ISSN 1041-9489

SAFETY BRIEF

August, 2020 Volume 31 , No. 4

Triodyne Inc.

Consulting Scientists - Safety Philosophy & Technology

450 Skokie Blvd., #604
Northbrook, IL 60062
(847)-677-4730
FAX: (847) 647-2047

Officers:
Ralph L. Barnett
Dolores Gildin

e-mail: infoserv@triodyne.com
website: triodyne.com

On the Safety Theorem

by

Ralph L. Barnett

Professor, Mechanical and Aerospace Engineering, Illinois Institute of Technology, Chicago, IL
Chairman, Triodyne Inc., 450 Skokie Blvd., Ste. 604, Northbrook, IL

Abstract

The contrivances of humankind come into existence through divine intervention, stealth, creative impulse, transformation, systematic design, evolutionary forces, and accidental benevolence. According to the safety theorem the elements of this cosmic stew have a common property, they can all cause harm. The safety theorem appears in many of the most important safety concepts, e.g., the colloquial definition of safety, the technical definition of safety, the control hierarchy, risk abatement, "safety through design" protocol, alternative design theory, and the classification of safety devices.
According to the safety theorem,

- The colloquial definition of safety, freedom from the occurrence of injury or loss, exists only as a concept not a reality.
- A safe state does not exist, it may be approached asymptotically in the sense that a cup cannot be emptied by drinking half, followed by drinking half the remainder, etc. You may get as close to empty as you want; but, an infinite number of trials will not empty the cup.
- Laypeople by and large mistakenly believe that products can be made perfectly safe if enough money and time were focused on their design.

This paper offers a proof of the safety theorem together with some of its applications.

Introduction

The principal objective of this paper is to demonstrate that the following hypothesis is a theorem, i.e, a provable statement of truth:

Safety Theorem:
"*Every physical entity created by man or nature is a hazard capable of causing harm."*

This theorem is proved by inductive inference.

A. Inference

Inference is the act of deriving knowledge by reasoning which involves either deduction or induction. Inferences based on deduction are always correct. On the other hand, inferences based on induction, however logical, may not be true. This is the problem of induction. To focus properly on inductive reasoning, we begin with a brief account of deduction for contrast and completeness.

B. Deduction

"All dogs are mortal. Sherman is a dog; therefore, Sherman is mortal."

This example of deduction illustrates the general characteristic of reasoning from a general truth to a particular instance of the truth. In the more general sense, deduction is any process of reasoning by which one draws conclusions from principles or information already known. A valid deductive argument is one

This paper has been published in the *American Journal of Mechanical Engineering*, 2020, Vol. 8, No. 2, 50 - 53.

where the truth of its premises guarantees the truth of its conclusion; in some sense the conclusion is already contained in the premises.

C. Induction

While engineers and other applied scientists have a particular appreciation for the elegance of deducing specific truths from general truths and would like to think that this type of thinking is human nature, the fact is that most human information processing time is spent doing the opposite: deriving general truths from specific instances based on our experience, intuition and sometimes faith.

The method by which a general law is inferred from observed particular instances is called induction or inductive reasoning. It is a form of non-deductive inference in which the conclusion expresses something that goes beyond what is said in the premise; the conclusion does not follow with logical necessity from the premise. As an example, we can infer the general law that "All crows are black" based on observing a very large number of black crows and not seeing any other color. On the other hand, since all crows have not been observed, can we logically claim to have proved our inference?
Arguments based on induction do not appear to have the rigor or persuasiveness of deductions which are regarded as rationally grounded. Ultimately, however, the premises in deductive arguments rest on induction from observed cases. The only way around this dose of realism is to establish, if you can, general statements whose truth can be known a priori.

D. Isaac Newton (1642 – 1727)

Newton introduced a "four-rule" philosophical method for studying physical phenomena. His fourth rule was to consider every proposition obtained by induction from observed phenomenon to be valid until a new phenomenon occurs and contradicts the proposition or limits its validity. Newton explicitly dealt with the fact that induction does not necessarily produce truth; nevertheless, his method used induction to produce one of the greatest bodies of scientific knowledge ever amassed by an individual.

E. Technical Definition of Safety

Hazard has been defined in MIL-STD-882D as:

Hazard:
"Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. [Ref. 1]"
The magnitude of hazard is called severity.

Clearly, any exposure to a hazard will result in harm. This observation has led to another concept called Risk. [Ref. 2] Risk is a combination of hazard severity and hazard exposure. A mathematical transliteration of this notion is.

Risk = f (hazard severity, hazard exposure) (1)

where f is a function of the independent variables hazard severity and hazard exposure. The dependent variable Risk is the antonym of Safety (tech definition), thus,

Risk = 1/Safety (technical safety) (2)

Risk is a measure of the effect of accidents associated with a product or system. A derivative of the Safety Theorem can be inferred from the definition of Risk,

"Eliminating a hazard eliminates the Risk associated with the hazard."

This statement highlights a logical disconnect in the current safety dialog. Consider the assertion in ANSI B11.TR3-2000 (Risk Assessment),

"zero risk does not exist and cannot be attained."

This same document recommends "Eliminate the hazard" as its first mitigation strategy. For example, to ameliorate an asbestos problem remove the asbestos. Note that the hazard is gone, the hazard exposure is gone, and the Risk is gone.

Proving the Safety Theorem

A number of important references are presented which support the Safety Theorem.

A. ***Of Acceptable Risk - Science and the Determination of Safety***, William W. Lowrance, 1976.

Page 8: "We will define safety as a judgment of the acceptability of Risk, and Risk, in turn, has a measure of the probability and severity of harm to human health.

A thing is safe if its Risks are judged to be acceptable.

By its preciseness and connotative power this definition contrasts sharply with simplistic dictionary

definitions that have "safe" meaning something like "free from risk." Nothing can be absolutely free of Risk. One can't think of anything that isn't, under some circumstances, able to cause harm. Because nothing can be absolutely free of Risk, nothing can be said to be absolutely safe. There are degrees of Risk, and consequently there are degrees of safety."

B. ***Accident Prevention Manual for Business and Industry***, Engineering and Technology, 13th Edition, National Safety Council, 2009.

Page 7: "Acceptable Risk does not mean zero Risk, which is unattainable."

Page 8: "Residual Risk: The Risk remaining after preventative measures have been taken. No matter how effective the preventative actions, there will always be residual risk if a facility or operation continues to exist." "All Risks to which the concept of safety through design applies derive from hazards. There are not exceptions."

C. ***On the Practice of Safety, 3rd Edition***, Fred A. Manuele, 2003:

Page 244: "No thing or activity is Risk-free. Also, in the practical world, all Risks will not be eliminated."

Page 275: "Definitions and Comments. The following is typical of what is becoming universally accepted language with respect to hazards and Risks:

A hazard is defined as the potential source of harm. Hazards include both the characteristics of things and the actions or inactions of people. Identifying hazardous human error potential, as well as the physical aspects of hazards, is an important part of the hazard identification process. All Risks with which safety practitioners deal derive from hazards. There are no exceptions. For a particular hazard the first and best approach is to eliminate the hazard. If there are no potentials for harm, there are no hazards. If there are no hazards, there are no Risks. Hazards eliminated result in zero Risk from those hazards. But it is not possible to eliminate all hazards."

Page 285: "Logic and Support of the Safety Decision Hierarchy

1. If the hazards are eliminated in the design and the redesign processes, Risks that derive from those hazards are also eliminated. If there are no hazards, there is no potential for harm and thereby no Risk. Obviously, hazard elimination is the most effective way to eliminate Risk.

Page 285
Conclusions - 1. We must accept that a state of zero Risk cannot exist where hazards have not been eliminated."

D. ***ISO/IEC Guide 51: The Concept of Safety (Section 5), Safety Aspects - Guidelines for the Inclusion in Standards***: "There can be no absolute safety: Some Risk will remain, defined in this guide as residual Risk. Therefore a product, process or safety can only relatively be safe."

E. ***Safety Engineering***, Gilbert Marshall, 1982

Page 5: "Nothing is really free of hazards, and a hazard may be present without being recognized. An object may be considered foolproof, meaning that there is no way misuse it, but, again, nothing is really foolproof."

Comment: Henry David Thoreau - "It is impossible to make anything foolproof because fools are so ingenious."

F. ***Accident Prevention Manual for Training Programs***, Merle E. Strong, 1975.

Page 138: "Some degree of hazard is associated with every form of activity; therefore the highest degree of injury elimination can be achieved only by careful, painstaking attention to safety in every form of activity carried on in an establishment or undertaking in question."

Page 139: "No work activities can ever be made entirely hazard free."

G. ***Safety and Health for Engineers***, Second Edition, Roger L. Brauer, 2006.

Page 31: How Safe is Safe Enough? "What is accepted as safe is neither constant or absolute. Each person in society establishes what level of safety and health is acceptable. Not everyone agrees whether things are safe enough. People would like to be free from Risks. However, every activity has some Risk. The level Risk that society finds acceptable is a moral issue, not just a technical, economic, political, or legal one."

Page 75: Reducing Liability Risks. There are Risks in any product.

Page 648: Eliminating or Reducing Risks. "If Risks are known, one can attempt to eliminate them.

However, it is not possible to eliminate all Risks; some can only be reduced."

H. ***Occupational Safety Management and Engineering, Fifth Edition***, Willy Hammer and Dennis Price, 2001.

Page 102: "It is impossible to have an accident without the presence of a hazard."

I. ***Reading in Industrial Accident Prevention***, Dan Petersen Jerry Goodale, 1980.

Page 179: "Given a certain Risk, is it an acceptable Risk? After all, there is some Risk involved in every human endeavor."

J. ***Safety Management, Fourth Edition***, Grimaldi and Simonds, 1984.

Page 139: "The best safety program in the world, however, will not eliminate all accidents.

Page 299" Layout in Design. "If it isn't there it can't go wrong," R.J. Redding, Intrinsic Safety, 1971.

K. ***Introduction to Safety Engineering***, David S. Gloss and Marian Gayle Wardle, 1984.

Page 3: There is no such thing as "absolute safety", nor can it ever be achieved.

L. ***Safety Through Design***, Wayne C. Christensen & Fred Manuele, 1999.

Page 5: "Designing to minimum Risk - acceptable Risk - is a goal of this safety through design concept. That does not mean designing to zero Risk, which is impossible."

Page 73: "However, as a benchmark, it must be accepted that there is no such thing in the real world as absolute safety, where even Risks from random events are ruled out."

M. ANSI B11.TR3-2000: Risk Assessment and Risk Reduction – A guide to estimate, Evaluate and Reduce Risks Associated with Machine Tools

Page ii: "This technical report explicitly recognizes that zero risk is virtually unattainable."

Page vi: "This technical report recognizes that zero risk does not exist and cannot be attained."

Emergence of the Safety Theorem

A. Medical Devices

The popular medical ethics dictum, "First Do No Harm," is decimated by the Safety Theorem, "Every physical entity created by man or nature is a hazard capable of causing harm."

The Food and Drug Administration (FDA) began with the Food and Drug Act of 1906 at a time when medical devices were not prominent in the practice of medicine. Over the next seventy years, this changed significantly which resulted in the Medical Device Amendments of 1976. Along with the original FDA charter which was to assure the safety and efficacy of drugs, this same requirement was imposed on medical devices.

The FDA assigned all medical devices to one of three classes that reflected their basic premise that all medical devices must be safe and effective to qualify for use on humans. All risks must be absent or well understood and weighed with respect to outcome benefits.

The three medical device classes by increasing risk are:

Class I – (insignificant risk) requires:
- general controls

Class II – (moderate risk) requires:
- general controls
- special controls

Class III – (significant risk) requires:
- general controls
- special controls
- pre market approval

Observe that all three classes have risks. Further, the risks are compared to the outcome benefits as found in the Risk-Utility Theory in product liability. [Ref. 3]

B. Public Safety

The Safety Theorem implies that humans are always confronted with a infinite number of hazards and associated risks. Implementation of risk reduction measures will reduce many of these risks to a "tolerable risk" level. The unbounded remainder of risks are called "residual risk" which we must mitigate using personal vigilance. The development of personal vigilance skills in children is compromised by the imposition of too many prophylactic measures.

C. Reasonably Foreseeable Use

Risks that are not reasonably foreseeable are "tolerable risks" that require no mediation. The Safety Theorem implies that the number of hazards associated with these risks are unbounded.

D. Hazard Identification

Structural design in brittle state materials recognizes that a crack may form at any point of the construct. This results in an infinite number of hazards which is consistent with the Safety Theorem. Risk analysis standards such as MIL-STD-882D call for the identification of only a finite number of hazards. Don't be surprised if an entire ship breaks in two under benign conditions [Ref. 4].

E. Protective Measure Hierarchy

Protective measures are defined in ANSI B11.TR3-2000,

3.13 protective measures: Design, safeguarding, administrative controls, warnings, training or personal protective equipment used to eliminate hazards or reduce risks.

Page 6 of this document contains Figure 2: Relationship between supplier and user showing the hierarchy of applying protective measures: The third footnote in this figure states,

"The supplier/user should take into account that adding a safeguard may add additional hazard(s) or increase risk(s) from other hazards."

The Safety Theorem tells us that adding an additional safeguard will introduce new hazards even if the net Risk improves.

Comments

There is no physical entity that is incapable of causing harm. The colloquial notion of safety as the absence of harm is a myth together with the idea of a finite number of hazards. In a theoretical subsystem, absolute safety requires the removal of all hazards. Every mitigation strategy begins with the hope of designing them out.

References

[1] MIL-STD-882D, "Standard Practice for System Safety," Department of Defense, 10, February, 2000.

[2] Lowrance, William W., "Of Acceptable Risk – Science and the Determination of Safety,"1976.

[3] Barnett, Ralph L., "On the Multiple Definitions of Safety," American Journal of Mechanical Engineers, June 2020.

[4] Parker, Earl, "Brittle Behavior of Engineering Structure," John Wiley & Sons, 1957.

Acknowledgment

This is the second paper describing Triodyne's research in the area of fundamental safety philosophy. It is a pleasure to acknowledge the encouragement and support of the Robert Clifford Law Firm.