Fault Tree of Radar Sensor: Main Tree



**Figure 3: Fault Tree of Radar Sensor--Primary Fault Branch**

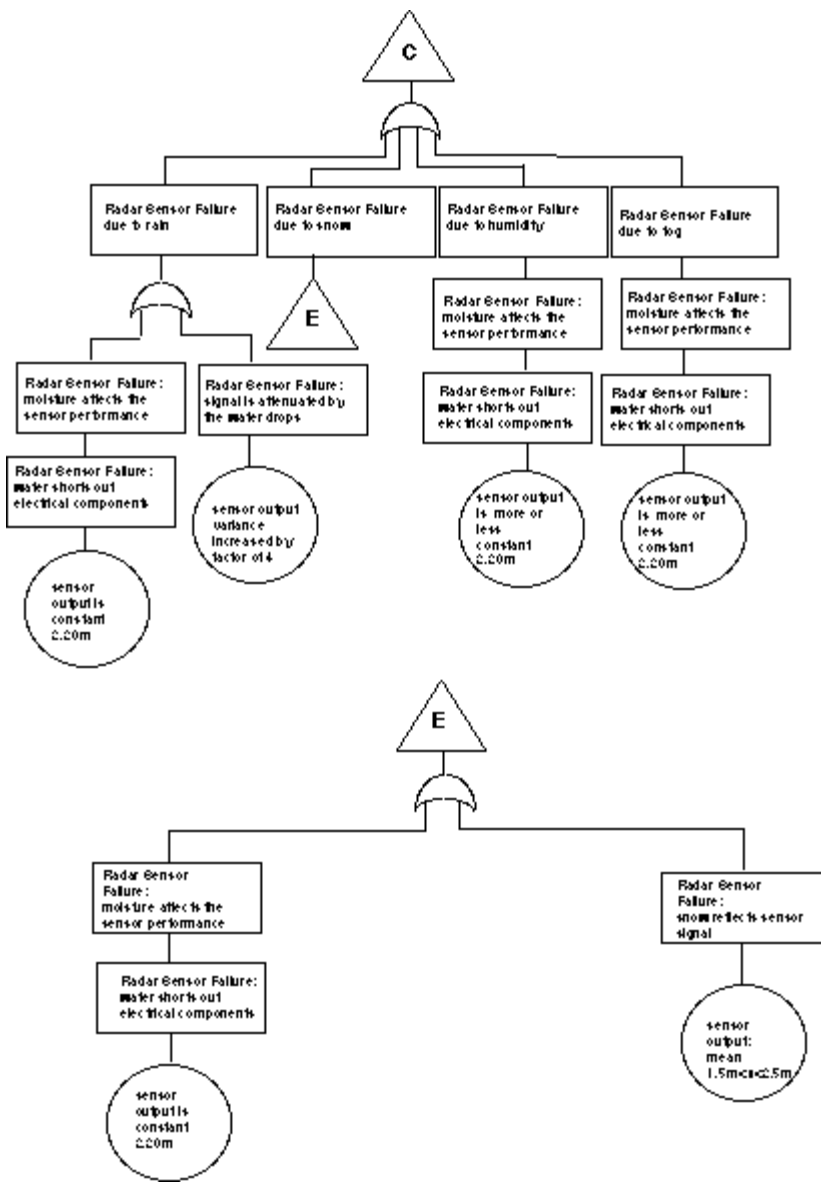


Figure 4: Fault Tree of Radar Sensor--Weather Condition Branch

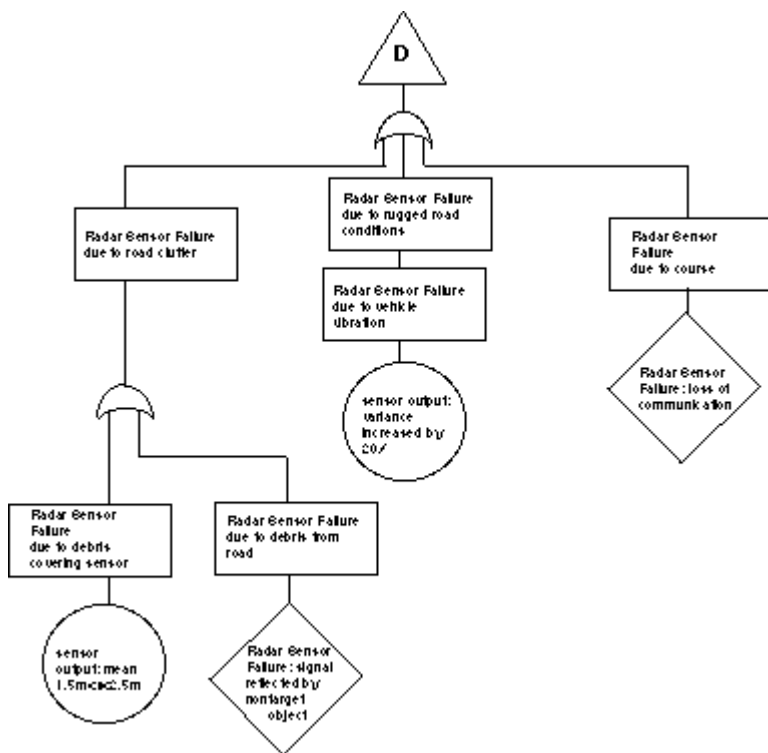


Figure 5: Fault Tree of Radar Sensor--Road Condition Branch

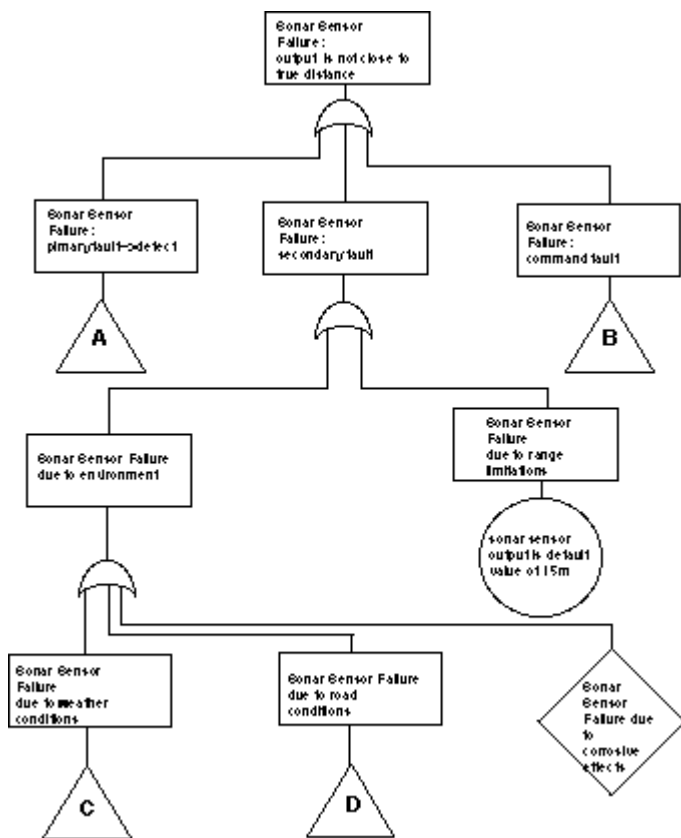


Figure 6: Fault Tree of Sonar Sensor--Main Branch

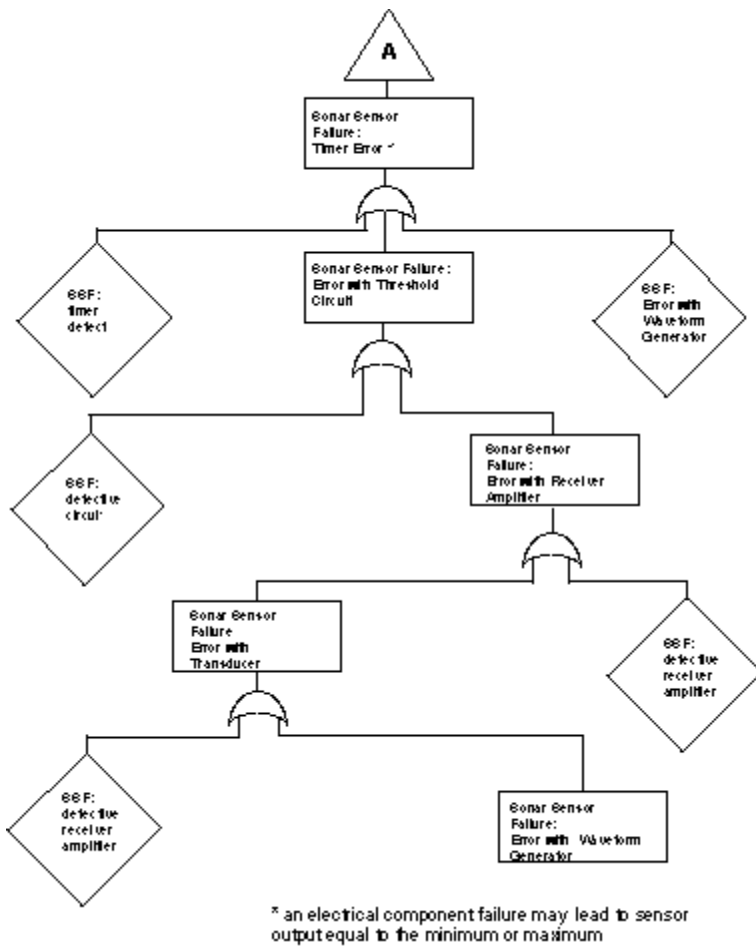


Figure 7: Fault Tree of Sonar Sensor--Primary Fault Branch

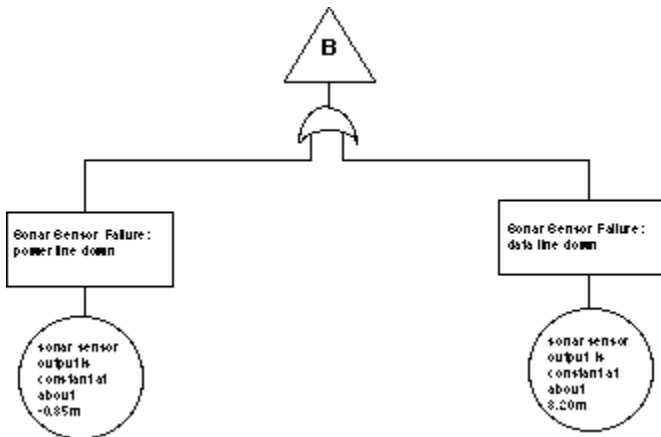


Figure 8: Fault Tree of Sonar Sensor: Command Fault Branch

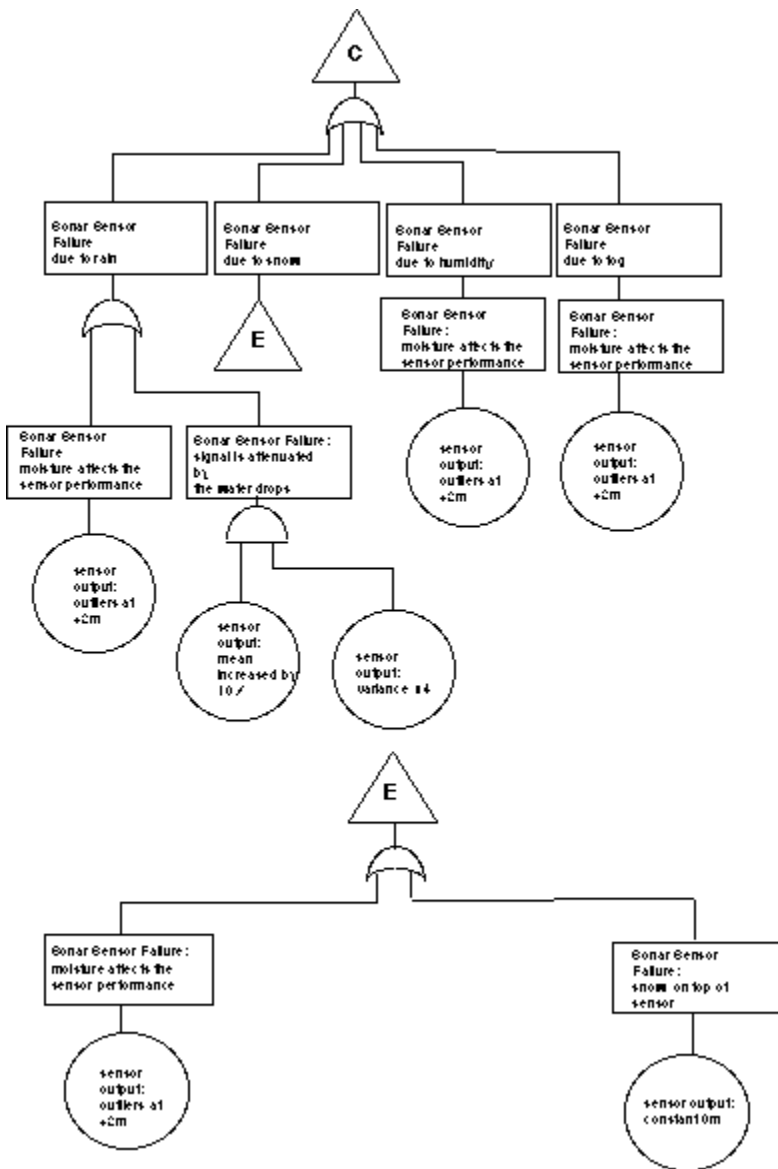


Figure 9: Fault Tree on Sonar Sensor: Weather Condition Branch

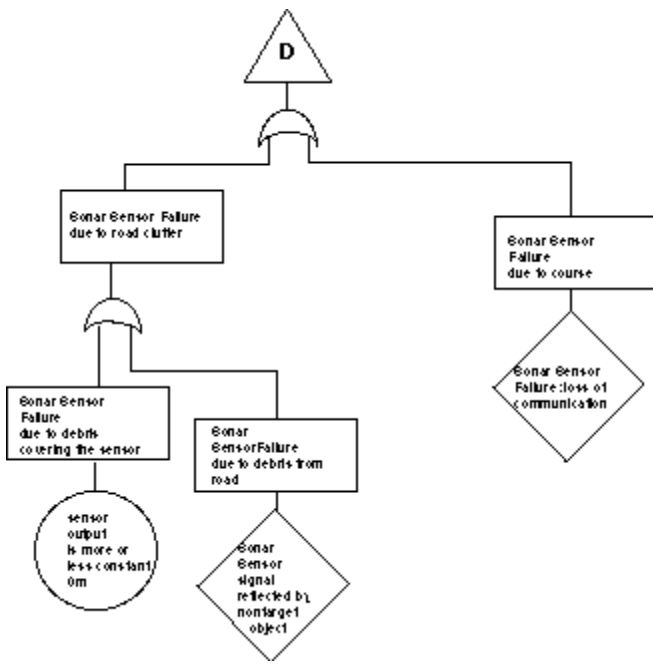


Figure 10: Fault Tree of Sonar Sensor--Road Condition Branch