Safety and Techniques

Using the Tools of Science and Industry to Build a Comprehensive Caving Safety Program

By William Storage

Safety is commonly viewed as avoidance of hazards. In scientific safety analyses hazards are defined as conditions likely to cause injury—an interaction of humans with obstacles or undesirable forces. I'll use this definition, even though it may differ slightly from common usage, where hazards may be viewed as the physical obstacles themselves. Since darkness, water, and pits are the normal environment of caves—we choose to experience these—it is not productive to view them as hazards. Thus for our purposes, most of the hazards of caves involve the dangerous interaction of cavers and these environmental factors.

The box on the right contains a partial list of caving hazards, derived from accident reports. Note that it includes hazards resulting from using equipment, such as mechanical failures and certain inherently dangerous characteristics of the equipment. For example, an inherent characteristic of rappel racks is that they can be threaded backwards.

Risk can be viewed as the likelihood of an accident, multiplied by the severity of its consequences. Assigning a numerical value to severity is obviously subjective, but it helps to capture the "weight" of a risk. For example, a frayed rope and a frayed bungee cord used for ascender positioning might be equally likely. But the consequences of failure are much different and thus we would say the risk of frayed rope is much greater.

From a social sciences perspective, predictive models of human behavior—errors and accidents—can be made by using statistics. From history we can rather accurately tell how many fatal auto accidents will occur next year. We know something, but much less, about who will be involved. History tells us what kind of caving accidents to expect and gives us an idea about how many.

Similarly, the likelihood of equipment failure can be expressed as a probability. When we view a total population of equipment, statistics and engineering analysis can be used to predict failures within a certain limited framework.

Recognizing that safety involves both probabilistic and humanistic elements yields the conclusion that safety is measured in relative terms. There is no such thing as a safe activity or product—there is only more safe and less safe. We cannot prevent accidents in caves; we can only make them less severe and less common.

Current safety efforts have not made an appreciable change in caving accident rates. In fact, the rate of fatal accidents seems to be increasing, even considering the effect of increasing participation (a Safety and Techniques article on this topic is in preparation). To reduce the frequency and severity of caving accidents—to make caving safer—we will have to make some changes. Many opportunities exist. In this article I will discuss various aspects of caving safety and address industrial and scientific tools directly.

Equipment Strength and the Margin of Safety

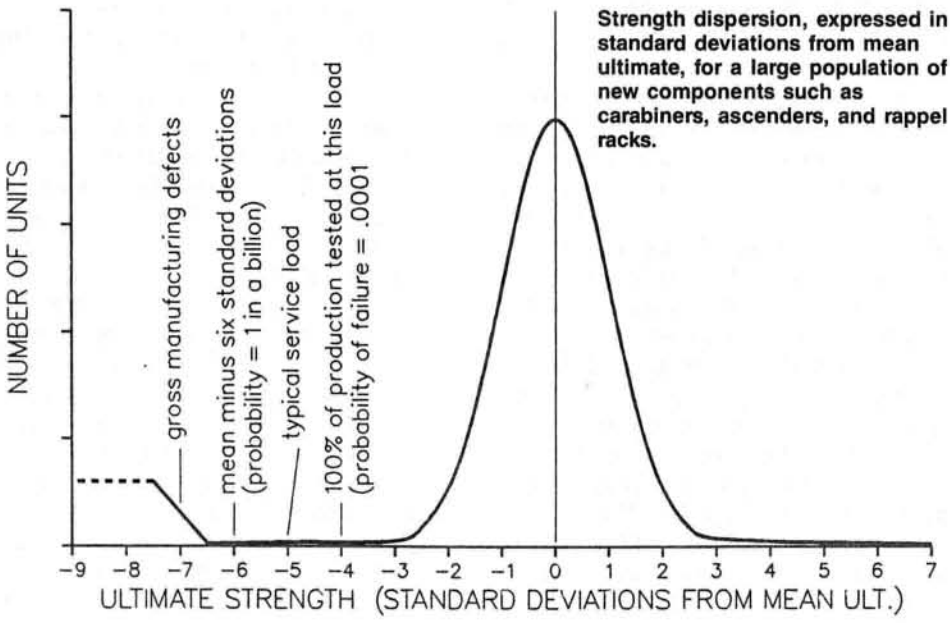
We may select our equipment and techniques on the basis of the relative degrees of safety that they offer, in addition to their level of performance or convenience. Equipment safety involves many aspects of design and manufacturing. Vertical equipment is often tested for strength, as an indication of safety. Cavers are fond of pull-testing cave gear to destruction and comparing strengths. Vertical gear is sometimes marketed with a comparison of the strength of brands X and Y. This is misleading. It gives strength too much importance. It has done caving and rock-climbing a tremendous disservice.

Many important properties of products are often totally ignored in an equipment evaluation which revolves around strength. The importance of spring rate and aging of rope has already been discussed in several previous STC columns. For other products, material properties like fracture toughness, the ability of a material to absorb energy after a small fracture is introduced, are important. The rotten condition of bolts throughout Appalachian caves shows that the importance of corrosion susceptibility is overlooked in equipment evaluation and selection.

Modulus of resilience must be considered when a designer selects a high-strength metal. Two materials might have identical ultimate strengths, but one with higher modulus of resilience would absorb more energy before failing. A number of other properties should also be considered. They are important in predicting the actual field performance of a piece of equipment; thus they are important for safety.

Historically, a concept commonly called margin-of-safety has been used to provide assurance that a piece of equipment would not break in service. Margin-of-safety is

STRENGTH DISPERSION OF NEW COMPONENTS



Hazards of Caving

Acetylene explosion—lamp, pack, register
Stove explosion
Scuba tank valve broken
Fall while climbing, traversing pits or canyon
Rockfall
Rockfall causing caver fall
Rockfall during earthquake
Collapse of dig
Bad vertical technique
Detachment from rope
Detachment from rebelay
Inability to change from rappel to ascent, and vice versa
Prusik knots jammed or won't grip
Ascenders slip on muddy or icy rope
Strangulation with vertical gear
Fall while climbing rope hand-over-hand
Fall from losing grip on handline
Rope anchor failure
Rope failure
Rope broken by falling rock
Ladder failure
Falling off ladder
Uncontrolled rappel
Harness carabiner opens during rappel
Rappel shunt defeated during uncontrolled rappel
Unwanted rappel shunt activation
Rappel off end of rope
Drop rope after access to passage below overhang
Rope recoils out of reach after rappel
Rappel into pit with no ascending gear
Foothang
Chemical contamination of rope
Animal eats rope
Rappel rack nut falls off
Hair or chinstrap caught in rappel rack
Sewn sling tears
Exhaustion
Lost
Through-trip—can't find second entrance
Out of light
Entrapment by flood
Drowning—passage flooded
Insufficient buoyancy
Asphyxiation—low oxygen, methane, blast fumes, engine exhaust
Hypothermia
Hypothermia while ascending through waterfall
Scaling pole failure
Fence wire wound
Struck by lightning while in cave stream
Locked inside gated entrance
Battery acid burn
Poisonous snakes
Rabid bat bite

defined as the ratio of ultimate strength to the design load—the expected highest load the item sees in service. Margin-of-safety is simply a calculated value and, for a number of reasons discussed below, is too simplistic to be useful for analysis of caving gear.

In the realm of engineering design, the margin-of-safety concept can be blamed for encouraging sloppiness in determining the loads encountered in actual service. Dynamic service loads, or design loads, usually can't be measured; they must be determined through analysis of equipment geometry, masses, and physics—the stuff engineers are paid to do. As we have mentioned in previous Safety and Techniques columns, the physics involved in determining dynamic loads of real caving is not always intuitively obvious. Early machinery designers were similarly plagued with the unpleasant physics of dynamically loaded equipment. They simply measured static loads—requiring no analysis—and applied a big "margin-of-safety" to account for the unanalyzed dynamics. Steam engines exploded, bridges collapsed, and ships sank. A big margin-of-safety applied to an incorrect design load is a killer.

Even when correct dynamic loads are used, a calculation of margin of safety that does not include factors for environmental effects can be horribly optimistic.

Equipment Reliability

Equipment reliability [note 1] is the probability that a piece of equipment will perform its function for a prescribed interval under stipulated environmental conditions. Stated differently, it is the likelihood that an item will not fail in a certain application. Underlying concepts are that properties vary between seemingly identical specimens in a predictable manner when considered statistically, and that the environment of use affects the likelihood of failure.

The reliability of devices like carabiners and rappel racks is of particular interest since a single failure might cause death. A failure rate of normally-loaded rappel racks of one in a thousand usages would be completely unacceptable. Indeed, one might ask what rate of catastrophic rack failures would be acceptable. In the nuclear and transportation industries, "acceptable" catastrophe probabilities in the range of one in ten million or one in a billion are used for design purposes.

Normal variations in material properties and production processes cause some amount of spread in the characteristics of individual pieces of equipment. When a large number of parts are pull-tested to destruction, their strength values will be *normally distributed* around the average (mean) ultimate strength. The spreading out (dispersion) of the ultimate strength values is described numerically by the *standard deviation* (a weighted average of the difference between individual values and a mean value).

The standard deviation of strength values for components like carabiners and ascenders is highly dependent on materials and production processes. The relative number of units with a strength value higher or lower than the mean falls rapidly away from the mean. For normally distributed data, the strength value corresponding to four standard deviations below mean still has an occurrence probability of about one in ten thousand—too high a probability to accept if it involves risking life. Since the tails of the normal distribution curve are so long, increasing the design strength (thus increasing mean strength and shifting the whole curve to the right) is not a very good way to reduce failure probabilities. Thus it is not a good way to improve safety.

Many responsible gear manufacturers chop the left tail off the curve by nondestructively testing 100% of components at a strength value above usage loads, but well below mean strength. By doing this they ensure that no individual ultimate strength will fall below the load the component sees in normal service.

Since a pull-test provides only a single data point, a pull test performed by cavers can at best give a rough idea of a mean strength value for a total population of similar items. The only strength you really know is that of the piece which is now destroyed and useless. Without abundant data, a potentially deadly assumption is being made about the dispersion of the strength data when a pull-test is the sole basis for evaluation. And the real lesson of strength distribution exercise is that no practical amount of destructive testing can justify not using 100% nondestructive testing when a single failure can be catastrophic.

Environmental Factors and Degradation in Service

Neither strength testing nor calculated "safety margins" can tell us how a product performs in service. We must remember the "under-stipulated environmental conditions" part of the definition of equipment reliability. Even tests of used equipment can't give us much reliable information, unless a very large sample is tested to account for the variations in degradation due to different environments. Corrosion, for example, can be a very haphazard process. Think about this as you ascend a rope left years ago by the team who first climbed the dome. What is the condition of the unseen anchor?

The margin-of-safety calculated for a new carabiner used underground is huge. It is related to safety, by virtue of the amount of loss of strength sustainable through degradation before failure. However, the rate of

that strength decay is so dependent on material properties unrelated to strength that initial strength becomes meaningless by comparison. Thus the calculated margin-of safety is not a measure of safety at all.

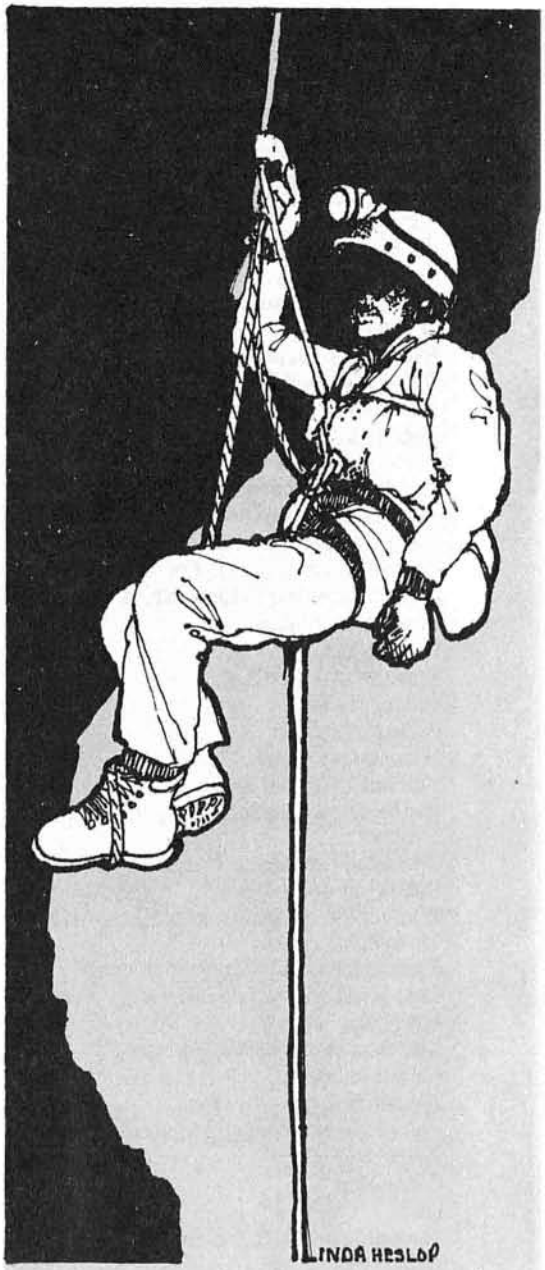
The number of caving and climbing accidents from failure of sewn webbing slings and harnesses is staggering. A dozen or so have been reported to *American Caving Accidents* in the last 15 years. Certainly, this is in part stems from undue confidence resulting from the strength myth. Users are aware that sewn webbing junctions are even stronger than the webbing, which itself may sustain 5000 pounds. The margin of safety is at least 20 to 1, right? Apparently not after mud, repeated drying, and abrasion have taken their toll.

In some cases **preoccupation with strength has driven cavers away from metals that would perform well in the cave environment.** The aluminum alloy used in carabiners, for instance, is the strongest reasonable aluminum at any cost. It's fine for sunny Yosemite, but cave mud can make it look like Swiss cheese in a matter of months. So why should we select this alloy for cave gear? We use it because there are few other choices—an acceptable reason, as long as we remember the limitations of equipment that was designed for a different environment.

An underlying principle of equipment design for harsh environments is that preserving a relatively low strength value is preferable to starting with a high value that degrades rapidly in service; preferable, that is, to consumers who base their purchases on the proper criteria. Responsible manufacturers can help by discussing and advertising their equipment's real virtues, rather than its strength.

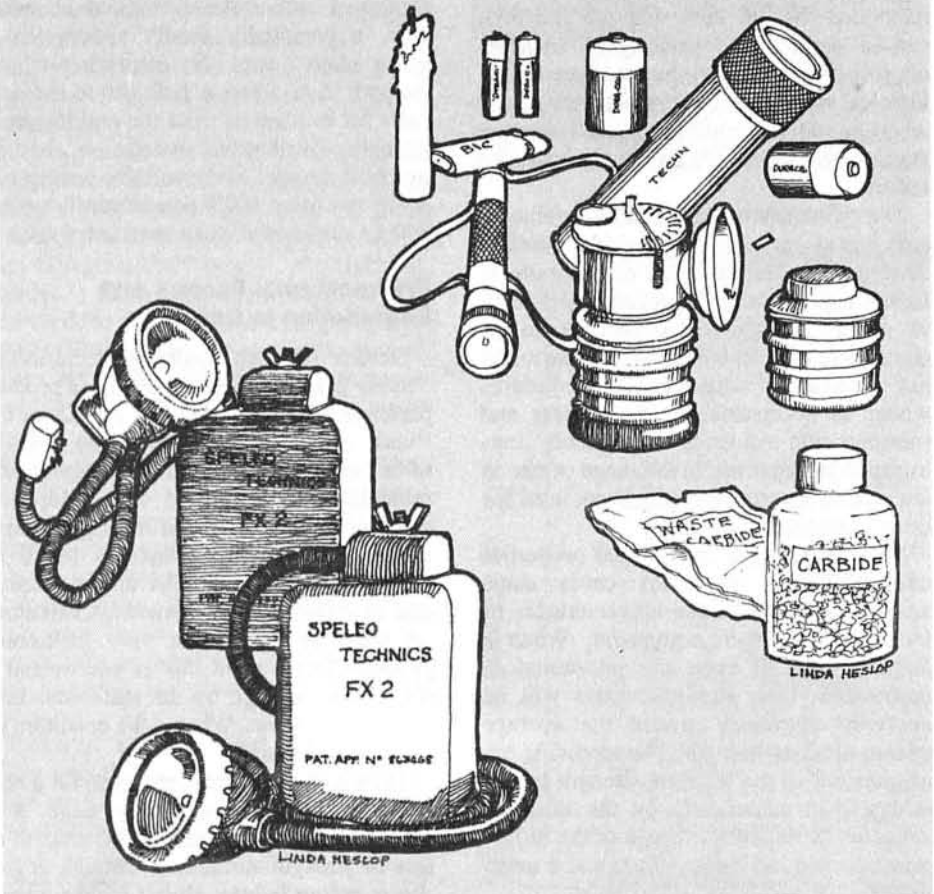
Failure Modes

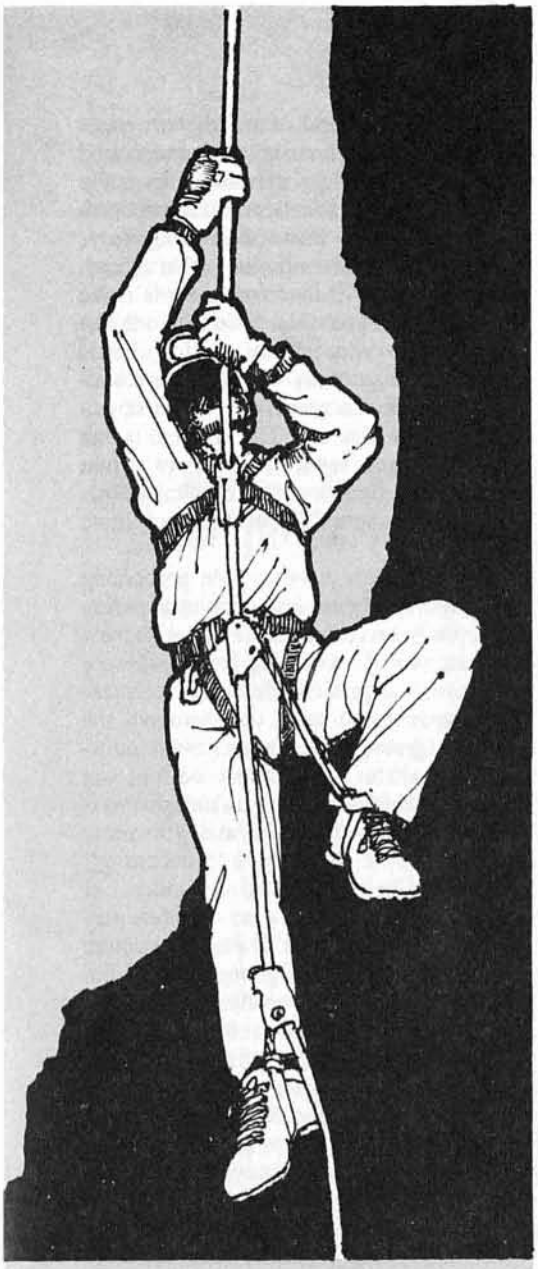
Viewing inherent characteristics of equipment as hazards requires consideration of technique, to determine the effect of failures of equipment during usage. Here an analysis of failure modes is useful (figure 2). A thorough failure mode analysis—in industry an FMECA; Failure Mode, Effects, and Criticality Analysis [note 2]—looks at all reasonable failure modes and their consequences. A failure mode analysis of a cavers rappel system, for example, identifies the rappel rack and the attachment carabiner as single-point critical failures. It thus points to areas where redundancy might greatly enhance safety. It can identify common-mode failures (two things that fail from one cause, such as chemical contamination of slings in a vertical system) and erroneous assumptions of independence. A failure mode analysis might show that a backup procedure ("Plan B") results in an



These cavers are touring a cold, wet cave. One is ascending with the three-ascender ropewalker system. The other is using a two-ascender frog system and carrying a spare ascender. What hazards does the ropewalker's third ascender really protect the caver from? Would failure of the ropewalker's chest

In a cold, wet, vertical cave, which combination is most reliable; (a) an FX-2 electric headlamp with a complete spare headpiece and battery, or (b) a carbide headlamp with spare bottom full of carbide, a full carbide container, a standard flashlight with spare batteries, a mini-mag light with spare batteries, a candle and a cigarette lighter? What has been our standard line about lighting for beginners?





ascender result in a significantly increased workload? In which system is loss of one ascender more critical? Are there any common-mode ascending system failures which simultaneously incapacitate both of the frog's ascenders?

Kayakers and sailboarders have found drysuits to be preferable to wetsuits in very cold water. They are warmer, lighter and more flexible than thick wetsuits. Without any knowledge of comparative probabilities of wetsuit and drysuit failure, what could a failure mode analysis tell us about the suitability of drysuits for deep penetration into a cold, wet cave?

unrealistic increase in required skill level—a consideration of particular interest for divers [note 3]. This type of analysis is invaluable for checking a newly developed system or procedure—inventors of the Highline Side-Kick Pulley Windlass and the technique for its use can avoid surprises by first evaluating failure and error modes of their gizmo on paper.

Redundancy and the Dilemma of Technology

The probability of a mechanical failure leading to catastrophe can be reduced by using a system or technique that employs redundancy. But if that redundancy leaves the caver carrying heavy, complicated gear or requires great effort and skill to use, the chance of error will be increased. A dilemma of technology is that one can always make a mechanical system more reliable at the expense of complexity, but when combined with the human element, safety may be compromised by the complexity.

An ongoing debate revolves around the rappel shunt. It tremendously increases the reliability of the mechanical portion of the rappeling system. But most types involve some type of increased workload. Several accidents have occurred where shunt-users mysteriously deactivated the device as they fell to the bottom of a pit. Critics speculate that these victims would never have lost rappel control in the first place if they had not been distracted by the shunt. Conceptually, the shunt may be a good idea, considering rappel accident statistics. But a shunt does add complexity to the rappel system. It requires *training*.

Another interesting case is dual-rope technique. Descending into pits with a separate belay rope greatly reduces the danger of rope breakage, detachment from rope, or loss of descent control. But it drastically increases the chance of getting hung up in a waterfall. And then a radical departure from normal procedure—with new risks—must occur to correct the situation.

Acceptance of single rope technique is soundly based on the idea that inherent rope defects (unprovoked failures) are extremely improbable, and that uncontrolled descent, detachment from rope, and "induced rope-failure" (e.g. abrasion and chemical contamination) can be prevented by *technique* and training.

Similarly, we can re-examine some of our truisms about ascender redundancy in light of the value of redundancy versus the cost of complexity. It is held by many cavers that two-ascender systems are "unsafe." Since safety is the avoidance of hazards, we can examine this belief in terms of the relevant hazards.

Lets consider a few points that would be revealed in a system failure-mode analysis. Say we accept the Federal Aviation Administration's "acceptable" probability for a life threatening condition—one in ten million. This means that it would be acceptable for one in ten million ropes (or other single-point critical points such as rappel racks) to fail from inherent flaws. I suspect that this level of reliability actually exists for today's equipment. Then for a two-ascender rig the acceptable probability of failure of one ascender or its attachment would be one in 3162, since both would have to fail to be life threatening (3162 times 3162 equals ten million). In other words, to be as safe against inherent flaws as a rope, the ascenders in a frog or Texas system would have to be about one three-

Failure/Error Mode [Cause] {Phase of Use}	Effect of Failure	Corrective Action	Comments
Structural failure [flaw or damage], removal from rope [error] {during ascent}	loss of redundancy, 1 failure from catastrophe, until replacement	switch to rappel and descend to reconfigure system, or attach spare ascender	some structural failures reported on older designs, highly unlikely on current design; erroneous removal is very likely
{during tyrolean traverse}	tendency to slide down inclined traverse line on primary attachment point	return to start of traverse if necessary; can probably proceed without ascender	low hazard criticality if rope angle is low—note importance of using full ascending system on steep rope traverses
{while crossing rebelay during descent}	loss of redundancy	none required	ascender is backup to assure rappel system integrity during cowstail removal
ascender jammed; won't move up or down [webbing or clothing caught in cam] {all phases}	climber can't slide ascender; note upper ascender cord caught lower ascender is common-mode failure effectively jamming both	weighting a third ascender attached above will allow jam to be cleared; possibility of using footwrap to unweight jam	attempt to clear jam by cutting may be fatal; occurrence can be reduced by avoiding loose clothing and the use of webbing and thin cord in vertical system
ascender slips [mud, ice, worn teeth] {any phase of operation}	inefficient climbing, tendency to slide down rope if both ascenders affected	clean ascender, pushing on cam reduces possibility of slipping	muddy rope is a common-mode cause of all ascenders slipping

An example of a failure mode analysis—in this case a Jumar ascender used in a standard frog rig, and for other ropework obstacles such as rebelays and traverses. A system analysis would consist of similar sheets for each component used.

thousandths as reliable as the rope. They are probably more reliable than that, or a number of such failures would have been reported. From the aspects of ascender failure, a third ascender on rope seems unnecessary.

So now you might be saying, "Yeah, but it's not failure that is important here; it is *error.*" We need to look at the ways a caver is likely to erroneously end up with only one ascender on rope. Users of frog and Texas systems claim that maintaining two points of connection to the rope is easier and less complex than with ropewalker systems, even with the ropewalker's third ascender. This claim seems ridiculous until we consider *all* the phases of ascender operation, including getting past the lip and over obstacles such as intermediate anchors or rebelays. A failure modes analysis must also consider that the third ascender (e.g. ascender riding above chest roller) can often fail latently; the climber doesn't know it's not functional until it is needed.

The point here is not to settle the ascender debate. But a method exists to explore such questions in a productive manner; and the "answer" might vary, depending on what types of conditions are anticipated.

Human Error

Undoubtedly the greatest potential for improving safety lies in the realm of error prevention. Unfortunately, human failures are much more common than mechanical ones. There is often a limit to the extent that we can eliminate or provide for hazards in equipment design, when incorrect usage is considered. Mechanical designers know well that equipment can be designed to be fool-proof, but it cannot be designed to be damn-fool-proof [note 4]. At this point technique must be designed to reduce the exposure to hazardous conditions caused by human error.

The entire spectrum of errors is relevant to caving accidents. Bad planning allows a group conducting a "through-trip" to take no ascending gear and then find the route blocked. Poor recognition of hazards allows novices to descend into blackness, hand over hand. Memory errors result in being lost. Perceptual errors contribute toward rappeling off the end of a too-short rope. Communication errors, both misunderstood messages and unclear meaning, can really complicate a bad situation. Like teenagers who court drug abuse and pregnancy, cavers make the reasoning error that successive "successes" with flood hazards make "failures" less probable. This is like thinking that five coin tosses yielding heads makes tails less likely on the sixth toss—clearly a logical error when viewed objectively, from a distance. The problem is that **errors do not seem like errors when perpetrated, and that the resultant accidents seem impossible beforehand** [note 4].

Humans simply have trouble processing information. So one key goal in avoiding accidents is to reduce the amount of new information and processing in the presence of hazards. To proceed through the potential hazards encountered underground, the caver integrates what he sees with information held in his memory. Since our processing ability is limited, decision making in one area reduces our ability to sense what's going on in another. "Interesting" situations—like a jammed ascender, or unexpectedly rappeling onto a knot—may increase brain workload to the point where crucial information is ignored. Psychologists call this "load-shedding." It helps account for the fact that safety awareness alone—consciousness of the presence of hazards while engaging in activities like caving—does little to reduce the likelihood of tragic error. This is not to belittle hazard awareness; it is necessary, but not sufficient to reach our goal [note 5].

Technique, Procedures, and Training

Technique should be designed to reduce workload—to minimize cognition and decision-making while it is being used. This can be done by establishing procedures in practice situations—places with minimal hazards—and adhering to those procedures underground. Procedures are critical for routine though potentially deadly activities—things like getting on and off rope, and switching from rappel to ascent. Good training consists of repetition of established procedures in a simulated environment. Unexpectedly encountering a knot during rappel should merely require recalling the procedure for crossing it or changing to ascent. Then the cognitive workload is kept low and the chance of error is reduced.

Poor procedure can be viewed as bad habits. It may be difficult to recognize by the person using poor technique because it usually has no ill effects. Bad habits may be repeated until they coincide with a subtly new set of circumstances yielding an oppor-

tunity for disaster. The slight difference between a new situation and those that did not produce interesting consequences produces bewilderment and false conclusions about Acts of God and freak accidents. If the incident merely results in a "near miss," the caver learns from "experience" and the bad habit is corrected. The cost of learning through this "experience" is far too high. We cannot tolerate a weeding-out process when lives are at stake. Bad habits can be prevented by training and a willingness to learn.

Standardized caving equipment, technique, procedures, and training, as are used in France and Quebec, would probably go a long way toward the goal of improved safety. While this concept offends our sense of individuality, such conformity undeniably reduces both the likelihood of error and the possibility of new and unforseen technical hazards. A reasonable compromise for us individualistic Americans might be for everyone to learn a set of standard procedures before adapting, tailoring, and customizing their equipment and techniques.

Reporting Accidents and Incidents

We can benefit greatly by reviewing caving accident data. By recording details of accidents and near misses, we can correlate hazardous environments, elements of technique that expose hazards, and errors in

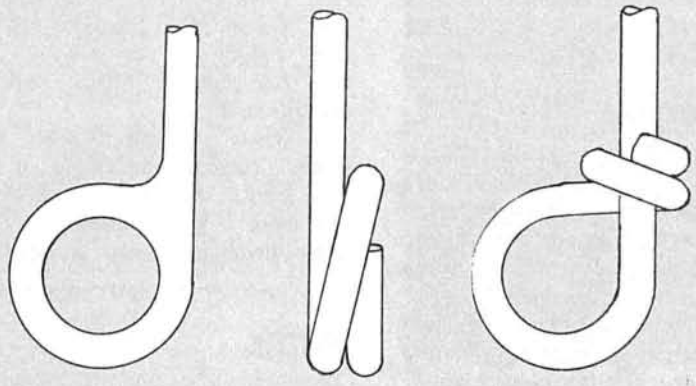
Strength vs. Reliability vs. Safety

Common misconceptions about cave gear—and probably every other kind of equipment—are that more strength means more reliability and more reliability means more safety. These misconceptions are intimately tied to the urge to pull-test equipment to destruction (this and the fact that it's fun to watch things break).

You can see the effect of the strength/reliability misconception on the evolution of the rappel rack. Rappel racks are available with at least three types of harness-attachment geometries, as shown in the diagram. The welded eye is stronger than the coiled and twisted varieties. But welding, particularly with stainless steel, is a much riskier process than bending. The producer has to be concerned with pre-heat, post-heat, contamination, and susceptibility to intergranular corrosion from chromium carbides formed in the weld zone. The corrosion and any increased chance of manufacturing defects detract from the reliability of the rack—even though the nominal design-strength has been increased by the presence of a welded junction. *More strength does not mean more reliability.*

The reliability/safety misconception involves the idea that by eliminating failures, an item will be made safe. This neglects the inherently hazardous characteristics of the equipment, itself. A rappel rack failure could result in separating the caver from his rope, but a more likely event with the same effect is threading the rack incorrectly. Regardless of which rack configuration is most reliable, its reliability has little to do with this aspect of rack safety.

To illustrate this, consider the probability of detachment from rope during a normal rappel, not including getting on and off rope, rebelays, or other obstacles. This probability is roughly expressed by the equation:



$$P = P(fail) \times F(cor) + P(detach) \times F(error).$$

where P(fail) is the probability of rack failure (assume failure at top of pit),

and F(cor) is the fraction of the time the rack is threaded correctly

and P(detach) is the probability of falling when the rack is threaded wrong

and F(error) is the fraction of the time the rack is threaded wrong.

Taking a guess at these probabilities:

P(fail) is assumed to be 1E-7 or 1 in ten million

F(cor) = .9999 (1 in 10,000 times, you thread incorrectly)

P(detach) = .9 (1 in 10 chance of successful rappel, even with error)

F(error) = .0001 = 1 - F(cor)

P = 1E-7 x .9999 + .9 x .0001
= 9.010E-5 = 1 in 11098.

Now lets say we improve the reliability of rappel racks so that only one in 100 million (1E-8) fail from defects. The total probability of a nasty accident from detachment from rope becomes:

P = 1E-8 x .9999 + .9 x .0001
= 9.001E-5 = 1 in 11110.

So improving the rack's reliability by a factor of 10 changes the chance of catastrophe from 1 in 11098 to 1 in 11110—a meaningless improvement of 0.1%.

Now lets look at a corresponding improvement in technique, while using the original, less reliable rack. If we, through training and adherence to established procedures, decrease the rate of incorrect threading from 1 in 10,000 to 1 in 100,000, the probability of catastrophe becomes:

P = 1E-7 x .99999 + .9 x .00001
= 9.01E-6 = 1 in 109,890.

Improving the error rate makes a dramatic improvement. Note that "P" is actually the sum of two individual probabilities; the equation's two terms are independent because error and mechanical failure are independent and uncorrelated. The equation is obviously dominated by the second term, representing human error resulting in accident. In this example, eliminating failures, does little to reduce the chance of accident. *More reliability does not mean more safety.*

Rather than making a big deal about rappel rack eye strengths, shouldn't our emphasis be on how to design a rack that reduces the possibility of error? What steps have been taken so far? Can anything else be done?

the application of technique. This information shows us a direct link between failures, errors and accidents. It tells us what errors are likely—what aspects of technique need attention in order to prevent accidents.

American Caving Accidents is an NSS publication which attempts to compile data on all North American caving accidents and safety-related incidents. For us to achieve the potential benefits of accident analysis, cavers must submit the data. It is important that data on near misses be submitted, in addition to more "interesting" accidents. After at least one fatal accident, we have learned that several similar nonfatal incidents were known in the caving community but were not reported. Many close calls point to areas where characteristics of equipment expose the user to danger in the event of an error in technique.

Accident Prevention

In science and industry, safety analysis tools have shown that even when no history exists accidents can be prevented by anticipating errors and failures, and by designing equipment and techniques accordingly. When heading off into uncharted territory, prior consideration of what might be encountered can prevent dangerous surprises. Failure mode analysis provides that consideration.

New forms of hazards in caves will occasionally be found. But the better we have done our homework—evaluating the effects of failures and practicing basic procedures—the better we will be able to recognize the potential for catastrophe before it happens. Rarely do catastrophes occur because we have consciously gambled and lost [note 6]. The often inappropriate use of the term "freak accident" strongly shows that a hazard simply wasn't recognized.

The tools of safety discussed above can prevent most accidents. Equipment manufacturers can employ (and generally do) sound engineering and quality control methods. Equipment designers (who are often cavers) can design with thoughts of failure modes and their effects, and the effects of likely incorrect use. Obviously, the greatest responsibility is in the hands of cavers themselves.

But I'm No Scientist, What Do You Expect Me to Do?

As cavers, we are all designers in the sense that our lighting and vertical equipment is often home-made or tailored, and is always assembled as a system from more basic components. Most of the tools of safety analysis do not require you to be a scientist. Nor do they require "common sense" [note 7]. They do require planning and a bit of discipline. So does going caving.

Here are some specific recommendations derived from the above discussion:

1. Identify specific hazards of the type of caving you do. Arguments about the "best" system are really foolish without consideration of the great variety of types of caves and caving activities. Deciding on the best technique for you requires knowing what you're up against.

2. Buy reasonable equipment (components) for your system and techniques. Avoid doing business with manufacturers who only talk about breaking strength. Be very cautious of home-made or experimental components in safety-critical applications.

3. Think about corrosion. Maintain your gear. Do not place corrosion prone permanent rigging in caves. All aluminum and non-stainless steels will corrode underground.

4. When you put together a vertical system, consider the effects of failure of each item in the system—in each phase of operation. If you're using a new arrangement—inventing a new technique—do an exhaustive failure mode analysis before using it or recommending it in *Nylon Highway.*

5. Rope is a great opportunity for single-point critical failures. Single-rope technique is justified only if induced failures (sawing over sharp edges, chemical contamination, etc.) are precluded. Good rigging and rope maintenance are fundamental.

6. Most importantly, avoid *errors* through hazard identification and training. Use established procedures for ropework. Memorize and practice to reduce the degree of surprise when a new obstacle arises.

7. Report accidents *and near misses* to *American Caving Accidents.* Outside of pain and suffering, close calls are as interesting and statistically useful as disasters.

Acknowledgements

I would like to thank John Ganter, Steve Worthington, and Bill Klimack for contributing ideas and examples used in this article. Linda Heslop and Bart Rowlett also contributed technical review and editing. Linda Heslop provided the illustrations.

NOTES

Note 1: This discussion of reliability and several examples used in this article were taken from an earlier article; "Strength, Reliability and Safety," by Bill Storage, in the Spring, 1988 *Nylon Highway.* A distinction is generally made between reliability and the probability of not failing. Reliability is usually defined as the inverse of failure rate, e.g. 20 failures per 1000 hours of use. Probability of success (not failing) is thus related to failure rate by the time duration under consideration. For low failure rates it is reasonable to approximate that the probability of failure equals the failure rate times the duration of exposure to failure.

Note 2: MIL-STD-1629A, Procedures for Performing a *Failure Mode Effects and Criticality Analysis* and MIL-STD-882B, *System Safety Program Requirements,* are commonly used in industry. Military Standards are available from technical libraries and document supply houses. One supplier I have dealt with is Engineering Documents, 2805 McGaw Ave., Irvine, CA 92713 (800-854-7179).

Note 3: For very complex systems, such as those used in cave diving, another technique, Fault Tree Analysis, can be used to show that fatal combinations of independent, seemingly minor failures are sufficiently improbable.

Note 4: "Damn-fool-proof" is taken from the chapter, "Mechanical Engineering Design in Broad Perspective," in *Fundamentals of Machine Component Design* by Robert C. Juvinall, 1983, John Wiley & Sons, New York, pp. 3-13.

Note 5: If mere awareness of hazards were sufficient to prevent errors, most commercial aircraft disasters would not have occurred. Surely, safety is very serious business to pilots, yet gross errors have occurred, such as flaps not deployed for takeoff.

Note 6: This point was developed by W.A. Wagenaar and J. Groeneweg in "Accidents at Sea: Multiple Causes and Impossible Consequences," *International Journal of Man-Machine Studies,* 1987, Vol.27, pp. 587-598. They also present strong arguments that mere hazard-awareness is ineffective and that habits and procedures must control human behavior in high-risk activities

Note 7: The problem with "common sense" is that it is not common, by either definition of "common;" it is neither ordinary nor equally available to everyone. The concept is not highly regarded by safety analysts. Instructing participants in high-risk activities to use common sense is even less useful than hazard awareness without specific procedures. It really doesn't seem quite fair to relegate those with less sense to die as a consequence.