The Space Congress® Proceedings

2000 (37th) Space Means Business in the 21st Century

May 3rd, 2:00 PM

Paper Session II-C - A NASA Predictive Safety Model

Michael Camet
The University of Texas at El Paso Bhupendra Deliwala, Kennedy Space Center, NASA

Rolando Quintana
The University of Texas at El Paso Bhupendra Deliwala, Kennedy Space Center, NASA

A NASA Predictive Safety Model

Michael Camet and Rolando Quintana; The University of Texas at El Paso
Bhupendra Deliwala, Kennedy Space Center, NASA

Abstract

A proactive methodology for accident prevention, called Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM), has been developed by utilizing the principles of work sampling and control charting. Sampling is performed to observe the occurrence of conditions that may become hazardous in a given system. These conditions, known as dendritics, could eventually result in an accident or occupational disease. The CHTFPM involves a random sampling for the occurrence of these dendritics. The collected data is then used to generate a control chart. Based on the pattern of the control chart, a system "under control" is not disturbed whereas a system "out of control" is investigated for potential conditions becoming hazardous. Appropriate steps can then be taken to eliminate or control these potentially dangerous and costly conditions to maintain a safe system.

Introduction

The formal methods of hazard analysis can be divided into two broad categories: inductive and deductive (National Safety Council, 1992). The inductive method forms the basis for such analysis as failure mode & effect analysis (FMEA), and operation hazard analysis (OHA). These methods emphasize the mode of failure, the triggering event(s) and the ultimate impact on people and property (National Safety Council, 1992). If inductive analysis details what can happen, deductive analysis informs how. An example would be fault tree analysis (FTA). It postulates failure of the entire system and then identifies how they contribute to the failure (National Safety Council, 1992).

However, the formal methods are limited in their effectiveness as they only come into picture once an accident has taken place. They are like a post-mortem report that identifies what happened and how it happened. They do not provide real time information on whether the conditions in a system are becoming hazardous, which may finally lead to an accident, an injury, or an occupational disease. Present safety methodologies basically provide feedback on hazards after accidents have happened. But what is required is a concept that indicates that the system under consideration is becoming hazardous. This information would facilitate to check and eliminate the hazard before accidents can happen.

This research espouses one such concept, namely Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM), which studies the system for occurrence of conditions becoming hazardous and takes steps to eliminate these conditions when their occurrence crosses certain preset limits or when they show an unnatural pattern. The concepts underlying this proactive approach to industrial safety are derived from work sampling and control chart theories. These theories emphasize a cost effective way of keeping a continuous check on the safety status of the system under consideration. CHTFPM involves a planned, systematically organized, and before-the-fact process characterized as the identify-analyze-control method of safety (National Safety Council, 1992). The emphasis is placed on an acceptable safety level designed into the system prior to actual production or operation of the system. The CHTFPM requires timely identification and evaluation of the conditions becoming hazardous - before losses occur. A policing and inspection approach aimed at enforcement of safety and health standards cannot generate effective preventive measures because it is episodic, external and coercive rather than sustained, internal and self-governed, and often arbitrary and indifferent rather than relevant and motivated. In essence, the CHTFPM is concerned with determining and maintaining a preset degree of safety, within the constraints of operational effectiveness, time, cost, and other applicable interfaces to safety that can be achieved throughout the lifecycle of the system. The premise here is that continuous improvement is very much valid for the discipline of safety engineering, as has been shown in the field of quality (Juran and Gryna, 1980).

Methodology

In CHTFPM, the safety status of a system is evaluated using dendritics, the core conditions leading to hazards in any given system. The effectiveness of CHTFPM depends on the identification of these dendritics for performing the sampling study of a given system. The steps taken for the creation of the CHTFPM, which will be briefly discussed, are the following:

1. The core elements (dendritics) are constructed.
2. A random sampling scheme is developed.
3. Samples are used to construct a safety control chart.
4. The control chart observations are tested for “out of control” conditions.
5. If an “out of control” condition is detected, appropriate action is taken.

The fundamental issue in the implementation of continuous hazard tracking is the identification of the core conditions leading to hazards in any given system. These core conditions can be termed as dendritics of a particular class of hazards, which if present may lead to a hazardous condition, which ultimately can result in an accident.

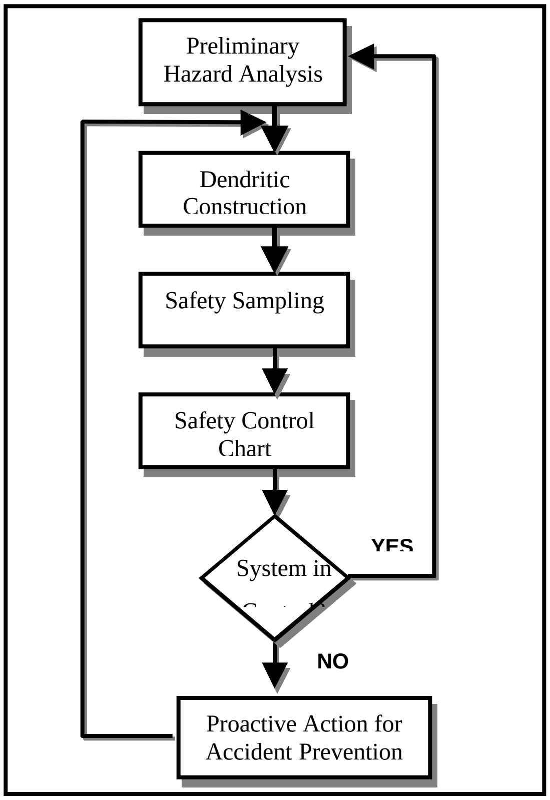


Figure 1- Schematic of CHTFPM

To develop the dendritics for a system, an analysis of the system must be performed using the preliminary hazard analysis (PHA). A PHA provides an initial risk assessment of a system, identifies safety critical areas, evaluates hazards, and identifies the safety design criteria to be used (Grimaldi and Simonds, 1989), (Roland and Moriarty, 1983). The CHTFPM will dynamically monitor the state of the system with respect to dendritics developed from this initial risk assessment. The PHA effort should thus commence during the initial phases of system development, or in the case of a fully operational system, at the initiation of a safety evaluation. A Pareto analysis can then be performed to list the dendritics based on hazard severity, hazard probability, risks, and operational constraints.

The CHTFPM is a concept of providing safety condition information in a statistically verifiable and economically viable manner by using the principles of work sampling and control charts. The basic hypothesis is that a random sample of a sufficiently large size, as in work sampling, reflects the state of the system being observed. Further, the plotting of the attribute, namely the existence or potential for a hazard, could indicate whether the system is safe or not, similar to the use of p-charts to perform quality control in industry (Feigenbaum, 1991), (Grant and Leavenworth, 1988), (Juran and Gryna, 1980).

Observations are plotted to obtain a safety control chart. If it is ‘under control’; *i.e.*, there is a no significant potential for a hazard, the sampling process is continued. However, if the control chart indicates that the system is ‘out of control’; *i.e.*, there is a significant potential for a hazard that could result in an accident, then proactive action should be taken to prevent an accident. Further, dendritics can also be continuously improved by studies of the system from new perspectives. A schematic of CHTFPM is provided in Figure 1.

As seen in Figure 1, the steps taken for the creation of the CHTFPM are: (1) Conduct a preliminary hazard analysis of the system, (2) The dendritic elements are constructed, (3) Determine frequency of sampling and sample size based on confidence level and desired accuracy, (4) Perform random sampling – each day provides the value of *c*, *p*, *u*, or *Z* (depending on which type of control chart is in use), (5) Samples are used to construct applicable safety control chart(s), (6) If the safety control chart(s) indicates the system in operating *in control*, sampling continues. However, if the safety control chart(s) indicates the system is operating *out of control*, it implies that the system is becoming hazardous. Appropriate investigative action is conducted to sampling of the system continues determine the cause(s) and corrective steps are taken. (7) Repeat steps 2 through 7 until the system is operating *in control*, (8) Perform a discriminant analysis to study the contributions each dendritic makes to overall system safety and to refine preliminary dendritic list.

Implementation and results

To demonstrate the potential use of CHTFPM at NASA (NASA FAR GRANT NAG 10225), one system at Marshall Space Flight Center was chosen for implementation. The Upward Flammability of Materials in Gaseous Oxygen Test, conducted in the Materials Combustion Research Facility at MSFC, is utilized to determine which metals are best suited for use in a high-pressure, 100% gaseous oxygen (GOX) atmosphere. The test is conducted by attaching an igniter to a 1/8-inch diameter, 12-inch rod of the candidate material and then igniting it in a chamber filled with 100% GOX at the proposed pressure, up to 10,000 pounds per square inch.

The nature of the testing that occurs is complex and involves potential hazards. All test operators are certified before conducting any tests. The operators receive training on the handling of compressed gas cylinders, oxygen compatibility, use of personal protective equipment, safe laboratory practices and hazardous waste disposal. Promoted combustion testing can be extremely hazardous because of the high pressures and temperatures inside the combustion chamber. The combustion chamber, where samples are ignited and allowed to burn, can be pressurized up to 10,000 psi with GOX. The hazards involved in promoted combustion testing are numerous. Operators can be exposed to electrical load and other ignition sources in the air and/or oxygen-enriched environments. Heavy parts of the test apparatus are handled and moved on a regular basis. Testing involves burning materials in an oxygen-enriched environment, thus introducing the hazards associated with explosions. The operators regularly work with pressurized systems and compressed gas cylinders containing oxygen. The operators frequently handle cleaning solvents that require personal protective equipment.

Dendritic construction requires multiple steps. The first step, the PHA, aids the analyst by identifying and evaluating hazards, and the safety design and operations requirements needed. The PHA is performed to document an initial risk assessment of a concept or system. It is based on the best available data, including mishap data from similar systems. The hazards associated with the proposed design or function are identified and evaluated for potential hazard severity, probability, time of exposure, and hazard classification. Design controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level shall be considered and documented. A PHA was performed to consider human error and environmental hazards.

The PHA, by granting a basic depiction of the hazards and the subsequent safety design criterion thereof, facilitated the second tool used in dendritic derivation, the failure mode and effects analysis (FMEA.) FMEA is defined as a bottom-up method of identifying the failure modes of a system and determining the effects on the next higher level. The FMEA constructed for the depiction of possible system failures was formulated as required per NHB 5300.4 (1D-2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, Paragraph 1D301-3.

Barrier analysis techniques can be used to examine administrative and procedural problems, equipment or system failures, injuries, accidents, and other similar events. A barrier analysis was performed on several hazards not identified on the PHA. Since this type of analysis works particularly well when analyzing human factors affecting system safety, only those hazards specifically pertaining to humans were included in this analysis. Many of the hazards included in this analysis were brought to light during discussions with combustion testing personnel and system engineers.

The last step in dendritic construction consisted of using the completed FMEA and barrier analysis to obtain a final list of conditions, or dendritics, that may become hazardous. After review of each item in the FMEA and the barrier analysis, a dendritic list was formed depicting possible occurrences that may result in system failure. Table 1 depicts the complete list of dendritics.

Table 1 – Dendritic List

1. Failure to adhere to SOP
2. Incorrect procedure used to don latex gloves
3. Same surface contact (bare hand and glove)
4. Personnel wearing dirty latex gloves
5. Trash and combustibles not in fire retardant containers
6. Test area not in “limited access control”
7. Test cell used for storage
8. Personnel limitations for a test cell exceeded (max or five)
9. Personnel not wearing safety shoes in test area or while moving heavy objects
10. Arms fully extended to the front while lifting object
11. Back bent forward while lifting object
12. Oxygen container dragged, slid, or rolled

Various documents reviewed for their applications to promoted combustion testing were “Working Safely with Compressed Gases and Cryogens,” “Safety and Health Plan for MRCF,” and “SOP for Promoted Combustion Testing.” Especially useful in dendritic construction were consultations with test engineers and technicians. These consultations provided practical insights into testing operations that could not be gained by simply reviewing the SOP.

The sampling sheet was designed so that it provides the analyst a closer look at the behavior of the system. That is, it provides the tally marks for the occurrence of each dendritic so that a Pareto analysis can indicate which one is most significant and causing the system to become hazardous. This can’t be considered statistically significant, but it provides an indication to what is the major dendritic influencing the system to behave in a degenerating manner. The sampling sheet provides the raw data and helps in collating required information. The analyst is required to note the time and day, mark the dendritics present, and inscribe any comments that may be needed for future review. Notation of the date/time and additional comments is absolutely necessary for the formulation of assignable causes, in the event that an out of control situation presents itself. Comments may include new or absent personnel, maintenance, *etc*.

Time order is the logical basis for the data collection in this study. Promoted combustion testing operations were videotaped over a period of two weeks. The videotaped operations were split into 100 subgroups with 4 samples in each subgroup. The random times necessary for the sampling scheme were generated using a random timer connected to a time lapse VCR (Gyyr, Model Number TLC3168HD). The videotaped operations sent by MCRF were played back as input into the time lapse VCR. A random timer that randomly records a set number of clips of certain duration controls the time lapse VCR. The random timer was then set to randomly record 4 samples from each subgroup. Each random sample was approximately 10 seconds long to allow adequate time to check for all 21 dendritics.

Because the underlying distribution of the data was Poisson, the *c* chart, which will plot the total number of occurring dendritics per subgroup, was selected. The UCL and the LCL will have approximately 99.73% of all normal observations within their boundaries, since 3σ means that approximately 99.73% of all observations should be within these limits. A preliminary sample, consisting of the first 10 subgroups was used to estimate *c*, and the results are depicted in Figure 2.

The trial control limits constructed from the preliminary study yielded no out of control points and were thus adopted for further use. Two control points are above the UCL, indicating that at that time the safety status of the system was degrading to an unacceptable level. Examination of the sampling sheets for the time periods pertaining to the out of control points indicates that an unusually high number of occurrences of the dendritic personnel not wearing safety shoes occurred. While two control points exceeded the UCL, the vast majority of points were within

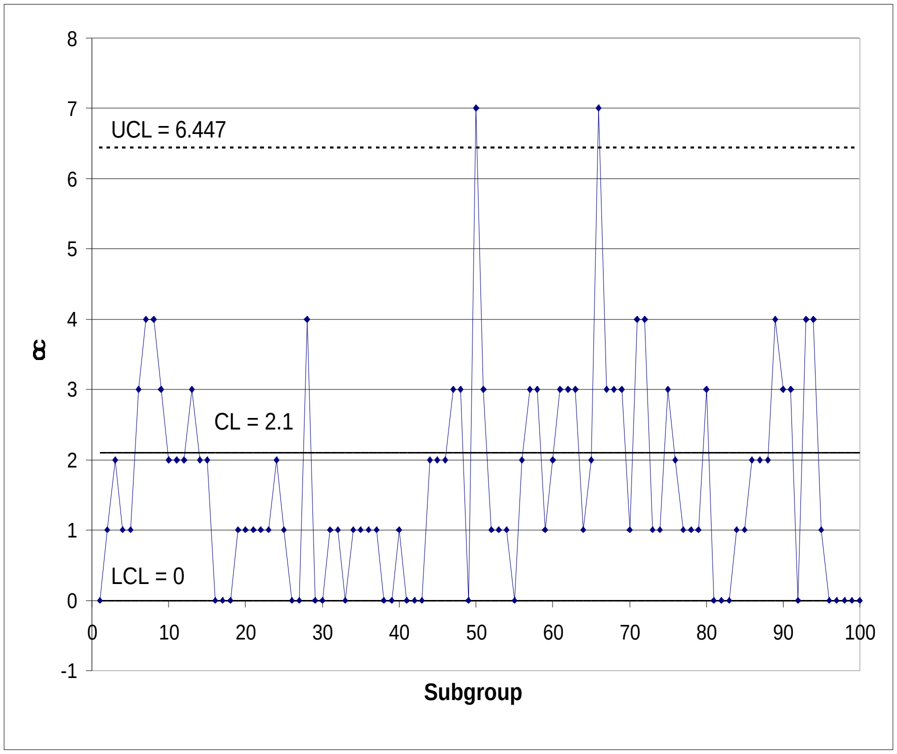


Figure 2 - c Chart for Promoted Combustion Operations

the control limits of the chart. The examination of safety logs and maintenance logs pertaining to promoted combustion testing operations for the previous year show no accidents or system failures. This indicates that the system possesses a relatively high degree of system safety. This fact corroborates the results of the application of the CHTFPM to promoted combustion operations.

The control chart shown in Figure 2 indicates that there is reason to suspect that the system may be becoming hazardous with respect to the sampled dendritics. This result provides the rationale to carry out a more comprehensive study of individual dendritic occurrences using Pareto analysis. This will provide an indication about which one of the dendritics has the highest frequency of occurrence. The Pareto analysis for the case study is depicted in Figure 3. The dendritics that did not occur during the data collection were not included in the Pareto Analysis. Pareto diagrams direct attention to possible problem areas even when an out of control situation does not exist. An experienced analyst can determine, from the Pareto diagram, an unusually high occurrence of a specific dendritic although it is still within an acceptable range.

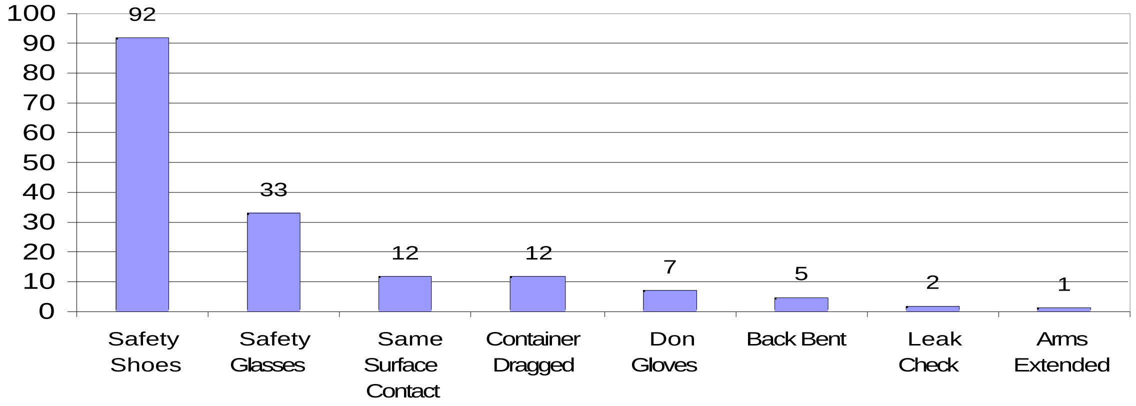
Considering the fact that the various dendritic elements were randomly observed, it is pertinent to conclude that each dendritic was given equal weight while performing the sampling study. In some situations, not all dendritics are equally important. In situations like this, what is needed is a method to classify dendritics according to severity and to weight the various types of dendritics in a reasonable manner. Montgomery's (___) demerit method using the first ten subgroups is used to calculate trial control limits. The parameters for the weighted *c* control chart are calculated giving:

$$CL = \bar{u} = 100\bar{u}_a + 50\bar{u}_b + 10\bar{u}_c + \bar{u}_d = 100(0.1) + 50(0.1) + 10(0.325) + 0 = 18.25$$

$$\hat{\sigma}_\mu = \left[(100)^2\bar{u}_a + (50)^2\bar{u}_b + (10)^2\bar{u}_c + \bar{u}_d\right]^{1/2} = \left[(100)^2(0.1) + (50)^2(0.1) + (10)^2(0.3255) + 0\right]^{1/2} = 17.906$$

$$UCL = \bar{u} + 3\sigma_u = 18.25 + 3(17.906) = 71.968\ ,\ \ LCL = \bar{u} - 3\hat{\sigma}_u = 18.25 - 3(17.906) = -35.468 \quad 0$$

Figure 4 depicts the weighted *c* chart using the above parameters, showing that Point 66 plotted out of control. Examining the sampling sheets that contain the data for point 50 and 66, one sees that three Class A dendritics occurred during subgroup 66 while only one Class A dendritic occurred during subgroup 50. The high number of Class A dendritics caused Point 66 to be out of control whereas Point 50 was not out of control because of the smaller weights attached to the dendritics that occurred in subgroup 50. Thus, the demerit scheme can be very useful when the classification of the dendritics is necessary due to their different degrees of seriousness.



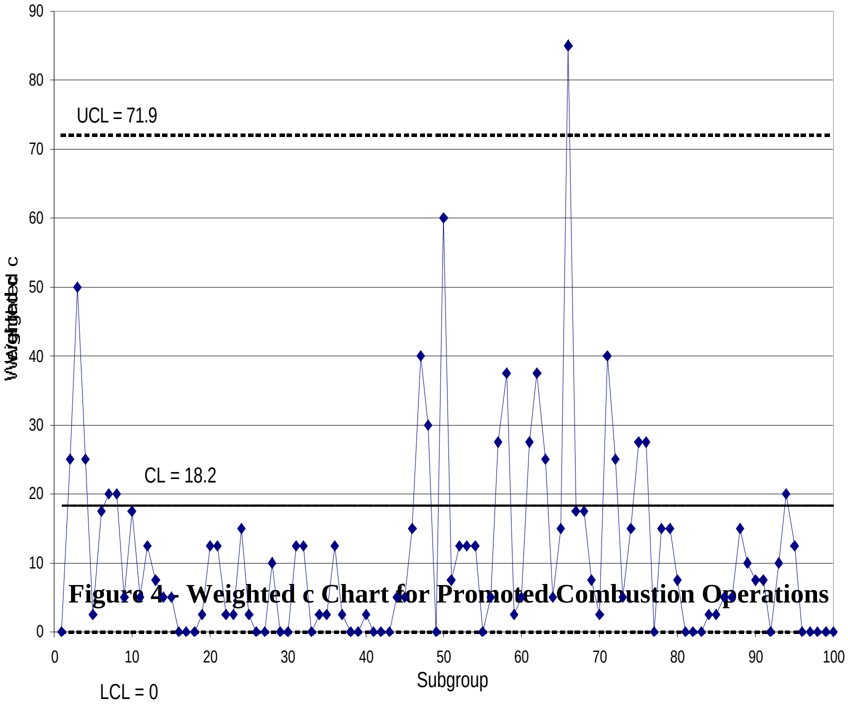


Figure 4 - Weighted c Chart for Promoted Combustion Operations

Conclusions

A predictive safety model for improving system safety has been developed. An initial risk and hazard analysis is performed on the system to determine the dendritics (the building blocks of hazards) of the system. Using the principles of work sampling and control charting, the safety status of the system is monitored for conditions that are becoming hazardous. If conditions are deteriorating, the control chart will give an out of control indication signaling the system analyst that corrective action needs to be taken to prevent an accident, system failure or unacceptable risk conditions. Condition monitoring continues, thus providing a check on the corrective actions taken.

Acknowledgements

This research was funded by NASA (NASA FAR GRANT NAG 10225). The authors acknowledge Mr. Eddie Davis at Marshall Space Flight Center for his insightful comments and suggestions, and Mr. Dean Byess, of NAS, Incorporated, whose extensive knowledge and technical assistance were instrumental in this research.

References

1. Feigenbaum, A.V., “Total Quality Control”, 3rd ed. McGraw-Hill, New York, 1951.
2. Grant, E.L., and Leavenworth, R.S., “Statistical Quality Control”, McGraw-Hill, New York, 1988.
3. Grimaldi, J.V. and Simonds, R.H., “Safety Management”, 5th ed., Irwin, Boston, 1989.
4. Juran, J.M., and Gryna, F.M., “Quality Planning and Analysis”, 2nd ed., McGraw-Hill, New York, 1980.
5. Kroemer K.H.E., Cumulative Trauma Disorders: Their Recognition and Ergonomic Measures to Avoid Them, *Applied Ergonomics*, vol. 20, pp. 274-280, 1989.
6. Montgomery D.C., “Introduction to Statistical Quality Control,” 3rd ed., John Wiley and Sons, New York, NY, 1996.
7. National Safety Council, Accident Facts, 1992 Edition, Chicago, The Council, 1992.
8. Roland, H.E. and Moriarty, B., “System Safety Engineering & Management”, John Wiley & Sons, NY, 1983.