Society for Risk Analysis Glossary

Approved June 22, 2015

Committee members:

Terje Aven (leader)
Yakov Ben-Haim
Henning Boje Andersen
Tony Cox
.Enrique López Droguett
Michael Greenberg
Seth Guikema
Wolfgang Kroeger
Ortwin Renn
Kimberly M. Thompson
Enrico Zio

The mandate for the committee as defined by the Council of the Society for Risk Analysis (SRA) is to: **prepare a suggestion for a new SRA glossary.**

Contents

2

June 22, 2015   Society for Risk Analysis Glossary

Preparing the glossary: rationale and process

Several attempts have been made to establish broadly accepted definitions of key terms related to concepts fundamental for the risk analysis field. Many scholars and institutions have devoted considerable time and effort to providing definitions and bringing some sort of unity and standardization to the field. The work has been based on the conviction that a scientific field or discipline must stand solidly on well-defined and universally understood terms and concepts.

Yet, experience has shown that to agree on **one** unified set of definitions is not realistic – the several attempts made earlier have not achieved success. The present work is founded on the idea that it is still possible to establish an authoritative glossary, the key being to allow for different perspectives on fundamental concepts and make a distinction between overall qualitative definitions and their associated measurements. For example, defining a probability cannot be meaningfully done without referring to different types of probability (subjective, frequentist, classical, …), but an overall qualitative definition such as "a measure for representing or expressing uncertainty, variation or beliefs, following the rules of probability calculus" could nonetheless be broadly accepted as useful.

Allowing for different perspectives does not mean that all definitions that can be found in the literature will be included in the glossary. The definitions included must meet some basic criteria - a rationale – such as being logical, well-defined, understandable, precise, etc. We will provide only definitions that are acknowledged by the committee – i.e., their meaning, rationale and justification will have to pass the scrutiny of its members.

Also, it is not the aim to present an all-inclusive glossary – only key generic concepts within the field of risk analysis are covered. This means that many terms specific of various application areas are not included. The committee hopes that the logic of the glossary can be useful also as a starting point for the development of these more specific terms.

Given the above, we claim that the present glossary is unique in its approach compared to existing risk analysis-related glossaries (including the ISO 31000 on risk management terminology), with its incorporation of different perspectives and its systematic separation between overall qualitative concepts and their measurements.

The target audience for the glossary is all individuals who have an interest in risk analysis, SRA members or not, ranging from risk analysis professionals and practitioners, to researchers, to students, to decision makers, to bureaucrats, to regulators, and to curious lay people who would like to get simple and practical explanations of key concepts in the field of risk analysis.

The glossary is planned to be updated from time to time to reflect the ongoing discussion, addressing comments and suggestions made. Please contact terje.aven@uis.no if you have some ideas.

The plan for the development of this glossary is defined by the following milestones:

  a) First discuss and agree within the committee on a structure for how to proceed – agreeing on the core set of terms to cover (June 13, 2014)
  b) A first draft of the definitions is produced (Sept. 1, 2014)
  c) Discussion and agreement on a draft glossary (Nov. 20, 2014)
  d) Presentation of a draft glossary at the SRA meeting in Denver and at the SRA council meeting there December 2014
  e) Sending the draft to SRA members and the Specialty Groups for comments (feedback before March 1, 2015)
  f) Committee conclusions for the glossary (May 1, 2015)
  g) SRA council approval (June 22, 2015)

The committee is grateful to the many professionals who have provided insightful and improving comments and suggestions to earlier versions of the glossary.

The glossary terms are divided into three categories:

1. **Terminology on basic concepts**
2. **Terminology on related concepts, methods, procedures**
3. **Terminology on risk management actions**

The terms are presented in alphabetical order except the first three: risk, uncertainty and probability.

1 Terminology of basic concepts

1.1 Risk

We consider a future activity [interpreted in a wide sense to also cover, for example, natural phenomena], for example the operation of a system, and define risk in relation to the consequences (effects, implications) of this activity with respect to something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences. There is always at least one outcome that is considered negative or undesirable.

Overall qualitative definitions:

    a) Risk is the possibility of an unfortunate occurrence
    b) Risk is the potential for realization of unwanted, negative consequences of an event
    c) Risk is exposure to a proposition (e.g., the occurrence of a loss) of which one is uncertain
    d) Risk is the consequences of the activity and associated uncertainties
    e) Risk is uncertainty about and severity of the consequences of an activity with respect to something that humans value
    f) Risk is the occurrences of some specified consequences of the activity and associated uncertainties
    g) Risk is the deviation from a reference value and associated uncertainties

ISO defines risk as the effect of uncertainty on objectives. It is possible to interpret this definition in different ways; one as a special case of those considered above (e.g., d) or g)), with the consequences seen in relation to the objectives.

Risk metrics/descriptions (examples):

    1. The combination of probability and magnitude/severity of consequences
    2. The combination of the probability of a hazard occurring and a vulnerability metric given the occurrence of the hazard
    3. The triplet (s_i, p_i, c_i), where s_i is the ith scenario, p_i is the probability of that scenario, and c_i is the consequence of the ith scenario, $i = 1, 2, \ldots N$.
    4. The triplet (C', Q, K), where C' is some specified consequences, Q a measure of uncertainty associated with C' (typically probability), and K the background knowledge that supports C' and Q (which includes a judgment of the strength of this knowledge)
    5. Expected consequences (damage, loss). For example, computed by:
        i. Expected number of fatalities in a period of one year (Potential Loss of Life, PLL) or the expected number of fatalities per 100 million hours of exposure (Fatal Accident Rate, FAR)
        ii. $P(hazard\ occurring)$

$$x\ P(exposure\ of\ object|\ hazard\ occurring)$$
$$x\ E[damage\ |\ hazard\ and\ exposure]$$

        i.e. the product of the probability of the hazard occurring and the probability that the relevant object is exposed given the hazard, and the expected damage given that the hazard occurs, and the object is exposed (the last term is a vulnerability metric, see Section 1.19)
        iii. Expected disutility
    6. A possibility distribution for the damage (for example a triangular possibility distribution)

The suitability of these metrics/descriptions depends on the situation. None of these examples can be viewed as risk itself, and the appropriateness of the metric/description can always be questioned. For example, the expected consequences can be informative for large populations and individual risk, but not otherwise.

1.2 Uncertainty

Overall qualitative definitions:

- For a person or a group of persons, not knowing the true value of a quantity or the future consequences of an activity
- Imperfect or incomplete information/knowledge about a hypothesis, a quantity, or the occurrence of an event

Uncertainty metrics/descriptions (examples):

- A subjective probability
- The pair (Q, K), where Q is a measure of uncertainty and K the background knowledge that supports Q
- A possibility distribution
- An info-gap model of the uncertainty

Epistemic uncertainty: as above for the overall qualitative definition of uncertainty and uncertainty metrics/descriptions (examples)

Aleatory (stochastic) uncertainty: variation of quantities in a population of units (commonly represented/described by a probability model)

1.3 Probability (likelihood, chance, frequency)

Overall definition:

A measure for representing or expressing uncertainty, variation or beliefs, following the rules of probability calculus

Different types/interpretations:

- Classical probability:

    The classical interpretation applies only in situations with a finite number of outcomes which are equally likely to occur: The probability of A is equal to the ratio between the number of outcomes resulting in A and the total number of outcomes, i.e.,

    $$P(A) = \frac{\text{Number of outcomes resulting in } A}{\text{Total number of outcomes}}$$

- Propensity/frequentist probability:

    A frequentist probability of an event A, denoted $P_f(A)$, is defined as the limiting fraction of times the event A occurs if the situation considered were repeated (hypothetically) an infinite number of times.

    The propensity interpretation holds that the probability is to be thought of as a physical characteristic; a propensity of a repeatable experimental set-up which produces outcomes with limiting relative frequency probability $P_f(A)$.

- Subjective (judgmental, knowledge-based) probability:

    a) *Reference to an uncertainty standard*: The probability $P(A)$ is the number such that the uncertainty about (degree of belief in) the occurrence of A is considered equivalent by the person assigning the probability, to the uncertainty about (degree of belief in) some standard event, for example drawing at random a red ball from an urn that contains $P(A)$ x 100% red balls.

    b) *Betting and related type of interpretations*: The probability of an event A is the price at which the person assigning the probability is neutral between buying and selling a ticket that is worth one unit of payment if the event occurs, and worthless if not.

Frequentist probabilities are in general unknown and must be estimated.

Likelihood: The same as probability

Chance: In a broad sense the same as probability. In a technical Bayesian context, a chance is the limit of the frequency in an exchangeable, infinite Bernoulli series (the Bayesian equivalent of a frequentist probability).

Frequency:

a) Number of events per unit of measurement of the related physical dimension considered (most commonly time)
b) Expected number of such events

1.4 Ambiguity

The condition of admitting more than one meaning/interpretation

Risk management and governance context:

- Ambiguity: The property of being open to different interpretations of risk assessment input and results
- Interpretative ambiguity: The property of being open to different interpretations of specific risk assessment input and results
- Normative ambiguity: The property of being open to different concepts and views related to the values to be protected, the termination of thresholds or standards, and the priorities to be made

1.5 Complex/Complexity

- A system is complex if it is not possible to establish an accurate prediction model of the system based on knowing the specific functions and states of its individual components
- Complexity: A causal chain with many intervening variables and feed-back loops that do not allow the understanding or prediction of the system's behaviour on the basis of each component's behaviour

1.6 Exposure

Exposure of something:

- Being subject to a risk source/agent (for example, exposure of asbestos)

1.7 Event, Consequences

Event:

- The occurrence or change of a particular set of circumstances such as a system failure, an earthquake, an explosion or an outbreak of a pandemic
- A specified change of the states of the world/affairs

Consequences: The effects of the activity with respect to the values defined (such as human life and health, environment and economic assets), covering the totality of states, events, barriers and outcomes. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences.

7

1.8   Harm, Damage, Adverse consequences, Impacts, Severity

Harm: Physical or psychological injury or damage

Damage: Loss of something desirable

Adverse consequences: Unfavorable consequences

Impacts: The effects that the consequences have on specified values (such as human life and health, environment and economic assets)

Severity: The magnitude of the damage, harm, etc.

1.9   Hazard

A risk source where the potential consequences relate to harm. Hazards could, for example, be associated with energy (e.g., explosion, fire), material (toxic or eco-toxic), biota (pathogens) and information (panic communication).

1.10   Knowledge

Two types of knowledge: Know-how (skill) and know-that of propositional knowledge (justified beliefs)

Knowledge is gained through, for example, scientific methodology and peer-review, experience and testing

1.11   Model

A model of an object (e.g., activity, system) is a simplified representations of this object

A probability model is a special type of models, based on frequentist probabilities (often referred to as chances in a Bayesian context).

1.12   Opportunity

An element (action, sub-activity, component, system, event, etc.) which alone or in combination with other elements has the potential to give rise to some specified desirable consequences

1.13   Resilience

Overall qualitative definitions:

– Resilience is the ability of the system to sustain or restore its basic functionality following a risk source or an event (even unknown)
– Resilience is the sustainment of the system's operations and associated uncertainties, following a risk source or an event (even unknown)
– Resilience is the ability of a system to reduce the initial adverse effects (absorptive capability) of a disruptive event (stressor) and the time/speed and costs at which it is able to return to an appropriate functionality/equilibrium (adaptive and restorative capability)
– The disruptive events maybe shocking or creeping, endogenous or exogenous
– A resilient system is one which sustains functionality despite large info-gaps (info-gap: the disparity between what is known, and what needs to be known to ensure specified goals)

Resilience metrics/descriptions (examples):

- Probability that the system is able to sustain operation when exposed to some types of risk sources or events (which can be more or less accurately defined)
- Probability that a system can sustain its functionality in the face of high stress or (unexpected) disturbances
- Probability that a system can restore functionality to its pre-disaster level (or higher) within a specified time

A resilient system is a system for which the resilience is judged to be high (this is a value judgment).

1.14 Risk source or risk agent

Element (action, sub-activity, component, system, event, etc.) which alone or in combination with other elements has the potential to give rise to some specified consequences (typically undesirable consequences)

1.15 Robustness

- The antonym of vulnerability
- A system is robust to uncertainty if specified goals are achieved despite large info-gaps (info-gap: the disparity between what is known, and what needs to be known to ensure specified goals)

1.16 Safe, safety

Safe: Without unacceptable risk

Safety:

- Interpreted in the same way as safe (for example when saying that safety is achieved)
- The antonym of risk (the safety level is linked to the risk level; a high safety means a low risk and vice versa)

Sometimes limited to risk related to non-intentional events (including accidents and continuous exposures)

1.17 Security, secure

Secure: Without unacceptable risk when restricting the concept of risk to intentional acts by intelligent actors

Security:

- Interpreted in the same way as secure (for example when saying that security is achieved)
- The antonym of risk when restricting the concept of risk to intentional acts by intelligent actors (the security level is linked to the risk level; a high security level means a low risk and vice versa)

1.18 Threat

Risk source, commonly used in relation to security applications (but also in relation to other applications, for example the threat of an earthquake)

Threat in relation to an attack: A stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain or misery

1.19 Vulnerability

Overall qualitative definitions:

- − The degree to which a system is affected by a risk source or agent
- − The degree to which a system is able to withstand specific loads
- − Vulnerability is risk conditional on the occurrence of a risk source/agent. If, for example, risk is interpreted in line with Section 1.1e), vulnerability is uncertainty about and severity of the consequences, given the occurrence of a risk source

Vulnerability metrics/descriptions (examples):

As for risk, but conditional on the risk source or event (load)

- − Expected loss given a failure of a single component or multiple components
- − Expected number of fatalities given the occurrence of a specific event
- − Expected system loss under conditions of stress
- − The probability that the system capacity is not able to withstand a specific load (the capacity is less than the load)
- − A probability distribution for the loss given the occurrence of a risk source
- − $(C', Q, K \mid risk\ source)$ (i.e., a risk description given the occurrence of a risk source, see Section 1.1)

As for risk, the suitability of these metrics/descriptions depends on the situation

A vulnerable system is a system for which the vulnerability is judged to be high

2   Terminology on related concepts, methods, procedures

2.1   Concern assessment

Systematic process to comprehend and assess the nature of effects and changes to the socio-economic environment, express and evaluate these effects/changes and associated uncertainties

2.2   Model uncertainty

Uncertainty about the model error, i.e., about the difference between the model output and the true value being modeled

2.3   Precautionary principle

- − An ethical principle expressing that if the consequences of an activity could be serious and subject to scientific uncertainties, then precautionary measures should be taken, or the activity should not be carried out
- − A principle expressing that regularity actions may be taken in situations where potentially hazardous agents might induce harm to humans or the environment, even if conclusive evidence about the potential harmful effects is not (yet) available

2.4   Risk analysis

Systematic process to comprehend the nature of risk and to express the risk, with the available knowledge (1.10)

Risk analysis is often also understood in a broader way, in particular in the Society for Risk Analysis (SRA) community. Risk analysis is defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level.

2.5   Risk appetite

Amount and type of risk an organisation is willing to take on risky activities in pursuit of values or interests

2.6   Risk assessment

Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge

2.7   Risk aversion

Disliking or avoiding risk

Technical definition: Risk aversion means that the decision maker's certainty equivalent is less than the expected value, where the certainty equivalent is the amount of payoff (e.g., money or utility) that the decision maker has to receive to be indifferent between the payoff and the actual "gamble."

2.8 Risk awareness

– Having an understanding of the risk (the risk sources, the hazards, the potential consequences, etc.)

– Being vigilant/watchful in relation to the risk and its potential consequences

2.9 Risk characterization, risk description

A qualitative and/or quantitative picture of the risk; i.e., a structured statement of risk usually containing the elements: risk sources, causes, events, consequences, uncertainty representations/measurements (for example, probability distributions for different categories of consequences – casualties, environmental damage, economic loss, etc.) and the knowledge that the judgments are based on

2.10 Risk communication

Exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media, general public)

2.11 Risk evaluation

Process of comparing the result of risk analysis (see risk analysis (2.4)) against risk (and often benefit) criteria to determine the significance and acceptability of the risk

2.12 Risk framing (pre-assessment)

The initial assessment of a risk problem, clarifying issues and defining the scope of subsequent work

2.13 Risk governance

The application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.

Risk governance includes the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken.

2.14 Risk management

Activities to handle risk such as prevention, mitigation, adaptation or sharing

It often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk

2.15 Risk perception

A person's subjective judgement or appraisal of risk

2.16 Safety analysis

– Systematic process to comprehend the nature of the safety of a system and to express the safety level

12

- Systematic process to determine the degree of risk reduction that is sufficient to obtain a "safe system"

3 Terminology on risk management actions

3.1 Public participation

A principle or practice expressing that the public has a right to be involved in the decision-making process

3.2 Risk acceptance

An attitude expressing that the risk is judged acceptable by a particular individual or group

3.3 Risk avoidances

Process of actions to avoid risk, for example, not be involved in, or withdraw from, an activity in order not to be exposed to any risk source

3.4 Risk insurance

Type of insurance that is taken out against risk

3.5 Risk mitigation

Process of actions to reduce risk

3.6 Risk policy

A plan for action of how to manage risk

3.7 Risk prevention

Process of actions to avoid a risk source or to intercept the risk source pathway to the realization of damage with the effect that none of the targets are affected by the risk source

3.8 Risk reduction

Same as risk mitigation: process of actions to reduce risk

3.9 Risk regulation

Governmental interventions aimed at the protection and management of values subject to risk

3.10 Risk sharing or pooling

Form of risk treatment involving the agreed distribution of risk with other parties

3.11 Risk retention

Acceptance of the potential benefit or gain, or burden of loss, from the risk (no insurance or transfer of the risk)

3.12 Risk tolerance

An attitude expressing that the risk is judged tolerable

3.13 Risk trade-offs (risk-risk trade-offs)

The phenomenon that intervention aimed at reducing one risk can increase other risks or shift risk to another population or target

3.14 Risk transfer

Sharing with another party the benefit of gain, or burden of loss, from the risk

Passing a risk to another party

3.15 Risk treatment

Process of actions to modify risk

3.16 Stakeholder involvement (in risk governance)

The process by which organizations or groups of people who may be affected by a risk-related decision can influence the decisions or its implementation