A process includes determining a probability of a failure mode of a system being analyzed reaching a failure limit as a function of time to failure limit, determining a probability of a mitigation of the failure mode as a function of a time to failure limit, and quantifying a risk reduction based on the probability of the failure mode reaching the failure limit and the probability of the mitigation.

**Abstract**

A process includes determining a probability of a failure mode of a system being analyzed reaching a failure limit as a function of time to failure limit, determining a probability of a mitigation of the failure mode as a function of a time to failure limit, and quantifying a risk reduction based on the probability of the failure mode reaching the failure limit and the probability of the mitigation.

**Claims**

17 Claims, 3 Drawing Sheets
100

102 RECEIVE A FAILURE MODE FOR A SYSTEM BEING ANALYZED (E.G. A ROCKET ENGINE)

104 RECEIVE A PLURALITY OF FAILURE SIGNATURES

106 DETERMINE A RISK PROBABILITY FOR A FAILURE MODE CORRESPONDING TO A LIKELIHOOD THAT A SELECTED FAILURE MODE WILL OCCUR

108 DETERMINE A CORRELATION RANKING FOR EACH OF THE PLURALITY OF SIGNATURES CORRESPONDING TO A LIKELIHOOD THAT A SELECTED SIGNATURE REPRESENTS THE FAILURE MODE

110 DETERMINE A FAILURE MODE RISK PROBABILITY FOR EACH SIGNATURE, COMPARING A RANKING OF A SELECTED SIGNATURE TO A SUM OF ALL CORRELATION RANKINGS FOR THE FAILURE MODE

112 FOR EACH SIGNATURE HAVING A NON-ZERO CORRELATION RANKING, DETERMINE A DISTRIBUTION CORRESPONDING TO A PROBABILITY THE SIGNATURE WILL OCCUR AT A GIVEN TIME TO FAILURE LIMIT IN THE SYSTEM BEING ANALYZED

114 DETERMINE AN EFFECTIVENESS SCORE FOR EACH OF THE PLURALITY OF SIGNATURES, THE SCORE CORRESPONDING TO AN ABILITY TO RESPOND TO A SELECTED FAILURE MODE USING A FDS TO PREVENT THE FAILURE MODE FROM REACHING A FAILURE LIMIT AS A FUNCTION OF TIME TO FAILURE LIMIT

116 CALCULATE A FAILURE LIMIT OCCURENCE PROBABILITY REDUCTION FOR EACH OF THE PLURALITY OF SIGNATURES

118 SELECTIVELY REPEAT STEPS 106-116 FOR A PLURALITY OF FAILURE MODES

120 CALCULATE SUM OF ALL FAILURE LIMIT OCCURENCE PROBABILITY REDUCTIONS FOR EACH OF THE PLURALITY OF FAILURE MODES

122 COMPARE THE SUM OF STEP 120 TO A SUM OF OVERALL FAILURE LIMIT OCCURENCE PROBABILITY REDUCTIONS IN THE SYSTEM BEING ANALYZED WITHOUT IMPLEMENTATION OF THE FDS TO DETERMINE A FDS RISK REDUCTION FRACTION

FIG. 1
All failures occur in 0.6 seconds

FIG. 2a

20% of failures occur in 0.4 sec.
30% of failures occur in 0.7 sec.
50% of failures occur in 1.2 sec.
Sum of all percentages = 100%

FIG. 2b

Continuous distribution skewed to fast failures.

FIG. 2c

FIG. 3
FAILURE DETECTION SYSTEM RISK REDUCTION ASSESSMENT

This application was made with government support under Contract No. NNM06AB13C awarded by NASA. The Government may therefore have certain rights in this invention.

BACKGROUND OF THE INVENTION

This application relates to failure detection systems, and more particularly to a method for determining the risk reduction of a given failure detection system.

A failure detection system ("FDS") may be used to identify failure signatures (e.g., a loss of engine coolant) indicative of failure modes (e.g., a radiator leak) in the hope that identification of the signature can prevent the failure mode from causing a failure limit (e.g., engine reaching temperature at which engine block will crack).

SUMMARY OF THE INVENTION

A failure detection system ("FDS") seeks to predict or provide notification of failures, to give a system operator an opportunity to prevent the occurrence of a failure limit in a system being analyzed (e.g., aircraft, automobile, welding process, etc.). Using the example of an automobile, one example failure mode is a radiator leak. This failure mode has many possible consequences. For example, as a result of the radiator leak, the engine could overheat beyond a threshold temperature, resulting in a final outcome of a cracked engine block, causing the engine to no longer work. Another example consequence could be an engine heating causing a gas line to break, with a final outcome of an engine fire.

A failure mode is a characteristic manner by which a failure may be, for example, a simple engine warning light, or a temperature gauge. A more primitive FDS could correspond simply performing a manual inspection of a structure, such as a vehicle. As another example, a FDS may correspond to a Health and usage Monitoring System ("HUMS") used to monitor the health of critical components of a vehicle, such as a rocket, and used to collect operational flight data utilizing on-board accelerometers, sensors, and avionic systems. One example of a HUMS FDS is the Advanced Health Management System ("AHMS"). A system being analyzed may have no FDS, such that a failure mode is simply allowed to follow its natural course which may or may not lead to a failure limit.

In a given system, there may be a plurality of failure modes. A failure mode is a characteristic manner by which a failure occurs. A failure mode may represent a specific way in which a system, device or process (e.g., aircraft, automobile, welding process, etc.) can fail.

Using the example of an automobile, one example failure mode is a radiator leak. This failure mode has many possible consequences. For example, as a result of the radiator leak, the engine could overheat beyond a threshold temperature, resulting in a final outcome of a cracked engine block, causing the engine to no longer work. Another example consequence could be an engine heating causing a gas line to break, with a final outcome of an engine fire.

A failure mode may have an associated failure limit, which is a defined as a failure threshold that can occur if a failure mode is left untreated. For example, a failure limit may be a known engine temperature beyond which engine damage will occur. A FDS seeks to predict or provide notification of a failure mode, to give a system operator an opportunity to prevent a failure limit from occurring.

A signature is a basic failure building block that is indicative of a given failure mode. For example, signatures of a radiator leak failure mode include loss of engine coolant, and could also include a gas line leak. Each signature may have an associated time-to-failure limit ("TTFL"), which is an elapsed time from an onset of the failure signature until a system reaches a failure limit.

It can be useful to compare different failure detection systems. For example, if a new FDS was very costly, a service provider of the FDS may wish to justify the increased cost of the FDS by demonstrating its improvement over a previous FDS. This improvement could be represented in the form of a risk reduction of the FDS. Equation 1, shown below, may be used to determine a risk reduction of a FDS.

$$R.R._{\text{fraction}} = \frac{FPMM_{\text{reduced by FDS}}}{FPMM_{\text{original}}}$$

where

- $R.R._{\text{fraction}}$ is a risk reduction fraction;
- $FPMM_{\text{reduced by FDS}}$ is a failure limit occurrence probability reduction (optionally measured in failures per million missions) after application of a selected failure detection system; and
- $FPMM_{\text{original}}$ is failure limit occurrence probability reduction (optionally measured in failures per million missions) prior to application of the selected failure detection system;

FIG. 1 schematically illustrates a method 100 of determining a risk reduction of a failure detection system. The method 100 may be used to determine $FPMM_{\text{reduced by FDS}}$ as shown in equation #1. The method 100 receives a plurality of failure modes for a system being analyzed (step 102). In one example the plurality of failure modes is received from an existing failure mode and effects analysis ("FMEA") system.
Of course, the failure modes may be received from other sources, or may be independently developed. The method 100 also receives a plurality of failure signatures (step 104). While it is understood that the method 100 could be performed with a single failure mode and a single failure signature, the method 100 will be described in relation to a plurality of failure modes and a plurality of failure signatures to provide an understanding of the wide applicability and scalability of the method 100.

A risk probability is determined for each of the plurality of failure modes (step 106). The risk probability corresponds to a likelihood that a selected failure mode will occur. In one example the probability is determined as a failure per million missions ("FPMM"), which is the failure probability of 10^{-6} per mission. Of course, other probability benchmarks could be used. Various sources of information may be used for this determination, such as historical data, simulations, expert analysis, and test and field usage data. Engineering analysis data may include, for example, data from computer simulations. Thus, both historical data of actual failures and predicted data of future failures may be used in determining the FPMM risk probability.

A robust risk probability determination may include accounting for variations in a given system. Using the example of an engine, when the engine comes off an assembly line, there are often variations of engine characteristics between engines produced from the same assembly line. For example, dimensions, pump efficiency, duct resistance, etc. may vary from one engine to another due to a margin of error in manufacturing. This can make predicting engine performance and predicting engine failure challenging. To address this difficulty, computer software may be used to generate random values (e.g., engine efficiencies, engine resistances, etc.) within a predicted range of variation. These randomly generated values may be used to produce a predicted cluster of engine builds, which could include both high performing and low performing engines. This predicted cluster could then be used in the determination of step 106. In one example the Monte Carlo class of computational algorithms may be used to determine a predicted cluster of engine builds. Of course, other algorithms and computer-based software and simulations could be used.

A correlation ranking is determined for each of the plurality of failure signatures according to a scale (step 108). The correlation ranking corresponds to a likelihood that a given signature represents the at least one failure mode. In one example the scale is 0-5, with 5 corresponding to a strong correlation between the failure mode and the signature. Of course, other scales and values could be used. Sources used in determining the correlation ranking could include, for example, historical data, engineering analysis and expert opinion.

Returning to the example failure mode of an automobile radiator failure, the signature of an engine overheating may be assigned a correlation value of "5" (high correlation to radiator failure), the signature of a gas line rupture may be assigned a correlation value of "1" (low correlation to radiator failure), and the signature of loss of tire pressure may be assigned a correlation value of "0" (no correlation to radiator failure).

A failure mode risk probability is determined for each of the plurality of signatures for that failure mode (step 110). The risk probability compares comparing a ranking of a selected signature to a sum of all rankings for a failure mode, and may be calculated using equation #2 below.

\[
FPMM_{i,j} = \frac{\text{Rank}_{i,j}}{\sum_{n=1}^{n} \text{Rank}_{n}}
\]

where

- \(i\) is a failure mode number;
- \(j\) is a signature number;
- \(n\) is a quantity of signatures for the failure mode; and
- \(\text{FPMM}_{i,j}\) is a failure limit occurrence probability reduction for the given failure mode (see step 106).

As an example, assume that a automobile radiator failure is a first failure mode, and has a risk probability from step 106 of "10" (FPMM_{i}="10") Assume also that signature 1 has a correlation rank of 5, signature 2 has a correlation rank of 1, and signature 3 has a correlation rank of 0. The denominator in equation #2 would be 5+1+0=6 (sum of correlation rankings). Signature 1 would then be assigned a risk probability of

\[
\frac{5}{6} \times 10 = 8.33 \text{ (FPMM}_{1,1})
\]

signature 2 would then be assigned a risk probability of

\[
\frac{1}{6} \times 10 = 1.67 \text{ (FPMM}_{1,2})
\]

and signature 3 would then be assigned a risk probability of

\[
\frac{0}{6} \times 10 = 0.0 \text{ (FPMM}_{1,3})
\]

Adding the various risk probabilities would yield a failure mode 1 total risk probability of 8.33+1.67+0.0=10.0.

For each failure signatures having a non-zero correlation ranking, a distribution is determined (step 112) corresponding to a probability that the signature will occur at a given TTFL. The distribution is a failure probability density function ("f function"). The "f function" captures a tendency of a signature to occur slowly (large TTFL), or quickly (small TTFL). Each "f function" may be determined in response to historical data, engineering modeling, and engineering judgment, for example.

FIG. 2a schematically illustrates a first example "f function" 40a in which all failures occur in 0.6 seconds (TTFL=0.6 seconds).

FIG. 2b schematically illustrates a second example "f function" 40b in which 20% of all failures occur in 0.4 seconds (TTFL=0.4 seconds), 30% of all failures occur in 0.7 seconds (TTFL=0.7 seconds), and 50% of all failures occur in 1.2 seconds (TTFL=1.2 seconds). The sum of all percentages is 20%+30%+50%=100%.

FIG. 2c schematically illustrates a third example "f function" 40c which represents a continuous distribution curve 42 that is skewed to fast failures.

An effectiveness score, or "g function," corresponding to an ability to respond to each of the signatures to prevent a failure using a FDS as a function of TTFL is determined (step 114). Each "g function" may be determined in response to engineering modeling of a system, the FDS, and failure signatures over a range of TTFL values, for example. A "g function" is solely failure signature dependent, and is consid-
where

- \( m \) is a quantity of failure modes;
- \( n \) is a quantity of signatures;
- \( \text{F.L.O.P.R}_{\text{overall}} \) is a probability that a failure limit would be reached in the system being analyzed but is mitigated by a FDS.

Once the sum from step 120 is available, the sum may be compared to (e.g., divided by) an overall failure limit occurrence probability in the system being analyzed without implementation of the FDS to determine a FDS risk reduction fraction, as shown in equation #1 (step 122).

Referring again to the example of an automobile, assume that a failure probability before introducing an FDS is 100 FPMM, and assume that each "mission" is a 100 mile drive at 60 MPH. Failure modes may include radiator failure, tire failure, and transmission failure. Failure signatures may include engine heating, loss of power to wheels, and loss of ability to accelerate. A maximum TTFL of interest at the beginning of the mission is 100/600=1.67 hours, which decreases to zero at the end of the mission. Assuming introduction of an FDS reduces an overall risk by 50 FPMM (the sum of the contributions of all the signatures over all the failure modes), yielding a risk reduction of 50% (by using equation #1).
quantifying a risk reduction based on the probability of the failure mode of reaching the failure limit and the probability of the mitigation, wherein said step of determining a probability of a failure of a system being analyzed as a function of time to failure limit includes:

a) determining a risk probability for at least one failure mode, the risk probability corresponding to a likelihood that the at least one failure mode will occur in the system being analyzed;
b) determining a correlation ranking for at least one failure signature, the correlation ranking corresponding to a likelihood that the at least one failure signature represents the at least one failure mode;
c) determining a failure mode risk probability for the at least one failure signature corresponding to a probability that the at least one failure signature will occur at a given time to failure limit in the system being analyzed.

3. The method of claim 2, wherein said step (a) is performed in response to historical data of actual failures, predicted data of future failures, or both.

4. The method of claim 2, wherein said step (a) includes: predicting a cluster of systems being analyzed; determining a probability that the failure mode will occur in each system in the cluster; and averaging the probabilities to determine an overall probability that the failure mode will occur in the system being analyzed.

5. The system of claim 2, wherein the correlation ranking of said step (b) is in a range from 0-5.

6. The method of claim 2, wherein said step (d) is only performed for a selected failure signature if the selected failure signature has a non-zero correlation ranking.

7. The method of claim 2, wherein the system being analyzed is a machine or a process.

8. The method of claim 2, wherein said step of determining a probability of a mitigation of the failure as a function of a time to failure limit includes:

d) determining a distribution corresponding to a probability that the at least one failure signature will occur in the system being analyzed without implementation of the failure detection system.

e) determining an effectiveness score corresponding to an ability to respond to the at least one failure signature using a failure detection system to prevent the at least one failure mode from reaching a failure limit in the system being analyzed as a function of time to failure limit.

9. The method of claim 8, wherein said step of quantifying a risk reduction based on the probability of the failure and the probability of the mitigation includes:

f) calculating a failure limit occurrence probability reductions for the at least one signature in response to the effectiveness score;
g) calculating a sum of failure limit occurrence probability reductions from said step (f) for each signature in the signature set; and

h) comparing the sum of failure limit occurrence probability reductions for the failure detection system to a sum of overall failure limit occurrence probabilities in the system being analyzed without implementation of the failure detection system to determine a risk reduction fraction of the failure detection system.

10. The method of claim 9, wherein said step (f) includes integrating on the computer a product of a function corresponding to the distribution of said step (d) and a function corresponding to the effectiveness score of said step (e).

11. The method of claim 9, wherein the failure detection system is a first failure detection system, and wherein said step (b) includes dividing the sum of failure limit occurrence probabilities for the first failure detection system by a sum of failure limit occurrence probabilities for a second failure detection system.

12. The method of claim 8, wherein said step of determining a probability of a mitigation of the failure as a function of a time to failure limit includes:

f) calculating a failure limit occurrence probability reduction for the at least one signature in response to the effectiveness score;
g) selectively repeating steps (a)-(f) for a plurality of failure modes;
h) calculating a sum of failure limit occurrence probability reductions from said step (g) for each signature in the signature set; and

i) comparing the sum of failure limit occurrence probability reductions for the failure detection system to a sum of overall failure limit occurrence probabilities in the system being analyzed without implementation of the failure detection system to determine a risk reduction of the failure detection system.

13. A computer-implemented system, comprising:

a) a storage module storing at least one failure mode for a system being analyzed; and

b) a microprocessor, the microprocessor being operable to determine a probability of the at least one failure mode of the system being analyzed reaching a failure limit as a function of time to failure limit, determine a probability of a mitigation of the failure as a function of time to failure limit, and quantify a risk reduction based on the probability of the failure mode reaching the failure limit and the probability of the mitigation.

14. The system of claim 13, wherein an input/output module is also operable to receive a plurality of failure signatures, and to output the risk reduction.

15. A computer-implemented system, comprising:

a) a storage module storing at least one failure mode for a system being analyzed; and

b) a microprocessor, the microprocessor being operable to determine a probability of the at least one failure mode of the system being analyzed reaching a failure limit as a function of time to failure limit, determine a probability of a mitigation of the failure as a function of time to failure limit, and quantify a risk reduction based on the probability of the failure mode reaching the failure limit and the probability of the mitigation; and

c) an input/output module operable to receive a plurality of failure signatures, and to output the risk reduction, wherein the microprocessor determines a probability of a failure of a system being analyzed as a function of time to failure limit by determining a risk probability for at least one failure mode, determining a correlation ranking for at least one failure signature, determining a failure mode risk probability for the at least one failure signature comparing the correlation ranking of the at least one failure signature to a sum of all correlation rankings for a signature set, and determining a distribution corresponding to a probability that the at least one failure signature will occur at a given time to failure limit in the system being analyzed.

16. The system of claim 15, wherein the microprocessor determines a probability of a mitigation of the failure as a function of a time to failure limit by determining an effective-
ness score corresponding to an ability to respond to the at least one failure signature using a failure detection system to prevent the at least one failure mode from reaching a failure limit in the system being analyzed as a function of time to failure limit.

17. The system of claim 16, wherein the microprocessor quantifies a risk reduction based on the probability of the failure and the probability of the mitigation by calculating a failure limit occurrence probability reduction for the at least one signature in response to the effectiveness score, calculating a sum of failure limit occurrence probability reductions for each signature in the signature set, and comparing the sum of failure limit occurrence probability reductions for the failure detection system to a sum of overall failure limit occurrence probabilities in the system being analyzed without implementation of the failure detection system to determine a risk reduction of the failure detection system.