ISSN 1041-9489

SAFETY BRIEF

March, 2022 Volume 32, No.2

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

# A Protocol Triumvirate - Risk Assessment and Risk Reduction

by

Ralph L. Barnett

Professor Emeritus, Mechanical and Aerospace Engineering, Illinois Institute of Technology, Chicago, Illinois
Chairman, Triodyne Inc., 450 Skokie Blvd. #604, Northbrook, IL 60062

**Abstract** Scientific laws are introduced to engineering students in the various disciplines, for example, Ohm's law in electrical engineering; Newton's law in mechanical engineering; Boyle's law in fluid mechanics; Entropy in thermodynamics; Avogadro's constant in chemical engineering; and the Mass - Energy Equivalence (E = mc2) in physics. Ask someone to cite some of the laws in safety engineering! Indeed, ask a safety practitioner to define safety. Will he explain that the technical definition of safety is the reciprocal of Risk which is defined almost everywhere as a combination of hazard severity and hazard exposure? This challenged definition of safety is really a description that has been replaced by the safety community with Risk Matrices developed through consensus not research. It has, nevertheless, been incorporated into guidelines for conducting Risk Assessment and Risk Reduction which is the subject of this paper. Generally, if we characterize a contrivance, the protocols for its risk assessment and risk reduction include five building blocks: Hazard Identification, Definition of Risk, Risk Acceptance Criteria, Hierarchies of Control, and Control Management. The value of these protocols for defining safety and improving safety, derives from the fact that the combination of building elements includes the concepts of Design and Safeguards which are supported by the classical engineering disciplines. In addition, users of the protocols are introduced to the full safety toolbox together with an enlightened presentation covering most of the significant historical safety observations. On the other hand, these building blocks have never been validated by research and the protocols have not been compared to risks computed from actual statistical data. The protocols are critiqued in this paper primarily through the lens of their authors. With time, the risk protocol that was originally presented as a guideline has undergone a metamorphosis into a faux-safety theorem by virtue of its introduction into a variety of consensus standards and safety reference books. It has achieved ubiquity and currently carries the mantle of a gold standard for determining Tolerable Risk. Notwithstanding its value, it remains an art form that does not contribute to the basic underpinnings of safety technology. Protocols present in three different forms. The most advanced are directed toward products that reflect critical mishaps such as aircraft design and weapon design; these protocols contain an extra building block, Validation and Documentation, together with Risk Acceptance Criteria that include independent authority outside the purview of the design team. An intermediate level protocol that is championed by ISO/IEC deals with non-critical mishaps that also include the extra building block, Validation and Documentation, without the requirement that Risk Acceptance Criteria embrace independent scrutiny. Finally, a very popular protocol of a type recommended by ANSI for non-critical mishaps, has no validation requirements and uses Risk Acceptance Criteria for the determination of tolerable risk that reside in the discretion of the designers.

***Keywords****: risk, hierarchies of control, risk matrix, mishaps, system safety*

## INTRODUCTION

The Food and Drug Administration (FDA) requires that every mishap with medical devices be investigated and recorded. Product liability lawsuits that result in trials leave a paper trail that is available to the public. Hospitals write up descriptions of traumatic injuries; historically, the records from approximately 100 hospitals are reviewed by government agencies in an attempt to represent the experiences of approximately 5100 hospitals with a trauma capability. Almost every manufacturer keeps a record of accidents caused by each of their products. In short, the United States is drowning in data that would allow the safety community to calculate the harm exhibited by almost every product. Harm caused by an accident is measured by Risk which is defined as a combination of hazard severity and hazard exposure. Measured Risk would be available for every brand and model product or any type of product if only the statistical data could be accessed. For a given product, Risk might be presented as a bell-shaped curve; Total Risk for a product could be described monetarily; the Risk per Man Hour of exposure could be expressed; or the Risk per Unit Time might be specified. The myriad ways of presenting harm

*This paper has been published in the* ***American Journal of Mechanical Engineering****, 2020, Vol. 8, No. 3, 127 - 143.*

or risk would include the current use of a Risk Matrix, i.e., High, Medium, Low, and Negligible.

It is unfortunate that the power expended to delineate the affairs of every US citizen has not been harnessed to characterize accident statistics. In response to this state of affairs, the safety community has chosen to circumvent the straightforward approach to Risk Analysis that embraces analyzing, recording, and counting accidents, for an alternative approach that involves the development of protocols for performing Risk Assessment and Risk Reduction. Typically, the protocols involve the following building blocks: Hazard Identification, Definition of Risk, Risk Acceptance Criteria, Hierarchies of Control, Control Management. In the following subsections, all of the Risk Analysis elements are discussed beginning with a lexicon defining the important nomenclature used in the various risk algorithms.

A. Lexicon

1. Acceptable Risk: Risk that the appropriate acceptance authority is willing to accept without additional mitigation. [3]
2. Consensus: General agreement. Not necessarily unanimous agreement.
3. Consensus Standards: When there is consensus among stakeholders in a given safety area, this may result in the formulation of a standard, code, regulation, principal, or rule-of-thumb.
4. Contractor: An entity in private industry that enters into contracts with the Government to provide goods or services. [3]
5. Design: To plan and develop a device to meet the intended purpose and function during its lifecycle. [6]
6. Environmental Impact: An adverse change to the environment wholly or partially caused by the system or its use. [3]
7. Event Risk: The risk associated with the hazard as it applies to a specified hardware/software configuration during an event. Typical events include Developmental Testing/Operational Testing, demonstrations, fielding, and post-fielding tests. [3]
8. Extended Use: Use of a product or system in a way intended by the supplier; but, not intended by the designer.
9. Fielding: Placing the system into operational use with units in the field or fleet. [3]
10. Government-Furnished Equipment (GFE): Property in the possession of or acquired directly by the Government, and subsequently delivered to or otherwise made available to the contractor for use. [3]
11. Government-Furnished Information (GFI): Information in the possession of or acquired directly by the Government, and subsequently delivered to or otherwise made available to the contractor for use. Government furnished information may include items such as lessons learned from similar systems or other data that may not normally be available to non-Government agencies. [3]
12. Government-Off-The-Shelf (GOTS): Hardware or software developed, produced, or owned by a government agency that requires no unique modification of the lifecycle of the product to meet the needs of the procuring agency. [3]
13. Harm: Injury or damage to the health of people, or damage to property, or the environment. [4]
14. Hazard: Potential source of harm. [6]
15. Hazardous Situation: Circumstance in which people, property, or the environment is/or exposed to one or more hazards. [4]
16. Initial Risk: The 1st assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard. [3]
17. Intended Use: Use in accordance with information provided with a product or system, or, in the absence of such information, by generally understood patterns of usage. [4]
18. Level of Rigor: A specification of the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required. [3]
19. Lifecycle (of a machine): [6]
    - Design and construction
    - Transport and commissioning
    - Use
    - Decommissioning
20. Manufacture: (see supplier)
21. Mishap: An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [3]
22. Mitigation Measure: Action required to eliminate the hazard or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood that a mishap will occur. [3]
23. Program Manager (PM): The designated Government individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment of the system/product/equipment to meet the user's operational needs. The program manager is accountable for credible cost, schedule, and performance reporting. [3]
24. Protective Measures: Design, safeguarding, administrative controls, warnings, training, or personal protective equipment used to eliminate hazards or reduce risks. [6]
25. Reasonably Foreseeable Misuse: Use of a product or system in a way not intended by the supplier. This includes extended use. [4]
26. Residual Risk: Risk remaining after risk reduction measures have been implemented. [4]
27. Risk: Combination of hazard severity and hazard exposure. [4]
28. Risk Analysis: Systematic use of available information to identify hazards and to estimate the risk. [4]
29. Risk Assessment: Overall process comprising of a risk analysis and a risk evaluation. [4]
30. Risk Evaluation: Procedure based on the risk analysis to determine whether tolerable risk has been exceeded. [4]
31. Risk Reduction Measure: Action or means to eliminate hazards or reduce risks. [4]
32. Safeguarding: Guards, safeguarding devices, awareness devices, safeguarding methods, and

safe work procedures. [6]

33. Safety (colloquial): Freedom from risk which is not tolerable. [4]
34. Safety Critical: A term applied to a condition, event, operation, process, or item whose mishaps severity consequence is either Catastrophic or Critical (e.g. safety-critical function, safety-critical path, and safety-critical component). [3]
35. Safety-Critical Function: A function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity. [3]
36. Severity: The magnitude of potential consequences of a mishap to include: death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss. [3]
37. Supplier: An entity that provides or makes available for use all or part of a machine or system. [6]
38. System: The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results. [3]
39. System-of-Systems: A set or arrangement of independent systems that are related or connected to provide a given capability. [3]
40. System Safety: The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and costs throughout all phases of the system lifecycle. [3]
41. System Safety Engineering: An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated. [3]
42. System Safety Management: All plans and actions taken to identify hazards; assess and mitigate associated risks; and track, control, accept, and document risks encountered in the design, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and infrastructure. [3]
43. Target Risk: The projected risk level the PM plans to achieve by implementing mitigation measures consistent with the design order of precedence in the Hierarchies of Control. [3]
44. Tolerable Risk: Level of risk that is accepted in a given context based on the current values of society. [6]
45. User: Any entity that utilizes the machine, system, or related equipment. [6]
46. User Representative: For fielding events, a Command or agency that has been formally designated in the Joint Capabilities Integration and Development System process to represent single or multiple users in the capabilities and acquisition process. For non-fielding events, the user representative will be the Command or agency responsible for all personnel, equipment, and environment exposed to the risk. For all events, the user representative will be a peer level equivalent to the risk acceptance authority. [3]

B. Product Characterization

Technologists have always strived to provide humankind with products and machines that do their bidding. This has resulted in a marvel of technology that has sprung into existence through unfettered intuition and systematic discipline. With each contribution of a contrivance, there are corresponding risks that are the preoccupation of the safety community. To assess each risk, one begins with the characterization of the product or system. Each of the protocols studied for this paper contain an extensive write-up of the elements required to begin a risk assessment. The actual details are not the focus of this paper, only the overall commonality among the protocols.

C. Hazard Identification

The identification of hazards is a classic building block of almost every safety analysis including the Risk Protocols under study. The Safety Theorem assures us that every physical contrivance presents an infinite number of hazards. This theorem, which is discussed by Barnett in [1], can be stated as,

Safety Theorem:

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

For noncritical mishaps risks are normally assessed for intended, extended, and reasonably foreseeable misuses of a product. For critical mishaps additional risks may be identified that arise from speculation or systems safety analysis. It should be noted that almost all safety standards focus on hazards and their mitigation.

The identification of product misuses is among the most challenging exercises in risk analysis. This derives from the quotation, "It is impossible to make anything foolproof because fools are so ingenious (Author unknown)." The prediction of miscreant behavior remains a risky art form.

D. Definition of Risk

At the present time, no quantitative definition of risk is available. The various qualitative definitions of risk; Colloquial, Standards, Regulatory, Torts, and Heuristic; have recently been presented by Barnett in [2]. In spite of this dreadful state of affairs, the Definition of Risk remains a building block that is incorporated into every Risk Analysis protocol. In order to accomplish this, the safety community has introduced the notion of a Risk Matrix. Here, by entering the independent variables hazard severity and hazard exposure into a risk matrix, one obtains a four- or five-part Risk ranking, e.g., High, Serious, Medium, Low, and Eliminated. A typical Risk Assessment Matrix is shown in Exhibit 1 which is taken from the Department of Defense, MIL-STD-882E [3].

It should be noted that the lowest risk category, Eliminated, rarely appears on other Risk Protocols. For critical mishaps, this is often the only category for Tolerable Risk.

The shortcomings associated with the definition of risk include the creation of a Risk Matrix; MIL-STD-882E, for example, recommends the Risk Assessment Matrix described in Exhibit 1 "unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense Component

policy." Further, the definition of risk has not been compared to real statistical data. The characterization of the input variables used in the Matrices, hazard severity and hazard exposure, are treated extensively in the various protocols.

**Exhibit 1. Risk assessment matrix (MIL-STD-882E [3])**

| RISK ASSESSMENT MATRIX | | | | |
|---|---|---|---|---|
| Severity / Probability | Catastrophic (1) | Critical (2) | Marginal (3) | Negligible (4) |
| Frequent (A) | High | High | Serious | Medium |
| Probable (B) | High | High | Serious | Medium |
| Occasional (C) | High | Serious | Medium | Low |
| Remote (D) | Serious | Medium | Medium | Low |
| Improbable (E) | Medium | Medium | Medium | Low |
| Eliminated (F) | Eliminated | | | |

Notwithstanding their attempts, the protocols use subjective language to pigeonhole continuous variables into only a handful of categories. In the end, Risk presents at only four or five levels which are not refined enough to make distinctions among competitive products or to sign-off on the mitigation of catastrophic hazards.

E. Risk Acceptance Criteria

At any stage in the development of a product its risk can be determined using a Risk Assessment protocol. The magnitude of this risk is now processed by the building block "Risk Acceptance Criteria" where a decision is made to either accept the risk or mediate the design until a tolerable risk is achieved. Each of the protocols provides guidance in making this decision, e.g., ISO/IEC Guide 51:2014E [4] suggests that Tolerable Risk can be determined by:

47. The current values of society;
48. The search for an optimal balance between the ideal of absolute safety and what is achievable;
49. The demands to be met by a product or system;
50. Factors such as suitability for purpose and cost-effectiveness.

Risk acceptance is always a subjective judgment call.

F. Hierarchies of Control

Whenever the determination of risk is too high, design mitigation efforts are undertaken as prescribed by the building block, Hierarchies of Control. A collection of these hierarchies is discussed by Barnett in [5] where a full set of protective measures is organized to systematically reduce the risk of a product or system. Such hierarchies constitute rules-of-thumb born from speculation and given legitimacy by consensus, not research. A typical hierarchy may incorporate the following safety concepts: Eliminate Hazards, Reduce the Hazard Severity, Safeguard, Warn, and Use Personal Protective Equipment. Each of the hierarchies of control reviewed by Barnett began with the admonition Eliminate the Hazard. As it turns out this is a unique amelioration strategy because of the following Elimination Theorem:

Elimination Theorem:

"A system can achieve Zero Risk if and only if all its hazards are eliminated."

Other than eliminating the hazard, all other remediation strategies continue to exhibit hazards with their associated risks. Furthermore, the analyst should take into account that adding a protective measure may add additional hazards or increase risks from other hazards.

G. Control Management

The final building block common to every Risk Analysis protocol, Control Management, concerns itself with the order and application strategy of all the other building block disciplines used in the pursuit of tolerable risk. It specifies the role of the machine/system supplier and user in the application and documentation of risk assessment and risk reduction procedures. Management schemes may be introduced that are unique to a genre of protocols, e.g., validation requirements may be called for when critical mishaps are foreseeable. This subject will be pursued further in the following sections of this paper.

## 2. Risk Acceptance and Risk Reduction Protocols

Our survey of the available Risk Analysis protocols reveals three general types of protocols that are distinguished by their inclusion or exclusion of Critical Mishaps, their requirement for Validation, and their reliance on in-house or independent authority for Risk Acceptance Criteria. All embrace the same building blocks; to wit, Product/System Characterization, Hazard Identification, Definition of Risk, Risk Acceptance Criteria, Hierarchies of Controls, and Control Management. Every protocol includes the full collection of protective measures and each candidate has a detailed description of the elements that enter into every building block.

A. Type 1 Protocol Characteristics: No Critical Mishaps, No Validation Requirements, and In-House Risk Acceptance Criteria

A typical Type 1 protocol is associated with the ANSI B11.TR3-2000 Technical Report for Machine Tools, "Risk Assessment and Risk Reduction - A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools [6]." Exhibit 2 describes the risk assessment and risk reduction process depicted in the report with all of the classic building blocks. The Risk Analysis objective is to achieve a tolerable risk for the product/system under consideration. Generally, this task requires the participation of the product Supplier and the product User. The management of their activities is shown in the flowchart described in Exhibit 3 entitled "Relationship between supplier and user showing the hierarchy of applying protective measures." Referring to this exhibit, we observe that that the risk is continually reduced to a level called, Residual Risk. When the residual risk is found to be tolerable, the Risk Analysis is complete. The in-house Risk Analysis team establishes the appropriate Tolerable Risk level. The following Type 1 protocols are available:

1. "ANSI B11.TR3-2000, Risk Assessment and Risk Reduction - A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools," American National Standards Institute, Inc. 1819 L Street NW, Washington, DC 20036.

- Comment 1[1]: This technical report is a guideline intended for use on all new or modified machines and equipment designs and processes.

[1] Most of the critiques are quotes from the source document.

- Comment 2: All of the ANSI B11 Series machine standards call for Risk Analysis protocols that are guided by this ANSI publication.
- Critique 3: Every building block incorporated into this report is fundamentally flawed. They are based on consensus, not research; they have not been validated; they embrace concepts that cannot be quantified; and they are embroiled in subjective language.
- Critique 4: "This guideline estimates risks (p. ii)."
- Critique 5: "This technical report recognizes that zero risk does not exist and cannot be attained. However, a good faith approach to risk assessment and risk reduction as described in this guide should achieve a tolerable risk level (p. vi)."
- Critique 6: "Because these tasks can be so diverse, the risk assessment process can best be conducted using a team of knowledgeable and affected persons (p. vi)."

2. "Safety Through Design," Wayne C. Christiansen and Fred A. Manuele, National Safety Council, NSC Press Product No. 17644 - 0000, 1999 [7].

- Comment 1: Mission - "To reduce the risk of injury, illness and environmental damage by integrating decisions affecting safety, health and the environment in all stages of the design process."
- Critique 2: "move from the 'retrofit' era to the 'Safety Through Design' era."
- Critique 3: "The work of the Institute for Safety Through Design is not only to have the safety through design concepts adopted by industry, but also to impact the university engineering education programs."
- Critique 4: "The editors envisioned and secured a series of excellent authors having a diversity of background, business and industry experience, and success in their areas of expertise, that provided material based on industry experience and minimally on academic postulations."
- Critique 5: "Readers will find divergent viewpoints, which are acceptable, since there has been success with many different approaches to their application."

3. ANSI/AIHA Z10-2005, "American National Standard - Occupational Health and Safety Management Systems," American National Standards Institute (ANSI) and the American Industrial Hygiene Association (AIHA), Appendix D and E, Published by American Industrial Hygiene Association, 2700 Prosperity Ave., Ste. 250, Fairfax, VA 22031, Copyright 2005, Stock Number: SMAA05-69 [8].

- Comment 1: Scope. This standard defines minimum requirements for occupational health and safety management systems (OHSMS).
- Critique 2: "The management system in this standard is designed to continually improve safety and health performance, and is aligned with the traditional Plan - Do - Check - Act approach for improving the workplace."

4. ANSI/RIA R15.06 - 1999, "American National Standard for Industrial Robots and Robot Systems - Safety Requirements," American National Standards Institute (ANSI) and Robotic Industries Association (RIA), Published by Robotic Industries Association, PO Box 3724, Ann Arbor, MI 48106, 1999 [9].

- Critique 1: An example risk assessment methodology is presented in Annex C. It begins with a brief list of general considerations.

General Considerations:

"One of the main keys to performing a successful risk assessment that captures all of the tasks and hazards associated with the equipment, is the participation of those individuals that work with and on the equipment. As a minimum this should include the following types of personnel:

- Operator
- Maintenance personnel (electricians, pipefitter, toolmaker, set-up, programmer)
- Engineer, System Engineer and or Design Engineer

Optimum group size would be 4 - 8 of the above types of personnel.

The other key players is the person performing the risk assessment. This individual should have experience in working with groups and have familiarity with the equipment process.

The process used to solicit input on the tasks and hazards is best conducted in a team brainstorming format."

- Comment 2: A standard requirement for control reliability is found in Clause 4.5.4; "Control reliable safety circuitry shall be designed, constructed and applied such that any single component failure shall not prevent the stopping action of the robot."

5. Engineering and Technology, 13th Edition, "Accident Prevention Manual for Business and Industry," Editors: Philip E. Hagan, John F. Montgomery, and James T. O'Reilly, Copyright 2009 by the National Safety Council, Chapter 1: Safety Through Design [10].

- Critique 1: A Risk Matrix is presented that is taken from MIL-STD-882D [11]. In addition, another Risk Acceptance Matrix is displayed in their Table 1-B that provides Numerical Gradings; this is shown in Exhibit 4. Quoting from Chapter 1, "It is presented here for people who prefer to deal with numbers rather than qualitative indicators, (take care, though: the numbers are arrived at judgmentally and are qualitative.)"
- Critique 2: The following two definitions are introduced in Chapter 1:
  "Acceptable Risk: Risk for which the probability of a hazard-related incident or exposure occurring, and the severity of harm or damage that may result are as low as reasonably practicable (ALARP) and tolerable in the setting being considered.

ALARP: The level of risk that can be further lowered only by an increment in resource expenditure that cannot be justified by the resulting decrement of risk."

Beware of terminating mitigation efforts on the basis of ALARP because of diminishing returns on amelioration efforts.

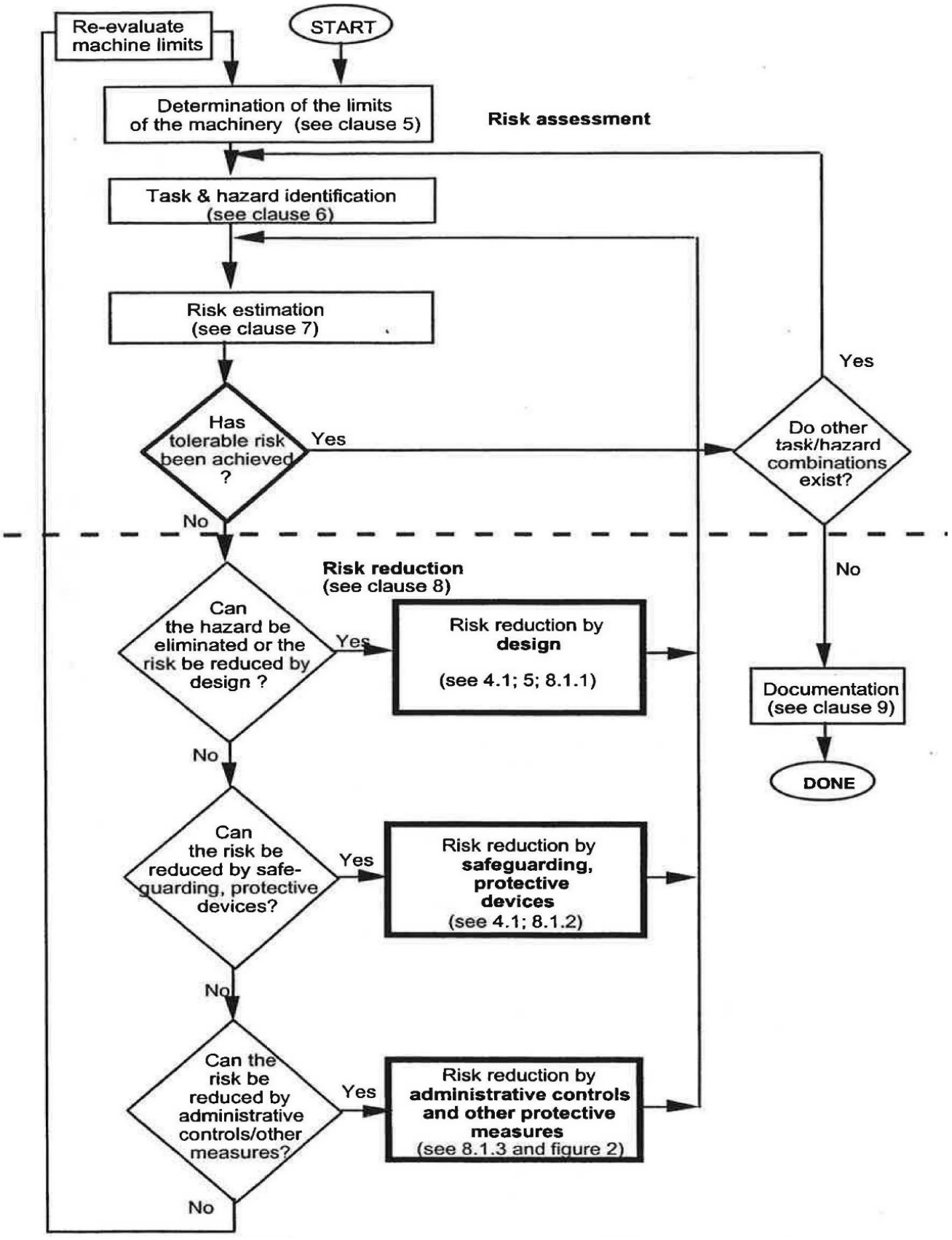
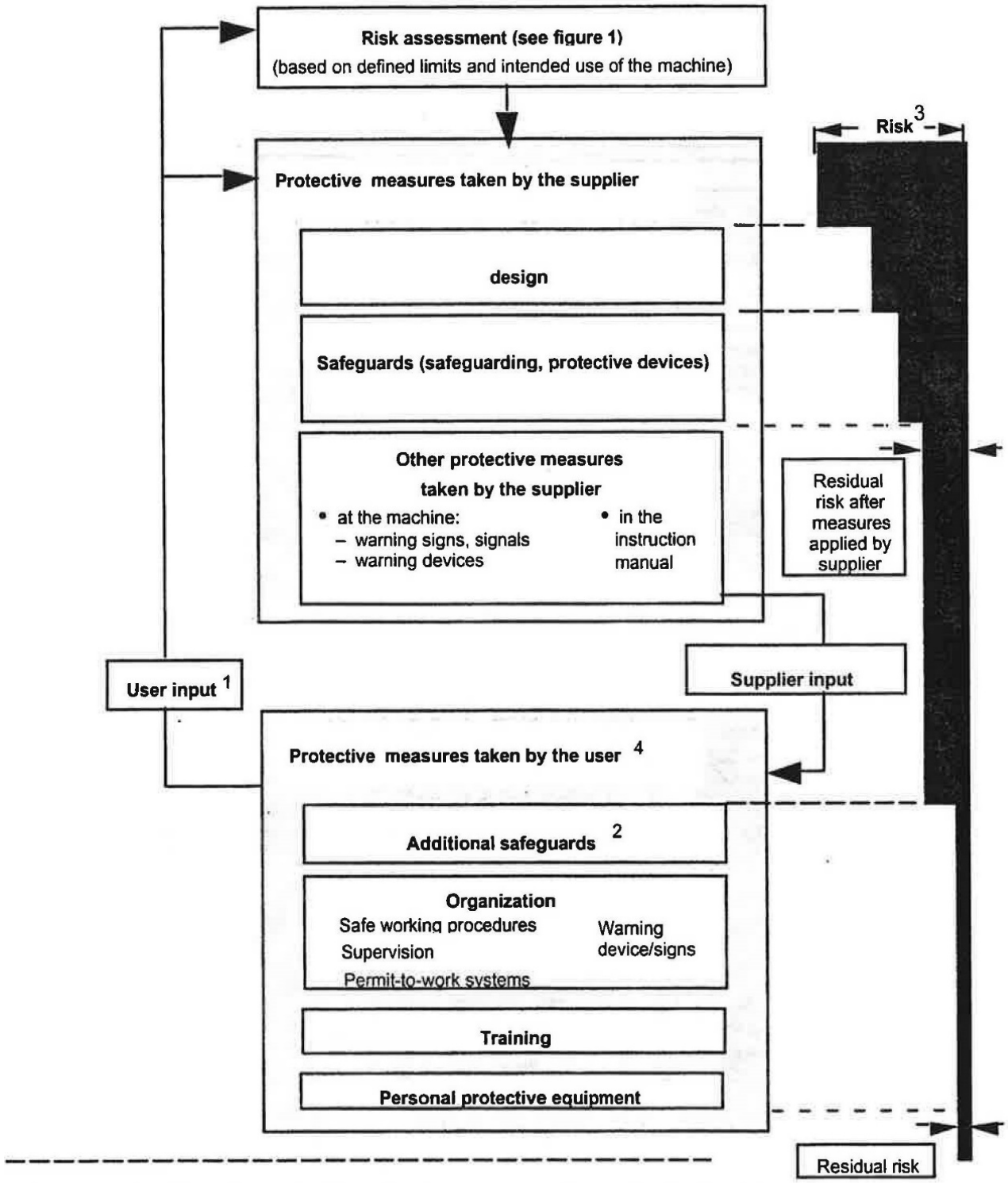



**Exhibit 2.** Risk assessment and risk reduction process (ANSI B11.TR3-2000 [6])




1 User input is that information received from either the user community regarding the intended use of the machine in general or that which is received from a specific user.

2 Those protective measures required due to specific process(es) not envisioned in the intended use of the machine.

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

4 Risk reduction taken by the user is to be considered collectively since not all elements may be implemented or in the order portrayed.

**Exhibit 3.** Relationship between supplier and user showing the hierarchy of applying protective measures (ANSI B11.TR3-2000 [6])

**Exhibit 4. Quantitative Risk Matrix**

| Table 1-B. Risk Assessment Matrix: Numerical Gradings | | | | | |
|---|---|---|---|---|---|
| Occurrence Probabilities and Values | | | | | |
| Severity Levels and Values | Frequent (5) | Likely (4) | Occasional (3) | Seldom (2) | Unlikely (1) |
| Catastrophic (5) | 25 | 20 | 15 | 10 | 5 |
| Critical (4) | 20 | 16 | 12 | 8 | 4 |
| Marginal (3) | 15 | 12 | 9 | 6 | 3 |
| Negligible (2) | 10 | 8 | 6 | 4 | 2 |
| Insignificant (1) | 5 | 4 | 3 | 2 | 1 |

Very high risk: 15 or greater; high risk: 9 to 14; moderate risk: 4 to 8; low risk: under 4.

6. ANSI B11.3-2002, "Safety Requirements for Power Press Brakes," American National Standard for Machine Tools, Approved February 14, 2002, Secretariat and Accredited Standards Developer: The Association for Manufacturing Technology, Attention: Safety Department, 7901 West Park Drive, McLean, VA 22102 [12].

- Comment 1: The standard uses "shall" language when calling for Risk assessment/risk reduction.
- Comment 2: The standard does not present enough details to assess risk; however, it refers extensively to ANSI B11.TR3 for guidance.
- Critique 3: Under Explanatory Information (p. 12): "Zero risk does not exist and cannot be attained. However, a good faith approach to risk assessment and risk reduction should reduce risk to a tolerable level. For further information on tolerable risk, see ANSI B11.TR3."
- Comment 4: A Risk Matrix is not presented in the standard.
- Comment 5: Annex B - Task/Hazard Identification (informative): This Annex lists sources of hazards associated with the design and construction, installation, use and care of the press brake. This two-page section projects the strength of a consensus standard.

7. ANSI B11.1-2001, "Safety Requirement for Mechanical Power Presses," American National Standard for Machine Tools, Secretariat and Accredited Standards Developer: The Association for Manufacturing Technology, 7901 Westpark Drive, McLean, VA 22102-4269, Approved November 6, 2001 [13].

- Comment 1: This standard requires the execution of a Risk Analysis.
- Critique 2: The standard explicitly calls out for most of the building blocks; Task and Hazard Identification, Hierarchies of Controls, Risk Acceptance Criteria, and Control Management. The building block Definition of Risk with its associated Risk Matrix is implicit; the determination of risk must follow ANSI B11.TR3-2000.
- Comment 3: The identification of reasonably foreseeable tasks is described in Clause 5.1.

8. ISO 14121-1: 2007(E), "Safety of Machinery - Risk Assessment - Part 1: Principles," First Edition, 2007-09-01, ISO, Case postale 56, CH 1211, Geneva 20, Switzerland [14].

- Comment 1: This standard is nominally identical to ANSI B11.TR3-2000.
- Comment 2: This standard is a typical Type I protocol; it differs from the ISO/IEC Guide 51:2014(E) which is a Type II protocol that includes an additional building block, Validation and Documentation.

9. ISO/TR 14121-2: 2007, "Safety of Machinery - Part 2: Practical Guidance and Examples of Methods," First Edition: 2007-12-15, ISO, Case postale 56, CH 1211, Geneva 20, Switzerland [15].

- Critique 1: "The purpose of risk assessment is to identify hazards, and to estimate and evaluate risk so that it can be reduced. There are many methods and tools available for this purpose and several are described in this document. The method or tool chosen will largely be a matter of industry, company or personal preference. The choice of a specific method or tool is less important than the process itself. The benefits of risk assessment come from the discipline of the process rather than the precision of the results; as long as a systematic approach is taken to get from hazard identification to risk reduction, all the elements of risk are considered. (p. v)"
- Critique 2: "The risk assessment is performed once again when the design is finalized, and when a prototype exists and after the machinery has been in use for a while. (p. v)"
- Critique 3: "Risk assessment is generally more thorough and effective when performed by a team. The size of a team varies according to the following:

a) the risk assessment approach selected;
b) the complexity of the machine;
c) the process within which the machine is utilized;

The team should bring together knowledge and different disciplines and a variety of experience and expertise. However, a team that is too large can lead to difficulty and remaining focused or reaching consensus. The composition of the team can vary during the risk assessment process according to the expertise required for a specific problem. A team leader, dedicated to the project, should be clearly identified, as the success of the risk assessment depends on his or her skills.

However, it is not always practical to set up a team for risk assessment and it can be unnecessary for machinery or hazards are well understood and risk is not high.

Note: Confidence in the findings of a risk assessment can be improved by consulting others with the knowledge and expertise, as outlined in 4.2.2 and by another competent person reviewing the risk assessment. (p. 2)"

- Critique 4: "Moreover, resources are better directed at risk reduction efforts rather than towards an

attempt to achieve absolute precision and risk estimation (p. 8)."

- Critique 5: "Generally, designers can only establish that risk has been reduced as far as practicable or that the objectives of risk reduction have been achieved (p. 8)."
- Critique 6: "A risk matrix is a multidimensional table allowing the combination of any class of severity of harm with any class of probability of occurrence of that arm. The more common matrices are two-dimensional but a matrix can have as many as four dimensions (p. 8)."
- Critique 7: "5.4.4.5 Quantified Risk Estimation: All of the above methods are qualitative in nature. Although numbers are used with some tools and others express risk levels numerically, their nature is essentially qualitative. There are no common reference data and a numerical risk level estimated using one tool cannot directly be compared to one estimated using another.

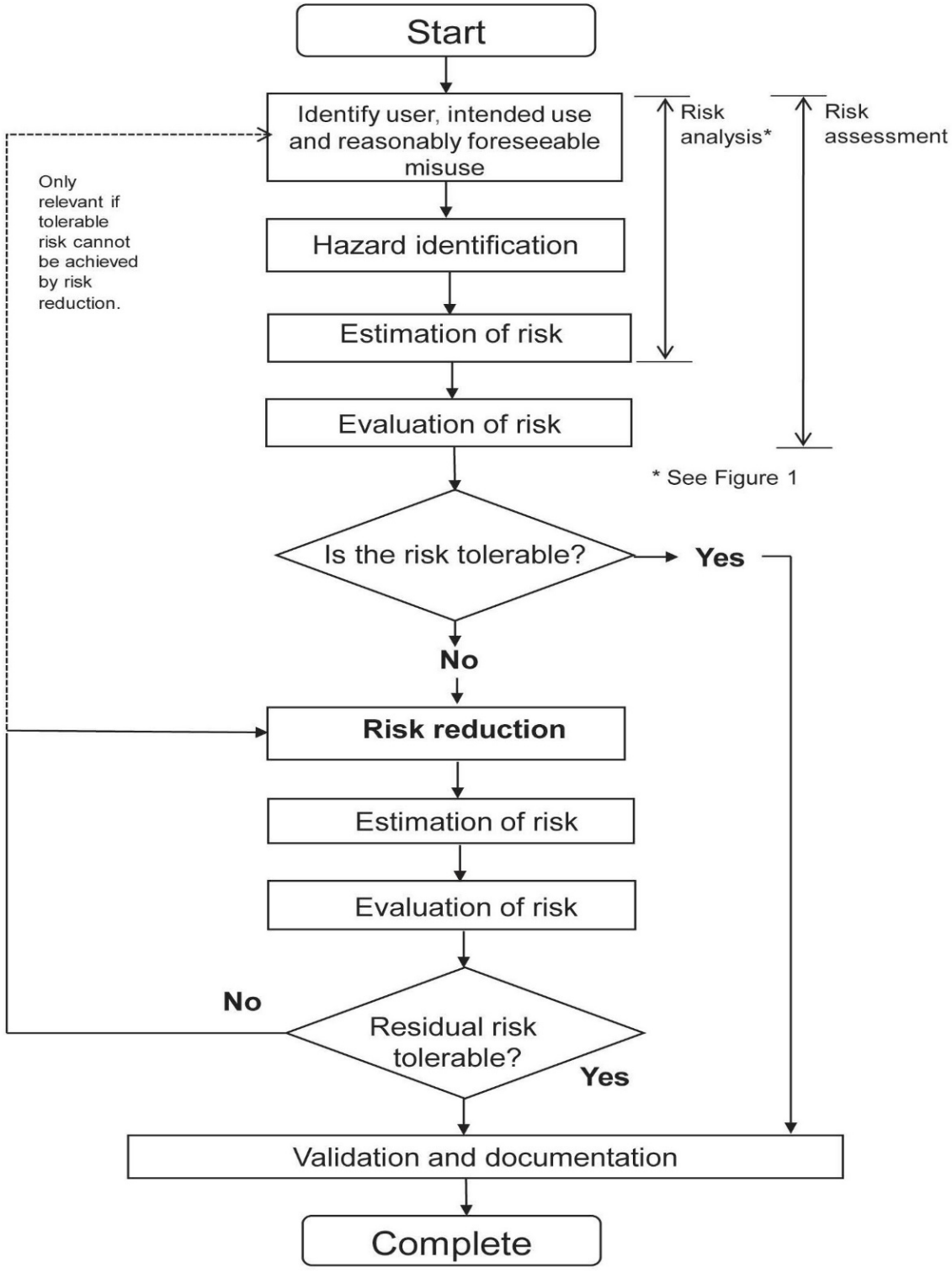



**Exhibit 5.** Iterative process of risk assessment and risk reduction (ISO/IEC Guide 51: 2014(E) [4])

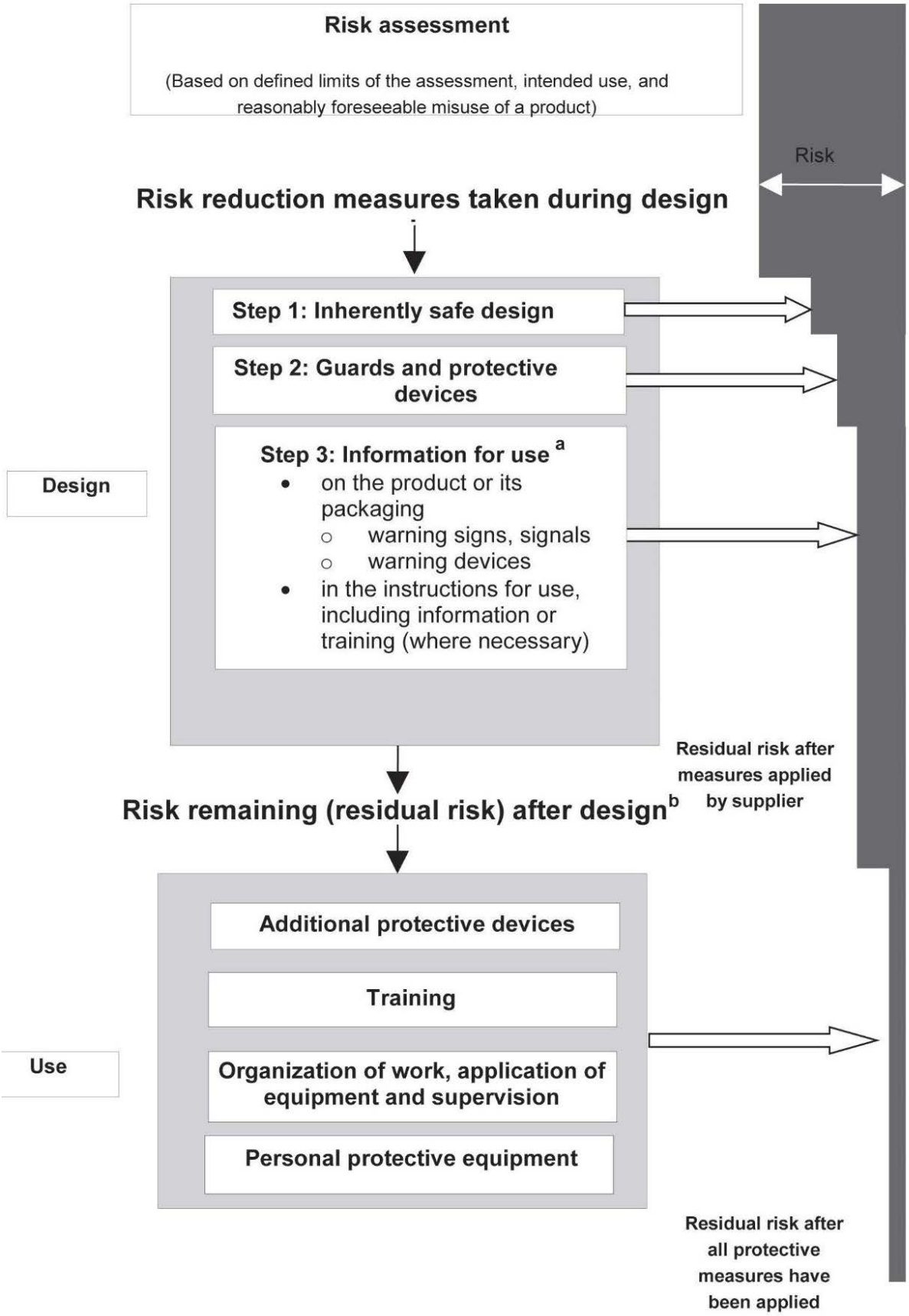



**Exhibit 6.** Risk reduction: combination of efforts at design and use phase (ISO/IEC Guide 51: 2014(E) [4])

Quantified risk estimation consists of the mathematical calculation, as accurately as possible with the data available, of the probability of a specific outcome occurring during a specific duration of time. Risk is often expressed as the annual frequency of the death of an individual. Quantified risk estimation allows the calculated risk to be compared with criteria that can be related back to an actual number of deaths per year or

accident statistics. It allows risk reduction measures to be evaluated in terms of by how much they reduce the risk so that the most cost-effective solution can be chosen. Unlike the qualitative methods that estimate the risk from each hazardous situation separately, quantified risk estimation is generally used to estimate the total risk from all sources to an individual (pp. 9 - 10)."

- Comment 8: "Documentation of the Risk Assessment: It is important that the process be properly documented in order to allow examination of decisions at a later date by others who've not been directly involved in the risk assessment (p. 15)."
- Comment 9: This document provides a thorough discussion of Risk Analysis that includes several different methods of determining risk. In addition, a number of different Risk Matrices are presented. There are no requirements for validation and no requirements for outside agencies to determine Risk Assessment Criteria.

B. Type 2 Protocol Characteristics: No Critical Mishaps, Requires Validation, and In-House Risk Acceptance Criteria

A typical Type 2 protocol is presented in the ISO/IEC Guide 51:2014(E), "Safety aspects - Guidelines for their inclusion in standards." The iterative process of risk assessment and risk reduction is outlined in Exhibit 5 where a new building block has been added, Validation and Documentation. Validation is discussed in Section 6.4, "Standards should include guidance to validate the implemented risk reduction measures, including: their effectiveness, e.g. test methods." Observe that the validation and documentation requirement has been placed as the last activity in the Risk Analysis process. Presumably, this step will mitigate the fundamental shortcomings of the building blocks and any errors made in the execution of the algorithms. Recall that the building blocks are rules of thumb that were created by consensus and speculation, not research. Exhibit 6, entitled, "Risk reduction: combination of efforts at design and use phase," is almost identical to Exhibit 2 for the Type 1 protocol. It is worth repeating that the Residual Risk must be equal to or lower than the Tolerable Risk before the product/system being studied is accepted. For Type 2 protocols the establishment of the Tolerable Risk level falls within the purview of the in-house Risk Analysis team.

The following Type 2 protocols are available:

1. ISO/IEC Guide 51:2014(E), "Safety aspects - Guidelines for their inclusion in standards," International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), Case postale 56, CH - 1211, Geneva 20, Switzerland.
   - Comment 1: "This Guide aims to reduce the risk arising from the design, production, distribution, use (including maintenance) and destruction or disposal of products or systems."
   - Critique 2: Important observation - "Where hazards or hazardous situations with multiple risks have been identified, care should be taken to prevent risk reduction measures chosen to reduce one risk from resulting in another intolerable risk."
   - Critique 3: "Inherently safe design measures are the first and most important step in the risk reduction process. This is because protective measures inherent to the characteristics of the product or system are likely to remain effective, whereas experience has shown that even well designed guards and protective devices can fail or be violated, and information for use might not be followed." It should be noted that every proposed set of Hierarchies of Controls begins with the admonition to "eliminate hazards."
   - Critique 4: "Work on a standard starts with the identification of all the safety aspects to be covered. At this stage, it is essential to gather all relevant information [e.g. accident data, research reports.]"
   - Critique 5: "Requirements for risk reduction measures (protective measures) should: a) be laid down in precise and clearly understandable language; b) be technically correct."
   - Critique 6: "Where performance-based risk reduction measures are prescribed by the standard, the requirements should include detailed verification methods for determining compliance with the performance requirements."
   - Critique 7: "It is advisable to minimize the use of subjective terms or words unless they are defined in the standard."
2. "ANSI B11.0 - 2020, "Safety of Machinery," American National Standard Institute, B11 Standards, Inc. POB 690905, Houston, TX 77269, Approved: December 16, 2019 [16].
   - Comment 1: Harmonization: "This standard has been harmonized with international (ISO) and European (EN) standards by the introduction of hazard identification and risk assessment as the principal method for analyzing hazards to personnel to achieve a level of acceptable risk."
   - Comment 2: "This standard guides machinery suppliers and users through a risk assessment process that identifies reasonably foreseeable hazards and reduces corresponding risks to an acceptable or tolerable level."
   - Comment 3: The ANSI B11.0 standard is a Type-A standard, i.e., a basic safety standard that gives basic concepts, principles for design, and general "foundational" aspects that can be applied broadly across different types of machinery.
   - Comment 4: "Risk assessment is a scalable process, which simply means that risk assessment can be applied to a single hazard, to multiple hazards of a simple machine, or to hazards on more complex (automated) machine systems."
   - Comment 5: "Risk assessment can be applied to new machines, to existing machines, or modified machines."
   - Comment 6: New definition: Point of Operation - The location in the machine where the material or workpiece is positioned and work is performed on the material or workpiece.
   - Comment 7: New definition: Risk Reduction Measure - this is the new name for "protective measure."
   - Comment 8: A thorough discussion of the risk assessment process is found in Clause 6 (pp. 37 - 49). An outline of this process is presented in

Exhibit 7. It should be noted that an additional building bock has been added to the Type-1 protocols; namely, Validate Solutions. This vital distinction identifies ANSI B11.0-2020 as a Type-2 protocol.

- Comment 9: A complete discussion of General Risk Reduction Requirements may be found in Clause 7. Both Clauses 6 and 7 are supported by Annexes A through H.
- Comment 10: A number of risk assessment matrices are treated in Annex F.
- Critique 11: Validation and verification of risk reduction measures is covered Clause 6.8. The shortcomings of the Type-1 protocols are circumnavigated in the light of an effective validation program.

3. ANSI B11.2 - 2013, "Safety Requirements for Hydraulic and Pneumatic Power Presses," American National Standard for Machines, Secretariat and Accredited Standards Developer: B11 Standards, Inc. POB 690905, Houston, TX 77069-0905, Approved: February 12, 2013 [17].

- Comment 1: Clause 4 - Responsibility: "Machine suppliers and users have responsibilities for defining and achieving acceptable risk. The supplier and user either separately or jointly shall identify hazards, assess risks and reduce risks to an acceptable level within the scope of their respective work activities. See ANSI B11.0."
- Critique 2: The following Normative Reference constitutes a provision of this American National Standard: ANSI B11.0-2010, Safety of Machinery; General Requirements and Risk Assessment. (Note: ANSI B11.TR3-2000 has been incorporated into the B11.0 standard.) This implies that the normal building blocks are adopted by the subject standard.
- Critique 3: The iterative process as it relates to risk assessment and risk reduction is identical to Exhibit 7. Observe the addition of the building block, Validate Solutions. Clause 7.4 entitled Testing and Start-UP describes the testing and start-up procedures that are required.
- Critique 4: Clause E7.4(a): "All testing and start-up procedures should be based on a risk assessment. This provides a confidence level for the procedure."
- Comment 5: This standard is a Type-C standard: "(machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines."

C. Type 3 Protocol Characteristics: May Address Critical Mishaps, Requires Validation, Requires Independent Authority for Risk Acceptance.

A representative Type 3 protocol is provided by MIL-STD-882E, "Department of Defense, Standard Practice, System Safety," USA, 11 May 2012. This system safety standard practice identifies the Department of Defense (DOD) Systems Engineering approach to eliminating hazards where possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence. The order precedence used in the Hierarchy of Controls adopted in this military standard is similar to those used in Type 1 and Type 2 protocols, e.g.,

- Eliminate hazards through design selection.
- Reduce risk through design alteration, i.e., reduce the severity and/or the probability of the mishap potential caused by the hazards.
- Incorporate engineered features or devices.
- Provide warning devices.
- Incorporate signage, procedures, training, and personal protective equipment.

The military standard also uses the same Definition of Risk encountered in Type 1 and Type 2 protocols. The Risk Matrix associated with this building block was presented in Exhibit 1. Aids for determining the independent variables associated with the risk matrix, severity and exposure (probability level), are displayed in Table 1 and Table 2 respectively. Type 3 protocols are distinguished from Type 1 and Type 2 protocols by two additional building blocks, Verify, Validate and Document Risk Reduction: Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing demonstration, or inspection.

Risk Acceptance Criteria: Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by an appropriate authority.

The following Type 3 protocols are available:

1. MIL-STD-882E, "Department of Defense, Standard Practice, System Safety," USA, 11 May 2012, https://assist.dla.mil

- Critique 1: Task 401 of this military standard is entitled Safety Verification. Under task description it states, "The contractor shall define and perform analyses, tests, and demonstrations; develop models; and otherwise verify the compliance of the system with safety requirements on safety-significant hardware, software, and procedures (e.g., safety verification of iterative software builds, prototype systems, subsystems, and components.) Induced or simulated failures shall be considered to demonstrate the acceptable safety performance of the equipment and software.
- Critique 2: The verification and validation requirement in the military standard compensates for the impoverished veracity of the standard building blocks. Where critical mishaps are possible in systems such as nuclear power plants or aircraft, validation is essential for achieving "near risk-free designs."
- Critique 3: The Government provides an exacting oversight capability on the performance of the Contractor and system user that is not available in the Type 1 and Type 2 protocols.

2. "Safety and Health for Engineers, 2nd Edition," Roger L. Brauer, Published by John Wiley & Sons, Inc., Hoboken, NJ, Copyright 2006, Chapter 36 [18].

- Comment 1: Presents the Military Standards (MIL-DTD-882 B, D)

3. "On the Practice of Safety - 3rd Edition," Fred A. Manuele, Wiley-Interscience, John Wiley and Sons, Inc., 111 River Street, Hoboken, NJ 07030, Copyright 2003, Chapters 13, 14, 15 and 18 [19].

- Comment 1: This reference book analyzes the MIL-STD-882D (10 February 2000) standard.
- Critique 2: The shortcomings of the fundamental building blocks which are components of all the Risk Analysis protocols are studied in great detail. The author identifies the subjective nature of the fundamental concepts that are the backbone of risk analysis and risk reduction. He asserts, with great justification, that the protocols represent an art form as opposed to an algorithm based on a solid scientific foundation. The protocols provide at best a qualitative representation of risk; they fall short of describing risk quantitatively.
- Critique 3: The "Validation" building block, which is not included in Type 1 protocols, is largely ignored in the author's treatment of System Safety. Mr. Manuele offers an important observation, "With the hope of generating a further interest by generalist safety professionals in the basics of system safety, I suggest that they concentrate on those basic concepts through which gains can be made in an occupational or product design setting and avoid being repulsed by the more exotic hazard/risk assessment methodologies."
- Critique 4: In my opinion, Prof. Ralph L. Barnett, by not pursuing exotic hazard/risk assessment methodologies and elaborate analytical methods we have left the safety profession bereft of the intellectual underpinnings that are the foundation of both engineering and scientific disciplines. Safety programs have all but disappeared from the universities in this country because of a lack of funding and political interest; discussing transitory codes, standards, regulations, and courtroom decisions are not the stuff that professors can publish without perishing.
- Critique 5: Type 3 protocols have flourished in those areas involving critical mishaps, e.g., the design of ships, missiles, and medical equipment. It should be noted that wherever safety requirements are unrelentingly strict, the manifold flaws in the risk protocols are bypassed in the pursuit of absolute safety. The risk methodologies emphasize the Design building block and call for Safeguarding Technology as the next rung in the Hierarchies of Controls. These two building blocks are dominated by engineering and scientific disciplines. The nonsense of the Risk Matrix is avoided in the search for zero risk. And finally, the demand by independent agencies for oversight review, requires validation activities that are rich in data gathering and testing and research.

4. "Introduction to Safety Engineering," David S. Gloss and Miriam Gayle Wardle, Wiley-Interscience Publication, John Wiley and Sons, Inc., Copyright 1984, Chapter 27 [20].

- Comment 1: The System Safety used in Military Systems, as described in MIL-STD-882B, is paraphrased with a summary of the building block, Demonstration and Validation (see pp. 570 - 572).
- Comment 2: A three dimensional Risk Matrix using the variables Severity, Probability, and Extensiveness is presented on page 430. This concept is attributed to the National Institute of Occupational Safety and Health (NIOSH).

5. "Army Military Airworthiness Certification Criteria (AMACC)," Prepared by: US Army Combat Capabilities Development Command, Aviation and Missile Center, and Aviation Engineering Directorate, Redstone Arsenal, AL 35898, 12 March 2019 [21].

- Comment 1: This document is 616 pages in length without appendices A through T which are available at https://tdmd.avmc.army.mil/standardaero.htm.
- Comment 2: This document describes the US Army Aviation Airworthiness processes and the criteria, standards and methods of compliance necessary for airworthiness assessment on US Army manned and unmanned aircraft systems.
- Comment 3: Paragraph 14 focuses on System Safety. This section covers the implementation of a comprehensive and robust system safety program which spans the system lifecycle. The purpose of the system safety program is to identify any associated system hazards/risks, and to eliminate them where possible, or mitigate the risks such that the residual risks are at acceptable levels. This must be accomplished using MIL-STD-882E.
- Critique 4: In Paragraph 4.1.2 beginning on page 42 under Verification Methods, "The contractor shall show verification methods of similarity, analysis, test, demonstration, simulation, or inspection for the air worthiness substantiation. Verification by test is the standard and most accurate method of verification."

6. "Safety Engineering," James CoVan, John Wiley and Sons, Inc., Copyright 1995, Chapter 4, System Safety, pp. 154 - 166 [22].

- Comment 1: Based on standard MIL-STD-882B.

7. NASA-STD-8719.7, "Facility System Safety Guidebook," NASA Technical Standard, January 30, 1998 [23].

- Comment 1: This NASA Technical Standard provides guidance for NASA facility and safety professionals who are involved with the facility acquisition or modification/construction process and lifecycle phases at NASA installations.
- Comment 2: All of the classic Risk Assessment/Risk Reduction activities are described in detail; the presentation follows the format described in MIL-STD-882C.
- Critique 3: Critically and Validation - "Complex facilities with multiple interfaces, potential unidentified residual hazards, high energy sources, and a variety of controls and interlocks may require an Initial System Test prior to the Operational Readiness Review to verify that all hazards have been identified and either removed or controlled, that the subsystems operate correctly, and that subsystem interfaces have been properly designed and constructed (Clause 5.6.1)."
- Critique 4: Criticality and Validation - "NASA is currently pursuing various advanced missions. To develop the appropriate technology for these visions, NASA conducts intensive ground testing. NASA performs both manned and unmanned testing. Manned tests, many times, are conducted in

oxygen-enriched and/or pressurized environments or neutral buoyancy tanks. Unmanned tests may use high pressure liquid hydrogen or oxygen, anhydrous ammonia, hydrazine, or other dangerous media. High temperatures, pressures, accelerations, and electrical potentials are typical in most NASA test operations. This requires a special test safety program. Because the NASA test environment can be hazardous and complex state-of-the-art hardware systems are used, the safety organization should develop an integrated, independent test safety program. (Clause 6.3)"

- Critique 5: Risk Acceptance Criteria - "Test safety engineers operate at the "nuts and bolts" level and fully understand all systems and subsystems that will be tested. They also work with members of various divisions to help reach the common goal of achieving a successful test. The safety organization should be completely autonomous of any test organization and reports to the Center Director. This maintains the necessary independence that is required for appropriate oversight. Reconciling the seemingly mutual exclusive relationships is key to providing a meaningful safety function. (Clause 6.3)"

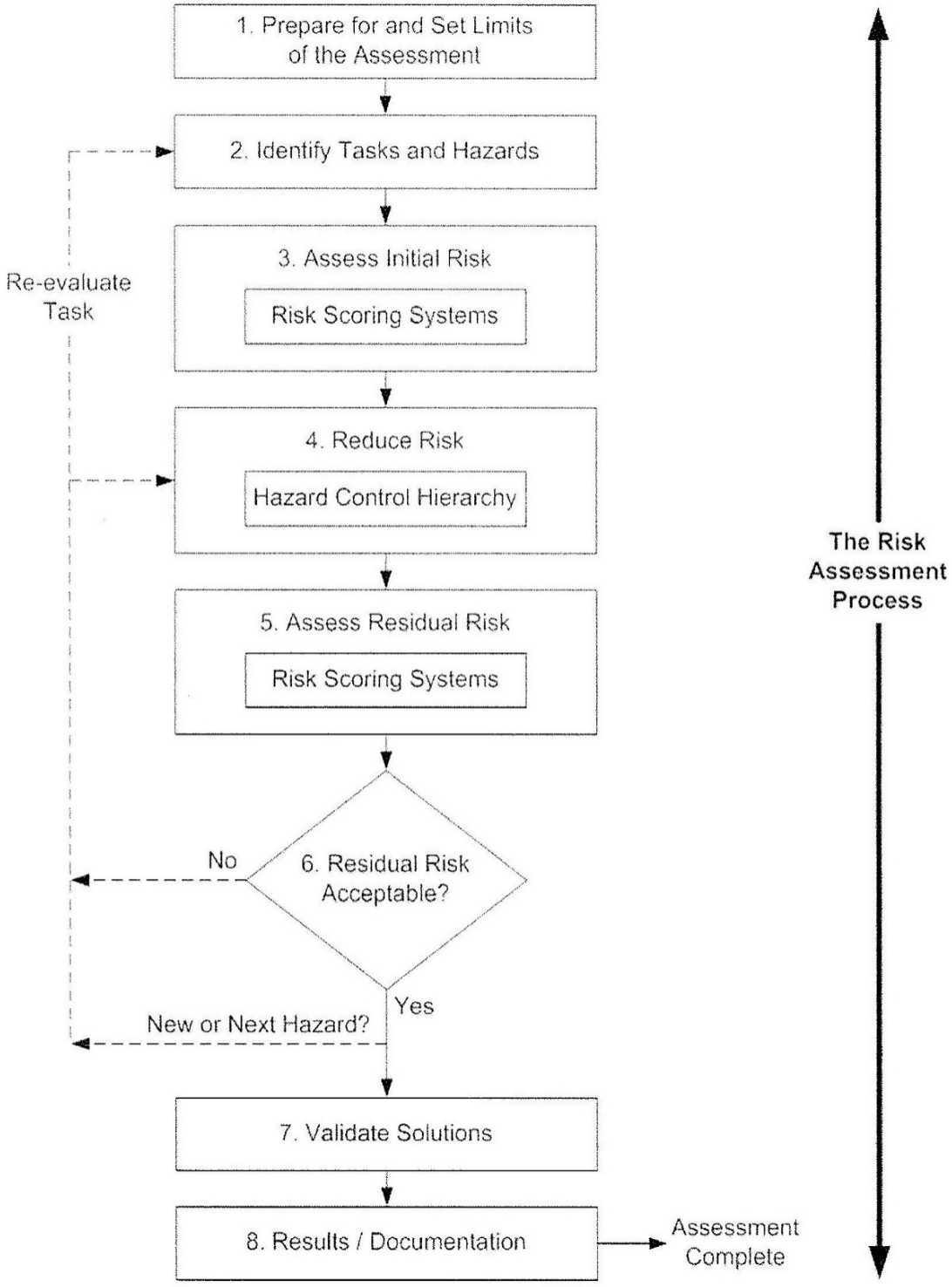



**Exhibit 7.** The Risk Assessment Process (ANSI B11.0-2020 [16], ANSI B11.2-2013 [17])

**Table 1. Severity Categories (MIL-STD-882E [3])**

| SEVERITY CATEGORIES | | |
|---|---|---|
| **Description** | **Severity Category** | **Mishap Result Criteria** |
| Catastrophic | 1 | Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M. |
| Critical | 2 | Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M. |
| Marginal | 3 | Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M. |
| Negligible | 4 | Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K. |

**Table 2. Probability Levels (MIL-STD-882E [3])**

| PROBABILITY LEVELS | | | |
|---|---|---|---|
| **Description** | **Level** | **Specific Individual Item** | **Fleet or Inventory** |
| Frequent | A | Likely to occur often in the life of an item. | Continuously experienced. |
| Probable | B | Will occur several times in the life of an item. | Will occur frequently. |
| Occasional | C | Likely to occur sometime in the life of an item. | Will occur several times. |
| Remote | D | Unlikely, but possible to occur in the life of an item. | Unlikely, but can reasonably be expected to occur. |
| Improbable | E | So unlikely, it can be assumed occurrence may not be experienced in the life of an item. | Unlikely to occur, but possible. |
| Eliminated | F | Incapable of occurence. This level is used when potential hazards are identified and later eliminated. | Incapable of occurence. This level is used when potential hazards are identified and later eliminated. |

## 3. Discussions and Observations

A. The last two decades have witnessed the widespread introduction of a risk analysis technique entitled, Risk Assessment and Risk Reduction, into the mainstream of professional safety philosophy. Because of this, the colloquial notion of safety as “freedom from harm” can be extricated from technical lexicons and replaced by the concept called Risk. Risk is defined as, “A combination of the probability of occurrence of harm and the severity of that harm.” Unfortunately, this definition demands that we give meaning to the notions probability of harm, severity of harm, combination, and the interpretation of harm. When a hazard gives rise to an accident, the resulting mischief is called harm and the magnitude of this harm is called Risk. The reciprocal of Risk is the definition of Technical Safety; if we use the word Risk we never have to use the word safety again.

For a given contrivance, the protocols for its risk assessment and risk reduction include at least six building blocks: Characterization of the product/system; Hazard Identification; Definition of Risk; Risk Acceptance Criteria; Hierarchies of Control; and Control Management. The reader should be aware of three different sets of criticisms for each of these building blocks.

1. The first criticism characterizes the protocols as art forms that are non-unique, qualitative in nature, and immersed in subjective language. This set of observations is treated extensively by Fred A. Manuele [18].
2. The second criticism constitutes a technical attack on the veracity of the building blocks. For example, the Hierarchy of Controls is not unique; in fact, for a given hierarchy various analysts may achieve different outcomes. The multiple hierarchies owe their existence to speculation and consensus, not research. Indeed, no validation has ever been reported. The Definition of Risk has a fundamental flaw that is circumvented by adopting multiple Risk Matrices that are based on consensus and speculation. The risk matrix artifice represents junk science without apology. The oldest building block, Hazard Identification, presents an unbounded number of hazards that are reduced to a finite selection of mediation candidates with the aid of concepts such as Reasonably Foreseeable Use,

Consensus Standards, Teamwork, Mediation and Prayer, and the Consultation of Experts. Prof. Barnett is only one of the observers that noticed that the Emperor has no clothes. These matters are further discussed in the peer-reviewed papers by Barnett,

- Safety Definitions: Colloquial, Standards, Regulatory, Torts, Heuristic, Quantitative [2].
- On the Safety Theorem [1].
- On the Safety Hierarchy and Hierarchy of Controls [5].
- Reasonably Foreseeable Use [24].
- Principles of Human Safety [25].

3. The final arbiters in this matter of efficacy are the authors of the various protocols that are unapologetically honest. My comments and critiques on the various Type 1 protocols reveal the following:

- The protocols estimate risks.
- A good faith approach to risk assessment and risk reduction should achieve a tolerable risk level.
- The risk assessment process can best be conducted using a team of knowledgeable and affected persons.
- The work of the Institute for Safety Through Design depends minimally on academic postulations.
- The process used to solicit input on the tasks and hazards is best conducted in a team brainstorming format.
- The benefits of risk assessment come from the discipline of the process rather than the precision of the results; as long as a systematic approach is taken to get from hazard identification to risk reduction, all the elements of risk are considered.
- Confidence in the findings of a risk assessment can be improved by consulting others with the knowledge and expertise and by another competent person reviewing the risk assessment.
- Moreover, resources are better directed at risk reduction efforts rather than towards an attempt to achieve absolute precision and risk estimation.
- All of the above methods are qualitative in nature. Although numbers are used with some tools and others express risk levels numerically, their nature is essentially qualitative. There are no common reference data and a numerical risk level estimated using one tool cannot directly be compared to one estimated with another.

The set of Type 1 protocols for Risk Assessment and Risk Reduction have been inserted into our consensus standards with “Shall” language demanding their adoption. They have never been formulated as a hypothesis with their veracity challenged in the tradition of the scientific method. A quantitative estimate of the probability of occurrence of harm has never been made on the basis of accurate and reliable data. The traditional methods of presenting approximate methodology with error estimates has been abandoned. More emphasis has been placed on the notion that the protocols provide a systematic methodology as opposed to their failure to deliver accuracy, consistency, and uniqueness. The Type 1 protocols represent art forms and rules of thumb that may or may not have value in the pursuit of safety. What is unequivocal is the fact that they do not contribute in any way to the foundations of safety theory. Indeed, they expose the soft underbelly of a wannabe profession.

Type 2 protocols differ from Type 1 protocols by their addition of a single invaluable contribution, Validation. Untapped data on Risk abounds in the manifold institutions of this country. The collection of accident data is a preoccupation of insurance companies, Workmen’s Compensation boards, government agencies, charitable organizations, medical institutions and the like. If this data were organized and marshaled into accessible formats, Risk Analysis would present a formidable database to the safety profession. In the meantime, proper Validation will circumvent the shortcomings of the Risk Assessment and Risk Reduction methodologies. The automotive companies and the medical device manufacturers have embraced validation as a way of life.

The capability of treating critical mishaps is a major distinction of Type 3 protocols. The catastrophic hazards treated by Type 1 and Type 2 methodologies are limited to the deaths of a handful of human lives. Critical mishaps involve casualties in the hundreds (plane crashes), thousands (explosions or toxic leakage at major installations), or millions (pandemics). A second feature of Type 3 protocols is heightened discipline. For example, the building block Risk Acceptance Criteria requires oversight by independent outside agencies as opposed to internal or in-house committee review. Furthermore, every subsystem is identified and managed by appropriate experts. They are then incorporated into the overall system by a sophisticated management group. Finally, Validation is infused into every identifiable hazards with testing, research, and historical review of documented experience.

For critical mishaps, the tolerable risk level is set so low that Risk Matrices are too crude to be meaningful. Flight tests and monitoring that sometimes never terminates, seaworthiness and military readiness exercises, and billion-dollar medical protocols are commonplace in Type 3 programs. Yet, in spite of the best efforts of engineering and science, oil spills and extraction mishaps occur, fleets of new aircraft are retired, missiles and aerospace disappointments are logged, and fertilizer explosions revisit our warehouses.

Type 3 protocols attempt to control the proclivities of humankind with its mis-information thresholds, politics, greed, conspiracy theories, and miscreant behavior including sabotage and hacking. Further, these protocols are charged with the taming of mother nature with her four faces,

- She is smarter than we are.
- She is more powerful than we are.
- She is meaner that we are.
- She has a sense of humor.

Fortunately, society has not looked to safety engineering for protection against critical mishaps; indeed, they have appealed to science and the founding engineering disciplines who are influenced by their code of ethics,

*First Canon of Ethics: “Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties.”*

# References


[1] Barnett, Ralph L., “On the Safety Theorem,” American Journal of Mechanical Engineers, Vol. 8 No. 2., pp. 50-53, March 2020.

[2] Barnett, Ralph L., “Safety Definitions: Colloquial, Standards, Regulatory, Torts, Heuristic, and Quantitative ,” American Journal of Mechanical Engineering, Vol. 8 No. 2, pp. 54-60, July, 2020.

[3] MIL-STD-882E, “Department of Defense - Standard Practice Safety System,” 2012. www.quickseawrch.dla.mil.

[4] ISO/IEC Guide 51: 2014(E), “Safety Aspects - Guidelines for Their Inclusion in Standards,” 2014. www.iso.org.

[5] Barnett, Ralph L., “On the Safety Hierarchy or Hierarchy of Control ,” American Journal of Mechanical Engineering, Vol. 8 No. 2, pp. 61-68, July, 2020.

[6] ANSI B11.TR3-2000, “ANSI Technical Report, Risk Assessment and Risk Reduction - A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools,” American National Standards Institute, 2000. www.ansi.org.

[7] Christiansen, Wayne and Fred A. Manuele, “Safety Through Design,” National Safety Council, 1999.

[8] ANSI/AIHA Z10-2005, “American National Standard for Occupational Health and Safety Management Systems,” American National Standards Institute, 2005. www.ansi.org.

[9] ANSI/RIA R15.06-1999, “American National Standard for Industrial Robotics and Robot Systems - Safety Requirements,” American National Standards Institute, 1999. www.ansi.org.

[10] Hagan, Phillip E., John F. Montgomery and James T. O’Reilly, “Accident Prevention Manual for Business and Industry, Engineering & Technology, National Safety Council, 2009.

[11] MIL-STD-882D, “Department of Defense - Standard Practice Safety System,” 2000. www.quicksearch.dla.mil.

[12] ANSI B11.3-2002, “Safety Requirements for Power Press Brakes,” American National Standards Institute, 2002. www.ansi.org.

[13] ANSI B11.1-2001, “Safety Requirement for Mechanical Power Presses,” American National Standard for Machine Tools, 2001. www.ansi.org.

[14] ISO 14121-1: 2007(E), “Safety of Machinery - Risk Assessment - Part 1: Principles,”, 2007. www.iso.org.

[15] ISO/TR 14121-2: 2007, “Safety of Machinery - Risk Assessment - Part 2: Practical Guidance and Examples of Methods,” 2007, www.iso.org.

[16] ANSI B11.0-2020, “Safety of Machinery,” American National Standards Institute, 2020. www.ansi.org.

[17] ANSI B11.2-2013, “Safety Requirements for Hydraulic and Pneumatic Power Presses,” American National Standards Institute, 2013. www.ansi.org.

[18] Brauer, Roger L., “Safety and Health for Engineers,” John Wiley & Sons, 1999.

[19] Manuele, Fred A., “On the Practice of Safety, 3rd ed.” John Wiley & Sons, 2003.

[20] Gloss, David S and Miriam Gayle Wardle, “Introduction to Safety Engineering,” John Wiley & Sons, 1984.

[21] US Army Combat Capabilities Development Command, “Army Military Airworthiness Certification Criteria (AMACC), 2019.

[22] CoVan, James, “Safety Engineering,” John Wiley & Sons, 1995.

[23] NASA-STD-8719.7, “Facility System Safety Guidebook,” NASA Technical Standard, January 30, 1998.

[24] Barnett, Ralph L., “Reasonably Foreseeable Use,” Safety Engineering and Risk Analysis, SERA - Vol. 8, American Society of Mechanical Engineers International Mechanical Engineering Congress, New York, NY, November 1998.

[25] Barnett, R.L. and W.G. Switalski, “Principles of Human Safety,” ASAE 87-5513, American Society of Agricultural Engineers International Winter Meeting, Chicago, IL, December 17, 1987, 39 pages.