Product Recalls: An Engineering Perspective

Exponent, Inc.

Jason L. Hertzberg

In recent years, extraordinary attention has been focused on the occurrence of consumer product recalls. For example, 465 consumer product recalls, involving 230 million product units, were conducted in the United States in 2009. [See Reference 1.] According to the CPSC, deaths, injuries, and property damage associated with consumer products place a societal burden within the United States of more than $700 billion dollars annually. Estimates for these costs include medical expenses, work losses, pain and suffering, legal costs, property damage estimates and other related factors. [See Reference 2.] In an effort to address the growing number of recalled products, Congress increased the maximum civil penalties for failing to report a potential substantial product hazard from $1.825 million to $15 million in 2009. [See Reference 3.] This dramatic escalation in monetary fine, coupled with the added potential for criminal penalties of up to five years' imprisonment and asset forfeiture, signaled a new chapter in the enforcement of consumer product safety in the United States.

Similarly, a raised awareness exists in the European Union. European manufacturers and distributors are obligated to notify regulatory authorities and to take necessary action (e.g., sales bans and recalls) if they become aware that they have placed a product in the market that might present unacceptable risks to consumers. From 2003 to 2008, the total number of such notifications increased from 139 to 1866, reflecting more than an order of magnitude increase. [See Reference 4.]

Given these recent developments, it is necessary for engineers who design and manufacture products to be familiar with technical considerations in the event of a potential recall. The following discussion addresses these matters.

Technical Considerations Regarding Potential Recalls

While basic requirements exist, the decision to report and potentially recall a consumer product is made on a case-by-case basis. [See Reference 5.] We will now outline a basic engineering approach that can help to determine, from a *technical* perspective, when and if to report a "condition" to the CPSC or other similar agency, and whether it is necessary to initiate a product recall. It is important for the reader to understand that 'reporting' a potential issue to the CPSC signals the beginning of an investigative period and does not necessarily mean that a product recall is imminent. The CPSC strongly encourages reporting, even if it is unclear whether a real danger or hazard exists. It is clear that a company must consider technical, as well as legal and regulatory perspectives when faced with a potential product recall.

In an engineering analysis of this kind, one can readily envision the need to address the following factors:

1. Determination of the Failure Process.
2. Identification of the Affected Product Population.
3. Assessment of Risk Associated with Product Failure.
4. Generation of an Appropriate Corrective Action Plan.

1. Determination of the Failure Process

To determine why a product has failed, a multidisciplinary approach typically is required. The range of expertise may include materials scientists, corrosion experts, mechanical, chemical and electrical engineers, and thermal scientists (i.e., fire cause and origin specialists). In addition, human factors (i.e., study of human-machine interactions) must also be considered, including an evaluation of warnings, labels, and instructions for the proper use of a given product.

To determine why a product has failed, it is necessary to identify the steps involved in the failure process and, if possible, the root cause that triggered that process. It is important to first distinguish between the terms *root cause* and *failure process*, as they are sometimes used interchangeably. The *root cause* is the fundamental, underlying reason for the failure. A *failure process* is the process by which final failure takes place. As such, if the *root cause* is removed or avoided, the *failure process* does not occur.

As an example of this distinction, consider the following fictitious scenario: A leading parts manufacturer sells thousands of seemingly identical rods to a medical device company. The rod is part of an implanted medical device that provides mechanical support in the body for an extended period of time. The rod design was used successfully for many years, with the exception of a single recent failure. Upon microscopic examination of the fracture surface of the explanted rod, it was determined that the rod failed by a fatigue process, indicating that the rod had been cyclically loaded during service. Furthermore, it was determined that a single fatigue crack initiated at a metal forming-induced surface discontinuity. In this hypothetical case, the *root cause* of the failure was a manufacturing defect; in turn, the *failure process* consisted of fatigue crack initiation at this forming-induced defect, fatigue crack propagation, and subsequent overload fracture of the rod's remaining unbroken ligament. It is important to note that an appropriate corrective action plan sometimes can be constructed even if the root cause is unknown.

There are many aspects to an engineering failure analysis investigation. The more information that is available for review, the more likely a complete understanding of the failure can be achieved. When faced with the failure of a product containing

many components, 'system level' data are often required. Examples of such additional information include:

1. A summary of events leading up to the incident, eyewitness accounts, incident reports/photographs, and documentation of product handling after the incident.
2. Application specific information including how and where the product was used.
3. The service/maintenance history of incident product(s) and similar models, including reports of previous issues.
4. The 'fingerprint' of the product including: the product manufacturing date; serial number; specific model and batch numbers; and the manufacturing facility where the product was assembled.
5. Any available product documentation including both design and manufacturing assembly drawings, operation manuals, warnings and instructions.
6. The timeline of product evolution, including changes in product design, materials, components, construction, packaging, warnings and instructions.
7. The quality control procedures incorporated by raw material vendors through the various manufacturing and assembly operations, including material certification sheets.

After reviewing these available file materials, the first step in determining the root cause and associated failure process involves a non-destructive analysis of the incident unit(s). This typically consists of a visual examination and photographic documentation of the product and, if possible, the surrounding environment at the time of the incident. All available markings and labels on the product should be recorded, as this information can sometimes be useful in limiting the extent of affected product. It is also prudent to perform a thorough examination of damage to the product.

Mechanical damage (e.g., impact, wear) can provide insight into the use or misuse of the product and the loads experienced during its lifetime. Patterns of thermal damage can provide insight into the origin of heat, smoke, or flame. In some cases, it is possible to pinpoint the region or even the component responsible for a fire, depending upon the degree of damage to the product. It is important to note that thermal damage patterns can be marred or inadvertently destroyed during handling or product removal from the incident site. Therefore, careful attention should be given to preserving both the product's thermal damage patterns as well as the surrounding environment for subsequent analysis.

X-ray imaging represents a powerful non-destructive method to examine the product's interior without the need for disassembly. Depending upon the densities of the materials of construction, it is sometimes possible to determine the extent of damage to inner components without disturbing their condition or relative position. Other potentially insightful non-destructive techniques are available which can be used to detect the presence of surface cracks. [See Reference 6.]

In most cases, non-destructive evaluations provide an incomplete assessment of the failure event; accordingly, a destructive examination is typically in order. However, once a product is altered from its original condition, valuable information can be permanently lost if proper procedures are not followed. Therefore, it is very important to carefully document product disassembly and the individual steps associated with the destructive examination protocol. In addition, if legal action has been taken or is pending as a consequence of the product failure, it is necessary to perform any destructive analysis in the presence of interested parties in order to avoid problems related to evidence spoliation.

After the product has been disassembled, it is often useful to examine the components at higher magnifications using optical and/or scanning electron microscopy. It is often possible to identify macroscopic and microscopic features that indicate the nature of a failure or the existence of a material or manufacturing defect. In addition, it is also possible to evaluate the chemical composition of a component using various methods, including energy dispersive x-ray spectroscopy. This can be helpful in determining the materials of construction, as well as the existence of contamination or corrosion products which may have contributed to the product failure. If chemical state information is required in order to determine thermal history or environmental effects, x-ray diffraction methods can be used to identify unknown crystalline phases. In some cases, it is possible to estimate the temperatures achieved during an overheating event by the colour of a metal oxide.

Important insight into the foreseeable use and/or misuse of a product can also be gained by reviewing the associated warnings, labels, and instruction manuals. Some of these deficiencies include:

1. Unclear or inaccurate description of required steps and/or precautions involved in assembly, operation, or maintenance of the product.
2. Ineffective placement of warning labels on the product.
3. Ineffective or inappropriate use of textual and pictorial components of the warning labels. For example, "Danger", "Warning", and "Caution" are terms used to convey decreasing levels of hazard. [See Reference 7.]
4. Ineffective usage of background colour or foreground text font and/or colour for warning labels.

Exemplar products, specifically new and identical products with respect to construction and function, serve as useful tools during these types of investigations. Laboratory testing of exemplar products makes it possible to support or refute proposed failure processes by evaluating various potential incident scenarios. The engineer can then determine if the test results are consistent with reported failures and the condition of available incident products.

2. Identification of the Affected Product Population

Once the failure process has been identified, it is important to determine if the product's failure is an isolated event or if a "pattern of defect" is identified. In this regard, it is prudent to carefully review available databases including product returns, warranty claims, customer complaints, and reported incidents. This exercise should be conducted on an ongoing basis to help determine recent trends in the nature of product failures and to compare this information with historical data. For example, is this the first product to be returned or is this the 20th product to be returned in the past three weeks? If there is a spike in the number of returns, are these failures of a similar nature? To answer these questions, a detailed examination of available failed products is often required. If none are available to examine, it is beneficial to review all available photographs and reports associated with these incidents.If a 'pattern of defect' is established, it is then necessary to determine the population that is potentially affected. Some of the important questions for an engineer to consider in this determination include:

1. Is there an inherent design issue? For example, are the material properties or performance characteristics inadequate? Is the problem associated with a defective component purchased from a supplier? Is this component single-sourced or multiple sourced? If the problem is with only one component supplier, is it possible to distinguish the affected population from the total product universe?
2. Within a given production facility, is there a batch problem tied to a manufacturing process deviation?

3. Is this problem associated only with certain models of the product? For example, are there differences in product construction that influence product susceptibility to a specific failure mode or unsafe condition? Can these performance differences be verified empirically?
4. Are there geographical considerations that make it possible to rule out certain populations of product? For example, are electronic products more likely to overheat and cause fires in certain countries based on standard power outlet voltages (e.g., a 110-volt supply is standard for wall outlets in the United States, whereas 220-volt service is standard in many parts of Europe)?

In many cases, the answer to the question, "How many products are affected?" can have a profound impact on a company's financial stability, especially if a recall is ultimately required. As the author has seen firsthand, the answer to this question can sometimes determine whether a company can emerge relatively unscathed from a product crisis or, instead, be forced into bankruptcy.

3. Assessment of Risk Associated with Product Failure

The risk associated with a product failure is generally expressed as a function of both the frequency of occurrence within the product population and the severity of its associated consequences. Accordingly, it is possible to assign a higher risk level to 1,000 products in the field that have a slight chance of failure resulting in serious harm as compared with 1 million products in the field that will likely fail but would cause little or no harm.

Analytical tools are helpful in evaluating the risk associated with various failure scenarios. To illustrate, Failure Modes and Effects Analysis (FMEA) is a *qualitative* risk assessment framework typically used to prioritise risk before a product is introduced to the marketplace. A traditional FMEA quantifies risk in terms of three categories: severity; probability of occurrence; and detection (i.e., the likelihood that existing process controls will detect this failure). Each category is rated on a relative scale (e.g., 1 to 5), with a lower rating corresponding to lower risk. The ratings for the three categories are multiplied together to calculate the risk priority number (RPN). The higher the RPN value, the higher the overall risk of a potential failure. By assessing risk using this framework, it is possible to logically and consistently compare relative risks that can be difficult to otherwise evaluate, similar to the European Union approach to risk assessment.

During an actual recall investigation, it is useful to review prior FMEA findings to challenge the assumptions made during the initial product development stage. When conducting such an investigation, there is usually little time to perform a complete FMEA to document all possible failure modes for all components; besides, analyses of many components may well be irrelevant to the problem at hand. In cases where a very specific failure mode is being investigated (e.g., an electrical fire), a targeted FMEA could be considered that is focused on all possible ways in which relevant components can cause that specific failure mode to occur. This represents a worst case analysis of consequences resulting from individual component failures, but does not address system level effects. Clearly, though a focused FMEA does not provide perspective on the overall risk profile for the product, it may represent an effective way to quickly identify the issues relevant to the problem that precipitated the current product crisis.

A Fault Tree Analysis (FTA) represents another valuable tool that can be used during a product recall investigation. Rather than being limited to individual component failures, FTA is a *quantitative* risk assessment methodology whereby the engineer identifies combinations of component or subassembly failures that can result in an incident or 'end point'. Using this approach, one begins with the final result (e.g., a fire) and works backwards from that event. The engineer assigns probabilities of failure to the individual steps required to create the specific 'end point'; this makes it possible to assess the overall risk of a failure. To enable the engineer to assign (i.e., estimate) the probabilities of events in the failure process, references can be made to existing databases that contain field failure data as well as component failure rates [see Reference 8] for various parts (e.g., fans, power supplies, and pumps). [See Reference 9.] Since FTA is a quantitative method, the probability of a specific 'end point' then can be calculated by multiplying together the probabilities of each step. For example, assume there is a 1% probability that each of three separate, sequential steps will occur. If all three steps are required to produce an 'end point', the probability of this resulting hazard is calculated to be 10^{-6}.

In order to fully understand the potential consequences of a product failure, targeted "worst case scenario" laboratory tests should be performed, if possible, to simulate a "perfect storm" with regard to foreseeable conditions. These tests can be more aggressive than those addressing proposed failure process(es). The purpose of these targeted tests is to determine the most extreme consequences in the event of a catastrophic failure, rather than just those observed in the reported failures. This approach can be used to determine if the malfunction of a product will lead to a potential safety hazard or merely a nuisance to the user. This type of information can be useful in deciding whether or not to recall a product.

As such, FMEA and FTA analytical tools enable an engineer to determine relative and actual risk values associated with a specific failure event; laboratory testing can certainly provide additional valuable insight. Nevertheless, the ultimate question remains: What level of risk is *reasonable*? Let's first consider the annual number of eye injuries associated with pens and pencils, as reported in the National Electronic Injury Surveillance System (NEISS) database. [See Reference 10.] NEISS is a publicly available and searchable CPSC database that contains statistically valid national estimates and specific information about product-related injuries that are treated in hospital emergency rooms. According to the database, an estimated 495 adult eye injuries associated with pens and pencils occurred annually between 2001 and 2004. While these writing implement-induced injuries are unfortunate, pens and pencils have not been removed from the marketplace and will likely continue to be the writing implements of choice in the future. As is the case for a kitchen knife, just because injuries are associated with the use of a product does not necessarily make that product unreasonably dangerous, nor does it necessarily imply that the product requires a design change. Pens and pencils have very sharp points that can find their way into one's eye if care is not exercised. Consumers willingly accept the inherent risk associated with these indispensable consumer products given the benefits received in the form of their low cost and functionality; therefore, this particular risk is deemed reasonable by society.

An insightful view of reasonable risk was published earlier by Tetelman and Starr [see Reference 11]. These investigators sought to understand acceptable societal risk in terms of the fatality rate in the United States from all causes; primarily using old age and disease factors, they calculated death events to occur at a rate of about 1% per year or approximately 10^{-6} per exposure hour. Based on this estimation, the probability of a "natural" death was determined to be an approximately "one in a million" per exposure hour event. According to Tetelman *et al*, risk data suggested that a 10^{-6} level might be considered as a baseline for assessing the risk posed by activities (and associated products) such as driving an automobile and/or by using commercial aviation. (Ironically,

Tetelman was killed in a commercial airline mid-air crash in 1978 while en route to an air safety conference.)

Tetelman *et al* pointed out that risks associated with certain activities and/or products during their initial introduction into the marketplace are relatively high and that, over time, these risk levels tend to decrease to this 10^{-6} baseline level. For example, during the early 20th century, the risk of fatality as a result of an automobile accident was far greater than the risk level due to natural causes. Over a period of time, the number of drivers increased dramatically while significant improvements were made with regard to vehicle safety and driver awareness. As a result, the risk level associated with driving approached an equilibrium value of 10^{-6}, the risk level due to natural causes. By contrast, the probability of death from "pure chance" events like lightning strikes was determined to be 10^{-9} per exposure hour, significantly lower than that associated with natural causes, as would be expected. While the reader may assume that there is universal agreement that the range of 10^{-6} to 10^{-9} per exposure hour would define the spectrum of acceptable risk (defined by the fatality rates associated with all causes and pure chance, respectively), this is not necessarily the case. For example, some individuals choose to lower their pure chance risk levels by never venturing outdoors when thunderstorms are predicted. The distinction between reasonable and unreasonable risk is clearly difficult to pinpoint or define; however, it is clear from both a judicial and regulatory perspective that the threshold for acceptable risk has been reduced considerably over the course of time (e.g., comparing societies from before the industrial revolution to those corresponding to the 21st century).

4. Generation of an Appropriate Corrective Action Plan

If the decision is made to recall a product, it is necessary to determine the most appropriate remedial action, commonly referred to as a corrective action plan. This plan, including notification of the customer, can take one of several different forms including: a customer or service technician implemented fix using a repair kit sent from the manufacturer; complete removal of all products from the marketplace; or an exchange for a new model. Though the original hazard(s) will be sufficiently mitigated or eliminated by implementing an appropriate fix, it is critical to avoid the introduction of new hazards as a result of a proposed corrective action. Therefore, it is prudent to carefully review potential correction actions, especially if a customer implemented fix is the preferred solution. This evaluation should assess the ease of implementation and determine what can go wrong during the process. Detailed instructions along with visual aids must be provided to the individuals performing the repair. Testing these procedures with individuals unfamiliar with the product can also be an insightful exercise during the development of remedial procedures. The bottom line with any corrective action plan is to consider the KISS principle of basic design: Keep-It-Simple-Stupid.

Proactive Considerations

Thus far, we have discussed technical aspects that must be considered when addressing a potential product recall. Having reviewed these aspects relating to the "back end" (i.e., product recall investigations), the reader can now understand and appreciate the importance of focusing considerable effort on the "front end" (i.e., product design and development stage) to avoid or, at the least, minimise the impact of a product recall. The elements of a product recall prevention and management initiative may vary, but an effective approach should consider the following components:

Think Like a Consumer

During the product design process and when generating instructions and warnings, it is critical for engineers to consider how consumers might interpret written instructions and warnings and how they might conceivably use their products. Thus, questions such as "Are the supplied warnings and instructions clear?" or "How might they be interpreted or misinterpreted?" are relevant to those charged with designing or evaluating products. As discussed, faulty product instructions, warnings or labels alone can constitute a product defect worthy of a recall, even if the product itself is not defective. Thinking like a consumer is a fundamentally important concept; incorporating this view into the product design process can raise awareness of important human factors before the product ever reaches the consumer.

Test Products Thoroughly

Risk analysis can take place in a variety of forms, including FMEA and FTA, as discussed. These are powerful tools in determining how a product can fail, especially when they reflect the experience of seasoned engineers and subject matter experts. After performing an FMEA, for example, a company can rank the risks associated with a product and then test accordingly to validate design assumptions and determine if additional action is required.

Problems can result when companies do not perform comprehensive testing of their prototype products before they arrive in their customers' hands. In some cases, products can fail in a manner that was not anticipated, thereby creating safety hazards. Various types of design validation tests can shed light on possible failure scenarios and resulting consequences. These include normal-use tests, in which the product is used in accordance with the instructions; misuse tests, in which the product is tested in ways that are reasonably foreseeable, (i.e., not precisely according to the instructions but in a manner that might be reasonably extrapolated from conventional use); and abuse tests, whereby the product is purposely abused with an aggressive testing approach to see what might happen. In addition, forced-failure tests can be performed to simulate the failure of specific components to determine the associated consequences, similar in concept to the "perfect storm" approach discussed earlier. If accelerated life testing is contemplated, care should be exercised to ensure that only operative failure modes are explored.

After completing this type of analysis, instructions can be revised and the product design can be modified accordingly.

In many cases, consumer products are evaluated by a certified testing laboratory (e.g., Underwriters Laboratory) to verify compliance with voluntary or mandatory standards; however, these tests should be considered as minimum requirements to be satisfied, as they do not necessarily prove that the product is entirely safe. In fact, testing to standards developed for classes of products is no substitute for product-specific testing. Testing should be considered for those scenarios not covered by voluntary or mandatory standards. It is easier and far less costly to understand how your product might fail during prototype or qualification testing in a laboratory than when in use.

Ensure Adequate Traceability

Good recordkeeping will increase the likelihood of traceability if a problem occurs. Creating a product "fingerprint" can help narrow

or define the extent of a problem and help clarify which products might be affected. In some cases, an engineering-based argument can be made for why a product recall need only be conducted for a specific population. Comprehensive documentation and product traceability can then allow a company to put a fence around the problem and limit costs associated with a total recall. *You cannot limit the scope of a problem if you cannot confirm the problem's boundaries.*

One example of a high level of traceability can be found in the watch industry. Schwab-Feller AG is one of the few companies in the business of manufacturing mainsprings which power mechanical watches. Their entire process involves a large number of individual steps, including numerous rolling operations, cutting, finishing, cleaning, polishing, heat treatment, spot welding, coating, and baking. Every spring lot is marked with a bar code identifier that enables the company to track the spring back to the raw material stage. In addition, it is possible to identify when the mainspring was fabricated and the individual who performed each step of the process. [See Reference 12.]

Manage Change Carefully

In some cases, a safe product is produced for a period of time and then something is changed. This modification may be a result of consumer feedback, a new component supplier, a manufacturing process change to increase efficiency, or perhaps new environmental regulations. Unfortunately, even minor changes can have enormous safety implications. In these circumstances, it is important to conduct those tests that will evaluate the effect of the proposed change(s) on product performance. For products without an historical risk analysis, this may be the time to update files and revisit technical assumptions.

References

1 United States Consumer Product Safety Commission's 2009 Performance and Accountability Report, www.cpsc.gov, November 2009, p. 6.

2 15 U.S.C. § 2064(b).

3 The Consumer Product Safety Improvement Act of 2008.

4 Keeping European Consumers Safe, 2008 Annual Report on the operation of the Rapid Alert System for non-food consumer products, RAPEX, The Directorate-General for Health and Consumers of the European Commission, Office for Official Publications of the European Communities, 2009.

5 16 CFR Part 1115.

6 ASM Handbook, Non-destructive Evaluation and Quality Control Section, Volume 17, 1989.

7 ANSI Z535.4-2002, American National Standard For Product Safety Signs and Labels, American National Standards Institute, Inc.

8 Military Handbook, Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, Department of Defense, 1991.

9 Nonelectronic Parts Reliability Data (NPRD), Reliability Information Analysis Center, Department of Defense, 1995.

10 http://www.cpsc.gov/library/neiss.html

11 Social Consequences of Engineering, "Chapter Ten- Public Risk and Engineering Safety: How Safe is Safe Enough?", edited by Hayrettin Kardestuncer, Boyd & Fraser Publishing Company, San Francisco, 1979.

12 Watch Time Magazine, December 2008, p. 237.

Jason L. Hertzberg, Ph.D., P.E.

Exponent, Inc.
185 Hansen Court, Suite 100
Wood Dale, IL 60191
USA

Tel: +1 312 952 8943
Fax: +1 630 274 3299
Email: jhertzberg@exponent.com
URL: www.exponent.com

Dr. Jason L. Hertzberg is a Director and Principal Engineer at Exponent, Inc. He has extensive experience solving complex technical problems in a wide variety of industries. In the area of consumer products, Dr. Hertzberg often performs targeted testing of new products, management of change during production, use of risk methodologies, substantiation of product performance claims, failure analysis of field-returned products, product recall investigations, evaluation of proposed correction action plans, and products liability. Dr. Hertzberg routinely addresses issues related to the mechanical behaviour and degradation of materials. He also has a strong background in mobile computing with extensive experience with handheld device technologies, having served as the Director of Competitive Analysis for Palm, Inc.