WHAT TO DO WHEN THINGS GO WRONG
AN ETHICAL SOLUTION

IEEE Petroleum & Chemical Industry - 2007

Robert A. Durham, PhD, PE
Member, IEEE
D^2 Tech Solutions, Inc.
PO Box 470926
Tulsa, OK 74147-0926
rdurham@d2ts.com

Marcus O. Durham, PhD, PE
Fellow, IEEE
THEWAY Corp
PO Box 33124
Tulsa, OK 74153
mod@superb.org

Abstract - What do you do when a piece of equipment fails, a contract is breached, or a design is challenged? Engineering training is focused on how to design or analyze a piece of equipment, but seldom involves skills necessary to resolve disputes or discrepancies. Occasionally things go awry. There are at least 10 issues that impact the decision to proceed with a failure case: Objective, Ethics, People, Time, Money, Technology, Quality, Safety, Environment, and Legal. The impact of these on a project is investigated in various contexts. A flowchart is proposed as a guide. A process of using them to evaluate the project is then developed. The first part is the technical issues: stop loss, gather data, determine origin, find cause, conduct analysis, research outside influence, and develop an opinion. The non-technical process is determining whether to recover or move on. Frequently, by following this analysis, problems can be mitigated before catastrophe. If there is a major event, the analysis provides a technique to evaluate the cost and make appropriate economic decisions.

Index Terms — Forensic engineering, failure analysis, risk management, project management

INTRODUCTION

"The problem is to find the least erroneous solution."
- Justice Benjamin Cardozo [1]

What do you do when a piece of equipment fails, a contract is breached, or a design is challenged? Formal technical training is focused on the skills necessary to design or analyze a piece of equipment. Seldom does it involve the skills necessary to resolve disputes or resolve discrepancy issues. [2]

What is the role of a engineer in error handling? Engineers determine what makes things work; as a result, they often become the first responders in forensic investigations. The engineer's investigation provides the basis for attorney's arguments during litigation.

By nature and training, engineers assume that their analysis is right and their way is the correct way. However, in a forensic investigation, there are usually experts on both sides of an issue. How is this discrepancy resolved?

English common law provides the basis for our system of jurisprudence. Lord MacMillian, Lord Chief Justice of England, wrote"In almost every case except the very plainest, it would be possible to decide the issue either way with reasonable legal justification."[1]

PROJECT TRADE-OFFS

A project is an extensive undertaking of multiple tasks for a definite purpose for a set time. To determine the status of a project, it is necessary to determine the standing of all of the issues involved. These are not ideals; they are the principles that define any project or venture.

The return on a project is simply the income less the expense. This is true not only in a monetary sense, but can be applied to other issues as well. The objective of a successful project, company, or any endeavor is to maximize the return on the investment.

The classic trade-offs for a project are time (t), money ($), and quality (Q). These components are actually constraints that can be combined into an energy equation.

*project energy = maximization of (Q * $ / t)*

Money flows from the customer to the project, and then to the supplier. The goods flow in the opposite direction. The customer's goal (energy) is to maximize quality and minimize money (expenses or costs), and to do so in the minimum time frame. The supplier's goals (energy) are to meet minimum quality standards, and to maximize money (price), in the budgeted time frame.

In a closed system with no other influence, the total energy is zero. Applying this principle, the supplier energy must equal the customer energy.

$$[(-Q_s)\ (+\$_s) / t_s] = [(+Q_c)\ (-\$_c) / t_c]$$

There is, therefore, a natural tension that develops between a client and supplier. The key purpose of a leader, whether it be a project engineer, project manager, manager or executive, is to produce a winning combination that effectively balances the interests of both the supplier and client.

The value of a product or project is the ratio of money to quality. This ratio is relatively constant: If quality decreases, it is expected that the money will decrease. If quality increases, price can be expected to increase. You cannot get "something for nothing." There is a minimum limit on quality and a maximum limit on money that a client will accept. The converse is true for the supplier.

Negotiation is the process of bringing the quality, money, and time, which are the interests of both the supplier and the client, into balance. The basis of all disputes is a perceived disparity in the quality, money, time, or some combination of all three.

SKILLS

Three skills are required for any project – people skills, money skills, and technological skills.

As people skills are often the most important, they are dealt with first. The first question is “is this the right person?” Is the person in the right place? Is the person performing adequately?

These questions require a substantial knowledge of the individual. What is his temperament? What is his relationship style? What is his experience? Is he flexible? Is he a problem solver? Does he understand the difference between doing the project and making the project successful for the client and the supplier? No one is perfect on all these issues. What is your plan, then, to balance and compensate for the weaknesses?

The technological skills apply to both the person and the equipment. Is the technology adequate to do the job? What are alternative technologies that may be better quality, more cost effective, or better for the time? Similarly, does the person understand the technology and its applications?

The money issue applies to revenue and expenses? Is the income being received? Is it adequate to do the job? Are the expenses in control? Can expense be managed without adversely affecting quality?

HOW TO TELL

How can you tell when something is going wrong? In some circumstances a catastrophe occurs. There is a big event that grabs your attention. In most cases a disaster is the result of attrition. Little things start compounding. In those cases, evaluation of the situation, and possible options for remediation, returns to the three constraints: Quality is suffering, money is out of line, or the timeframe is too long.

Often the first indication that something is amiss is a feeling. It is often not definable, but there is a sense that things are not as they should be. Generally, this is caused by the engineer subconsciously picking up clues about the three constraints that have not been adequately resolved. If there is a feeling that problems may be rising, it is important to perform an analysis to see which of the three constraint items is out of bounds.

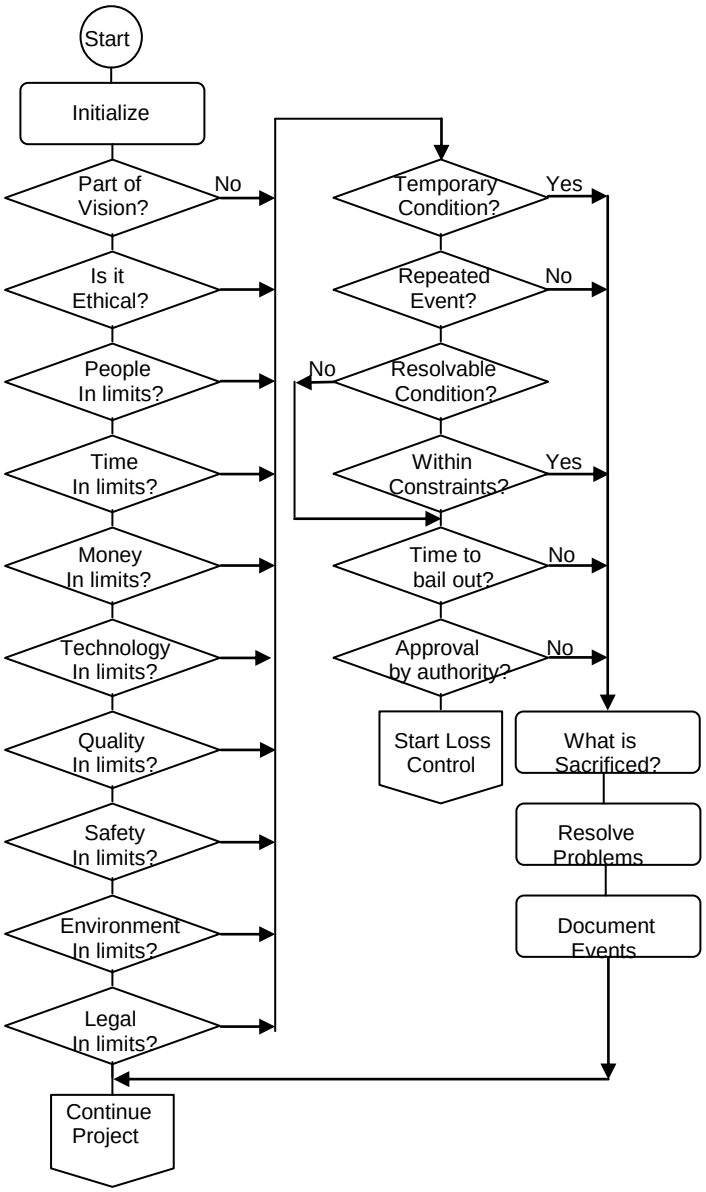
This analysis can be a series of questions or it can be a flowchart. Develop the questions or flowchart before the process begins. Once questions or decisions are defined, then there must be some boundary for each condition. Is the quality in limits? Is the schedule on track? Are the expenses under control?

Any item that has a negative answer then requires another series of questions. Is the problem temporary or on going? How long has it been going on? If the problem is on going, there is a final series of queries. Is the problem resolvable? Can it be done within the quality, time, and money constraints? If either of those questions are negative, then one question remains, is it time to bail out?

DECISIONS

The following flowchart is a good monitoring tool that should be evaluated on a regular basis. This flowchart gives the series of questions to ask. Some of these questions need to be answered with a probability function, rather than a yes/no response. Nevertheless, ultimately there comes the point of a go, no-go decision.

Evaluation Process



Whether used by an experienced leader or a novice engineer, the questions in the flowchart are the series of decisions that must be made. The novice may not have the

judgment to make precise evaluations; nevertheless, he can develop a plan of attack to hone that experience and skill.

If, as a result of this analysis, the decision is made to continue the project, then the evaluation process must be continued. It is not necessary for this to occur daily, but it should be performed regularly. Moreover, when there is a sense of something being amiss, this process provides a method of detecting the source.

If the decision is made to cut your losses and run, then the real challenge begins.

RISK MANAGEMENT

Often an engineer will be requested to pick up the pieces when there has been a catastrophe or a project failed to perform as expected? There is a very methodical process that must be followed, if risk is to be minimized.

1. Stop the loss
2. Gather data, photos, physical evidence, personal statements
3. Evaluate options
4. Determine consequences
5. Prepare report (written, verbal, memorial file)
6. Make decision whether to attempt recovery
7. Start recovery

STOP LOSS

The first objective is to stop the loss if it is continuing. The procedure used depends on the nature of the problem. Some of these require professional or expert assistance.

If there is personal injury, obviously reducing the impact or providing assistance comes first. Request professional help, even if you are certified to render assistance. Personal injury is a prevalent form of legal claims.

In the event of a fire, stop the progress if it is small enough. Do not expose yourself or anyone else to injury to reclaim anything. No item is worth the exposure that fire causes. Often the biggest risk is smoke inhalation, which exposes the body to toxic substances.

Seek professional assistance to assure the fire is under control. We have investigated numerous cases where the fire department was on site to extinguish a blaze. After they left, a smoldering substance under a cover proceeded to cause a secondary blaze. The second fire often causes much greater damage than the initial incident.

If investigating an incident, be cautious to determine the original cause. It is easy to be deceived by the secondary origin.

If the problem is a mechanical, electrical, or chemical malfunction, remove the energy source so it cannot cause more damage.

If the incident is a people problem, remove them from the process. This must be done with care and finesse. Determine established policy and legal requirements.

If the incident is financial, control the flow of cash. This may be by placing constraints on who can spend. Although this is the issue that often gets the most attention, it is also the easiest to monitor and to control.

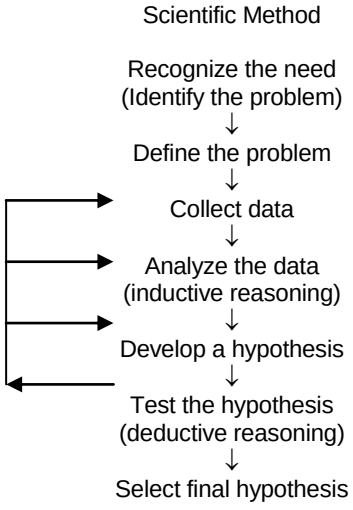
GATHER DATA

Gathering data to be used for later evaluation, as well as justification of actions, is the next step to take. Data takes many forms. It can be documents, photos, personal statements or physical evidence. Each has its own value, but the principles are equivalent. [3]

Any evidence collected must be protected in as pristine condition as possible for future evaluation by others. Only representatives of the owner, or law enforcement, can collect evidence. Wrap the material, label it, and store in a secure location.

There are numerous standards for gathering data that are published by professional organizations. [4,5,6] These address specific, often detailed, requirements for their clientele. [7,8]

The National Fire Protection Association (NFPA) is a major source of these documents. Their *Guide for Fire and Explosion Investigations* is the authority across the industry. [9] This document includes basic methodology using the scientific method to develop a hypothesis. Although the discussion in this paper is specifically about catastrophes like fire, its principles are valid for any risk management.



Gather information from all sources. There are two types of observers: Fact observers are ones that have first hand experience with some facet of the problem. Expert witnesses are ones that research and analyze the information and come to some conclusions. Experts have special knowledge and education.

When the expert is gathering sources of information, first-hand observers are preferable. Hearsay information must be filtered, but may indicate a direction of research that should be pursued.

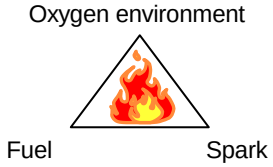
If it is possible for the expert to observe the problem after the damage, but before it is cleaned-up, he may also become a fact witness.

Record all observations for later analysis. Take detailed photographs and log each photograph so it can be identified later. The most credible photographs use Polaroid technology, because of their inability to be altered. It is also the least durable, most expensive, least convenient, and provides the least detail. High resolution digital is now accepted in most jurisdictions. Evaluate the situation and determine what technology is most appropriate. Any picture is better than none.

PUTTING OUT FIRES

Fire investigation is an excellent analog for any problem. The terminology is embedded in our language, and is relatable to anyone. 'Putting out fires' is often used as a metaphor for 'problem solving.' Although fire investigation is a very analytical process that requires substantial knowledge, training, and experience, it is also very intuitive.

To begin, three things must be present to have a fire - fuel, oxygen or environment, and ignition or spark.



Remove any one of these and a fire cannot exist. Similarly for any failure or breach, there must be fuel, an environment for the problem to develop, and a spark that ignites the conflict. Elimination of one or all of these factors before ignition is much easier than trying to contain the damage once the incident has occurred.

ORIGIN

What is the point of origin? Begin with the big picture. Look at all events and surroundings. From these, develop the pattern that points to the origin of the conflagration. There is a classic "V" shape that derives from the origin of a fire. Flames will burn up and out from the point of ignition. Very little damage will be below the point of origin. The smoke and burn pattern will be in the direction of airflow. The exception is a very flammable item than may burn down.

The pattern is observable from the perspective of the surrounding area, down to the very detail. Catastrophic damage may obscure the detailed pointing.

Years of experience can provide background, previous observations, and a sense of feeling. This very exposure may cloud some observations since the observer may be too close to the problem. An insightful, knowledgeable analyst will often notice a subtlety first. To use the common vernacular, it is hard to see the forest for the trees.

At this juncture only the location or origin of the problem has been identified, not the root cause.

CAUSE

What caused the failure? Begin with detailed observations and then move to a generalization about the area. This involves considering all possibilities in the area of the origin. List all possibilities, no matter how obscure.

The cause must have fuel, necessary environment, and ignition source. Eliminate possibilities one by one if they do not have all three components. For each possibility, note why it was eliminated.

Continue to eliminate possibilities, until arriving at the most probable cause.

ANALYSIS

Why did the failure occur? Begin with specifics rooted in technology. Technology primarily applies to the energy source, which may be a mechanical, electrical, or process issue. In virtually all systems, all three energy sources exist; therefore, it becomes a task of finding which source is the primary cause. Then determine the component that had the problem.

There is generally more than one issue that causes a failure. Analysis involves finding all of the conditions that came together at the time of the failure.

The components of a system are actually quite limited.

Component	Realization
Input	Energy source or data
Protection	Safety system or error checking
Change	Switch, valve, or decision
Path	Conductor, pipe, or method
Connection	Joint or fitting
Sensor	Monitor or detector
Control	Feedback system
Warning	Alarm or annunciation
Output	Display or result
Process material	Stuff that is handled

Each of these should be investigated to determine if it was part of the problem. There is seldom a yes/no answer, so it may be necessary to assign probabilities to each question. Eliminate the components that are not involved. Continue the elimination until the most probable component or components are identified.

Based on a quality assumption, the overriding consideration is very similar to the physicians' Hippocratic oath, "Above all, do no harm." It is more important that the system not harm than it is for the system to operate in a particular way.

With that theory in mind, some items take on a greater precedence. These are safety components, which include

protection, feedback, and warnings. *Protection* is the safety component that should isolate the energy source if something goes awry. *Feedback* is closed loop control that provides compensation if something gets out of range. Open loop control is not stable. *Warning* is the message about risks to preclude something going awry.

Component	Function
Protection	Isolate
Control	Compensate
Warning	Preclude

EXTERNAL

As noted earlier, seldom is it one component that causes a failure. Once the components are identified, the external influence that contributed to the failure is researched. The problem could be one of design, manufacturing, or application.

Design is the systematic process of contriving plans for a particular purpose. Design implies a special knowledge about the technology that will provide a product for the intended purpose and will operate safely. Design compromises are necessary to produce a viable project. Nevertheless, the designer is expected to know, and should know, the technical problems that could occur and take actions to mitigate them.

Manufacturing is the process of putting components together into a working system. Manufacturing implies the ability to create, produce, or turn out a finished product. Manufacturing is often done with a relatively low margin. This is necessary for profit in a competitive environment. Efforts are made to reduce costs as much as feasible. As a result, compromises may be used to save money. These compromises must be commensurate with quality and safety.

Proper management techniques, appropriate design, and suitable manufacturing and testing procedures will provide a safe product. Failure to use available safety procedures will expose the manufacturer and end user to unnecessary risks.

Application is how the system is employed. This is under the direction of either the user or owner. The system is typically intended for use by consumers, without explicit technical knowledge about the design, manufacturing, or constraints. The user has the responsibility to apply the device or system in a prudent method. The user is expected to not work on or modify the system. Furthermore, he is expected to not abuse, physically damage, or overload the device.

If a failure occurs, list all the possibilities. Eliminate possibilities one by one if they do not have a contribution to the failure. For each possibility, note why it was eliminated. Continue to eliminate possibilities, until arriving at the most probable cause. It could be any one of the above areas.

If the proper methodology is recognized and used in design, manufacturing, and application, as well as management, a catastrophe would not occur.

OPINION

After looking at the origin, cause, analysis, and external components, a hypothesis can be developed. This is based on the most probable results from each of the stages.

The hypothesis is tested against all the facts and probabilities. This is an evaluation in context of the gathered data and analysis. If there is any deviation from the theory that cannot be resolved, then a new hypothesis is necessary. This is an iterative process. It is often useful for the examiner to have a “sounding board” of another professional who play’s the devil’s advocate, shooting holes in theories as they arise.

A final hypothesis is obtained when all the available information correlates reasonably. The opinion is a judgment based on special knowledge. It is a belief or conclusion held with confidence based on evaluating all possibilities and developing the most probable scenarios.

Elizabeth Drew (1887-1965) was a poet and author who wrote *The Modern Novel*. [10]. Her observation is a succinct perspective on decision making.

“The world is not run by thought, nor by imagination, but by opinion.”
- Elizabeth Drew

Opinions must be based on ethics, character, and outstanding technical skills.

RESPONSIBILITY

One of the most common arguments proposed for a failure is negligence. Negligence can be allocated to the design, manufacturing, or application. Negligence requires four components: duty, breach of duty, proximate cause, and damages.

Duty is an act or a course of action that is required of one by position, social custom, law, or religion [11]. Duty is the responsibility to perform what is reasonably expected.

Breach of duty is failure to perform what is expected or required.

Proximate cause is an event sufficiently related to a legally recognizable injury to be held the cause of that injury. There are two elements needed to determine proximate cause: the activity must produce a foreseeable risk, and the injury must be caused directly by the negligence. [12]

Damages are the harm suffered from the act.

Four questions must be asked to determine if there was negligence.

1. Was there a duty to perform?
2. Was there a breach of the duty?
3. Was the proximate cause a result of the breach?
4. Were damages the result of the proximate cause?

If any of the questions is negative, then there is no negligence.

NON-TECHNICAL

The technical aspects of the investigation are complete. Now comes the challenge for leaders and managers, make a decision about recovery. This will involve as many evaluations as the technical components. Again these should be determined by making a list of possibilities. Possibilities are then eliminated until a most probable approach is found.

Several questions should be considered. What is the additional cost? Can negligence or responsibility be established? What is the probability of success? What can be recovered? Is it worth it?

This process will give a direction of whether to start recovery or to abandon the problem and count it as experience.

CONCLUSIONS

Occasionally things go awry. The objective is to find the least erroneous solution. To determine the status of a project, it is necessary to determine all the leadership issues involved. Use these standards as questions to determine where the deviation occurs. Then the process of risk management is started. The first part is the technical issues: stop loss, gather data, determine origin, find cause, conduct analysis, research outside influence, and develop an opinion. Then the non-technical process is determining whether to recover or move on.

REFERENCES

[1] Bennett, F. Lawrence, *The Management of Engineering*, John Wiley, New York, 1996. pp 224-225.

[2] Durham et al, *Leadership & Success in Economics, Law, & Technology*, DreamPoint Publishers, Tulsa, 2005.

[3] *Forensic Examiner*, Vol 14, No 4, Winter 2005 American College of Fornesic Examiners, Springfield, MO

[4] *Standard Practice for Evaluation of Technical Data*, ASTM E678-98, ASTM International, West Conshohocken, PA, 1998.

[5] *Standard Practice for Examining and Testing Items That Are or May Become Involved in Litigation*, ASTM E860-97, ASTM International, West Conshohocken, PA, 1997.

[6] *Standard Guide for Studying Fire Incidents in Oxygen Environments*, ASTM G145-96, ASTM International, West Conshohocken, PA, 1996.

[7] *National Electrical Code*, NFPA 70, National Fire Protection Association, Batterymarch Park, Quincy, MA, 2005.

[8] *National Electrical Safety Code,* IEEE C2, Institute of Electrical and Electronic engineers, New York, 2002.

[9] *Guide for Fire and Explosion Investigations*, NFPA 921, National Fire Protection Association, Batterymarch Park, Quincy, MA, 2001.

[10] American Heritage® *Dictionary of the English Language*, Fourth Edition, Houghton Mifflin Company, 2000.

[11] Drew, Elizabeth, *The Modern Novel*, Harcourt, Brace, New York, 1926.

[12] Wikipedia, The Free Encyclopedia, http://en.wikipedia.org, 2004.

VITAE

Marcus O. Durham is the Principal Engineer of THEWAY Corp, Tulsa, OK. He is also a Professor at the University of Tulsa.

He is a registered Professional Engineer, a state licensed electrical contractor, a FCC licensed radiotelephone engineer, an extra-class amateur radio operator, and a commercial, instrument pilot. Professional recognition includes Fellow of the Institute of Electrical and Electronic Engineers, Diplomate of American College of Forensic Examiners, Certified Homeland Security by ACFE, member of the Society of Petroleum Engineers, and task group member of American Petroleum Institute. He has been awarded the IEEE Richard Harold Kaufmann Medal “for development of theory and practice in the application of power systems in hostile environments.” He was recognized with 6 IEEE Awards for his Standards development work. He has been awarded numerous times for the over 130 technical papers he has authored. He is acclaimed in Who’s Who of American Teachers, National Registry of Who's Who, Who’s Who of the Petroleum and Chemical Industry of the IEEE, Who’s Who in Executives and Professionals, Who’s Who Registry of Business Leaders, Congressional Businessman of the Year, and Presidential Committee Medal of Honor. Honorary recognition includes Phi Kappa Phi, Tau Beta Pi, and Eta Kappa Nu.

Dr. Durham received the B.S. in electrical engineering from Louisiana Tech University, Ruston; the M.E. in engineering systems from The University of Tulsa, Tulsa, OK; and the Ph.D. in electrical engineering from Oklahoma State University, Stillwater.

Robert A Durham, PhD, PE is the Principal Engineer of D^2 Tech Solutions, an engineering and technology related firm concentrating on Mechanical and Electrical systems and conversions He is also Chief Engineer of THEWAY Corp, Tulsa, OK, an engineering, management and operations group that conducts training, develops computer systems, and provides design and failure analysis of facilities and electrical installations. He specializes in power systems, utility competition, controls, and technology integration.

Dr. Durham is registered as a Professional Engineer in five states. His work experience is broad, and encompasses all areas of the power industry. His technical emphasis has been on all aspects of power systems from electric generating stations, to EHV transmission systems, to large-scale distribution systems and power applications for industrial locations. He is a nationally recognized author; having received several awards from technical and professional organizations such as the IEEE, and has published magazine articles on multiple occasions. Dr. Durham’s extensive client list includes the development of a broad spectrum of forensic, electrical and facilities projects for many companies. He also is involved with the audit of market participants in competitive utility markets to ensure that these facilities are adhering to the rules of the market.

Dr. Durham received a B.S. in electrical engineering from the University of Tulsa, an M.E. in Technology Management from The University of Tulsa, and a PhD in Engineering Management from Kennedy Western University.