Safety margins in deterministic safety analysis

A. Viktorov
Canadian Nuclear Safety Commission
alex.viktorov@cnsc-ccsn.gc.ca

Abstract

The concept of safety margins has acquired certain prominence in the attempts to demonstrate quantitatively the level of the nuclear power plant safety by means of deterministic analysis, especially when considering impacts from plant ageing and discovery issues. A number of international or industry publications exist that discuss various applications and interpretations of safety margins. The objective of this presentation is to bring together and examine in some detail, from the regulatory point of view, the safety margins that relate to deterministic safety analysis.

In this paper, definitions of various safety margins are presented and discussed along with the regulatory expectations for them. Interrelationships of analysis input and output parameters with corresponding limits are explored. It is shown that the overall safety margin is composed of several components each having different origins and potential uses; in particular, margins associated with analysis output parameters are contrasted with margins linked to the analysis input. While these are separate, it is possible to influence output margins through the analysis input, and analysis method.

Preserving safety margins is tantamount to maintaining safety. At the same time, efficiency of operation requires optimization of safety margins taking into account various technical and regulatory considerations. For this, basic definitions and rules for safety margins must be first established.

1. Introduction

The objective of this document is to bring together and discuss in some detail, from the regulatory point of view, the safety margins that relate to deterministic safety analysis.

The concept of safety margins has acquired certain prominence in the attempts to demonstrate the level of the nuclear power plant safety by means of deterministic analysis, especially when considering plant ageing and discovery issues. A number of international [1, 2] or industry publications [3,4] exist that discuss various applications and interpretations of safety margins.

The subject of application and interpretation of safety margins is one of central issues in at least two projects undertaken currently by the Canadian nuclear power industry. One of them [5, 6] involves re-examination of the acceptance criteria for the Large Break LOCA. In the second [7], an independent panel of experts will re-assess the reactor trip acceptance criteria for events such as Loss of Flow and Small Break LOCA. The latter activity is triggered by the fact that the safety margins have been decreasing as a consequence of aging of the HTS components, notably the pressure tube creep, to the extent that some of the analysis limits can no longer be met without corrective measures – through changes in either the plant design, or operating conditions, or analysis methods.

When dealing with the deterministic safety analysis margins, two groups of parameters and limits will be of interest:

- Analysis output parameters: - these are the parameters predicted by performing safety analysis of an accident[1]. In particular, the parameters associated with failure mechanisms of safety provisions, such as physical barriers, are of importance. Limits are set for these parameters to ensure that failures of physical barriers are precluded, should an accident occur.

- Analysis input parameters: especially those that a) affect significantly the first group of parameters and b) could be controlled by the plant operator[2]. Limits are also set to these parameters as a practical way of controlling the analysis output parameters.

The interrelationship of analysis input and output parameters with corresponding limits will be explored to some extent in this paper. Definition of various safety margins will be presented and discussed along with the regulatory expectations for them.

Figure 1 provides a schematic illustration of the analysis as a means of translating the input parameters, which determine the pre-accident plant state, into the output parameters characterizing the severity of an accident. It is important to keep in mind the following:

[1] The term “accident” here is used in a broad context and includes both anticipated operational occurrences (AOO) and design basis accidents (DBA).
[2] This type of parameters is usually called, interchangingly, “plant” or “operating” parameters.

- there are margins associated with analysis output parameters and margins linked to the analysis input, and these are separate
- it is possible to influence margins through the analysis input, the analysis method and the analysis output.

It is also important to realize that the application of the safety margin concept in deterministic safety analysis is similar but still different from use of safety factors in the design practice. More discussion on this point can be found below.

2. Limits for analysis output parameters

2.1 Analysis output parameters

Any accident involves a wide variety of phenomena with numerous parameters that either influence or characterize, to various degrees, accident outcomes. However, of primary interest are those output parameters that allow quantifying "severity" of the accident (for example, fuel sheath temperature, or containment pressure). The limits would need to be established only for this group of output parameters.

Basically, each physical barrier to the release of radioactivity should have identified limits for each mechanism[3] that could challenge its integrity. The following barriers, as a minimum, should be considered:

Barrier	Examples of damage mechanism	Examples of output parameters associated with a failure mechanism
Fuel	Melting	Temperature
	Fragmentation	Maximum enthalpy
Fuel sheath	Melting	Temperature
	Deformation	Strain
Primary heat transport system (PHTS)	Rupture	Pressure, temperature
	Loss of strength and deformation	Temperature, pressure
Containment	Cracking	Global pressure
	Cracking	Local loads

A physical barrier may have multiple components facing different challenges, in particular, the PHTS which may need different limits for the pressure tubes (with associated calandria tubes), end-fitting assemblies, various piping, steam generator tubes, pumps, etc. Additional barriers may need to be considered as well - for example, secondary side piping, the spent fuel bay, fuelling machines; in other words, protective barriers need to be identified for any system that may contain radioactive products. The number of limits identified in such a way may appear quite large; however the practice shows that only a small number of bounding limits need to be firmly established.

[3] There may be several failure mechanisms affecting the barrier integrity at the same time; these mechanisms may be independent or inter-related.

In many cases, the failure mechanism would have only one governing parameter (such as the temperature when considering melting of the fuel cladding); in some situations however, the failure mechanism may be complex and depend on several parameters (the pressure tube failure would depend both on its temperature and internal pressure).

While in most cases the limits are established for parameters directly associated with a failure mechanism (such as pressure inside containment), in some cases analysis limits may be established with a surrogate parameter which would be easier to predict (for example, hydrogen concentration instead of loads caused by hydrogen burns) but still offer a reliable way to restrict the severity of a challenge to a barrier.

Finally, a special and a very important group of analysis output parameters relates to the predicted public doses (individual or population, whole body, organ-specific, etc). While these analysis output parameters are not linked to any physical barriers, the overall logic in establishing limits and quantifying margins remains essentially the same.

2.2 Failure limit

A failure limit[4] demarcates the zone of essentially no failures from the zone where failures can occur with non-negligible likelihood. As already discussed, a failure limit should be established for each credible mechanism that could challenge integrity of a physical barrier in the analyzed events.

Some simple rules to observe could easily be proposed. Thus, a failure limit should:

- Be based on experimental data obtained under sufficiently representative conditions
- Be set close to the values indicating non-failed state (rather than close to data for failed states) especially where the experimental data are limited,
- Account for measurement uncertainties and data scatter.

Here are some cases to illustrate the above.

Case 1. Figure 2a - ample experimental data (for both failed and un-failed outcomes) are available in the output parameter range of interest. Delineation between failed and un-failed states is clear to allow deriving a definitive failure limit.

Case 2. Figure 2b – only limited data exist (what is available does not allow accurate pinpointing the failure threshold). The failure limit is set close to the data indicating the non-failed state. The actual, real failure limit might be different - for example, corresponding to the dashed line on Figure 2b - but the available data would not allow justifying anything other than the line close to the non-failed data.

2.3 Analysis limit

[4] In some publications (e.g., [1]) this limit is called “safety” limit. Referring to this value as the “failure” limit seems preferable as it clearly indicates its essence – this is where a failure can be expected, based on available experimental evidence.

A **failure margin (1)**[5] separates the "failure limit" from an "analysis limit". Such a margin is needed to account for the following considerations:

- data derived from experimental conditions which are not typical for reactor operating conditions (i.e., temperature, pressure, flux, burn-up, etc)
- data derived from an experimental set-up differing from the reactor geometry (i.e., scaling distortions)
- effects from ageing or from differences in manufacturing of the plant components and of the experimental components
- provision for incomplete knowledge (unknown unknowns).

These aspects, inevitably present to some extent in any experiment, cannot be quantified and the failure margin is by necessity based on engineering judgement.

The analysis limit is a further abstraction of the reality (as can be seen from the illustrations on Figures 3a and 3b) - it would normally be set at a distance from the experimental data corresponding to failures. This is done, of course, deliberately to ensure that the physical barrier in question will not fail with high confidence even when all variables, including those we cannot quantify, (accident conditions, degree of degradation, manufacturing variances, etc) stack in the unfavourable direction.

The analysis limit is also known as the **acceptance criterion** because meeting this limit in safety analysis (in conjunction with satisfying other relevant requirements) would signify that the plant is safe.

The analysis limit (acceptance criterion) should be, in principle, set by the regulator (or another appropriate organization, for example the CSA); if there is no prescribed analysis limit, then the plant designer or licensee[6] should identify analysis limits for each barrier.

Depending on the importance of a SSC failure, the analysis limit may be indicated either as a **requirement** or an **expectation**. **Requirements** would have the appropriate legal basis (for example through incorporation into regulatory documents referenced in the licence) and permit no exceptions. **Expectations**, on the other hand, could allow certain flexibility, with exceptions justified in each case.

When the **analysis limit** incorporates adequate margin (the analysis limit set sufficiently far from the failure limit), **only then the analysis predictions could be at the analysis limit and an adequate safety would still be assured**.

Historically, some of the current analysis limits (or acceptance criteria) have been set at, or very close to, the failure limit; in this case the analysis prediction at the analysis limit is in fact very close to the failure threshold and would not be acceptable. This situation (safety and failure limits coinciding) should be avoided.

[5] See Table 1 in Summary section for definition of all margins.

[6] In the current Canadian practice, it is the designer or licensees who most often identify this type of a limit.

Frequently, there is only one value for the analysis limit – for example, maximum fuel sheath temperature, regardless of any variances in the conditions of a given accident scenario (Fig. 3b). Sometimes, however, the analysis limit is a function of one or several key governing parameters (Fig. 3a). This may be justified when there is strong experimental evidence to support the functional dependence of the failure limit and, by implication, of the analysis limit on the key governing variables.

2.4 Licensing analysis prediction

It is the extreme (maximum or minimum, whichever may be more challenging for the barrier integrity) analysis output parameter value that is used for comparing against the analysis limit. In most cases the parameter value would go down again after reaching its maximum (temperatures, pressures, etc) but occasionally it could be "frozen" at its maximum (for example, the fuel cladding oxidation or piping inelastic strain).

The difference between the analysis output parameter and the corresponding analysis limit (acceptance criterion) is another margin which we will call a calculated **analysis margin (2)** to distinguish from the margin described in Section 2.3 above. The reactor safety system trip set-points are established to make sure that these systems are effective in maintaining adequate analysis margins in case of an accident

The prediction of the safety analysis in support of initial operating licence in essence becomes a “target” to be preserved in subsequent re-analyses. The analysis margin originally accepted when issuing the licence could be decreased without breaking the analysis limit (in other words, be in conformance with regulatory requirements). Nevertheless, this would effectively amount to a decrease in the demonstrated safety and thus should be avoided where practicable (for example, through compensatory changes in design or operation).

Figure 4 illustrates various limits and margins discussed in Sections 2.1 - 2.4.

3. Limits for analysis input parameters

As it was said right at the beginning, the second category of the parameters that will be considered in this discussion is the analysis input parameters – namely, those that significantly influence the parameters characterising challenges to physical barriers.

The nuclear power plant operator may not have much influence over the accident outcomes, for example, simply because the accident progression would be too rapid to expect operator intervention before engineering system act automatically. On top of that, in the deterministic safety analysis the operator action simply cannot be credited before certain time. In fact, the largest influence that the operator exerts over an accident is through the control of plant operating parameters - such as a reactor power, neutron flux, pressures, temperatures, etc. - prior to an accident.

Multiple input parameters influence the same output parameter, for example, the fuel energy deposition following a LBLOCA is largely determined by a number of operating parameters, such as the initial reactor power, neutron flux distribution, moderator and coolant isotopic purity,

neutron poison concentration, as well as the speed of SDS action. It becomes the responsibility of a designer/licensee to identify the important operating parameters for each accident scenario considered in the safety analysis as the analysis input.

Hence, limiting of the output parameter of interest can be achieved by imposing appropriate limits on a host of input parameters (representing the initial operating conditions). Same effect may be achieved by different combinations of limits. The licensee is expected to identify such a set of limits for the operating parameters that would be optimal from the operational point of view while providing the desired analysis results.

The extreme values of the operating parameters used in the "conservative"[7] safety analysis will be called in this paper the "**safety analysis limit**" for the analysis input parameters. However, the operating parameters (analysis inputs) should not be allowed to reach such "safety analysis limits" in operation. The "operating limits" need to be established to account for the instrumentation uncertainty in indication of operating parameter values to the plant operator. Thus, the "operating limits" are the extreme values that can be observed in operation without reaching, with high confidence, the analysis limit for the analysis input parameters when accounting for uncertainties associated with the plant instrumentation. The difference between the operating limit and the safety analysis limit can be called the **instrumentation uncertainty margin (3)**.

Usually, the licensee would also have an **action limit** to alert of the parameter approaching the operating limit so that an action could be taken before the parameter reaches the operating limit. This would lead to the **action margin (4)**.

Finally, the actual value of an operating parameter would fluctuate within a certain range defined by the balance of plant operability considerations and the need to maintain comfortable margins (to avoid the need to corrective interventions). The distance to the action limit is the **operating margin (5)** – see Figure 5 for illustration of limits and margins associated with the analysis input.

The conservative method of performing the deterministic analysis assumes input operating parameters set at their safety analysis limits, thus incorporating all the above margins (3-5) at the onset of analysis. On the other hand, the best estimate plus uncertainty approach would use the actually observed values of operational parameters and account for various uncertainties through application of statistical techniques. Because in the latter case margins (3-5) are not included in the analysis, the calculated analysis margins (2) predicted by the best estimate methods are expected to be larger than margins for the same analysis output parameters predicted using a conservative approach.

The three margins associated with the analysis input form an essential element of the analysis conservatism.

4. Impact of Discovery Issues on Safety Margins

A discovery issue that is important from the deterministic analysis viewpoint could be a realization that:

[7] Such as the Limit of Operating Envelope (LOE) safety analysis methodology.

- a new phenomenon need to be included in the analysis (example – fuel string relocation in reactors fuelled against flow and the associated positive reactivity insertion in case of an upstream LOCA), or
- a phenomenon that is already included in the accident model, had previously been underestimated (example – underestimation of the void reactivity prediction by the older suite of physics codes).

The immediate effect would be reduction of the analysis margin (see Figure 4). It is probably worth mentioning that at this point there is no impact on the actual plant safety because no changes have occurred to the plant design or operating conditions. It is only the **"demonstrated by analysis"** safety that has been altered because of changes in relevant knowledge.

There are three principal ways to correct the effects of a discovery issue on the safety analysis results (and, thus, on the analysis margin):

a) Implementing operational restrictions by bringing down the safety and action limits for operating parameters (analysis input values for key operating parameters) and thus reducing margins associated with the analysis input (see Figure 5). The actual plant safety would be improved, but the demonstrated by analysis safety may improve, stay the same as before the discovery issue, or be worse (in other words, the analysis margin could be increased, unchanged or reduced) – depending on the impact of changes in the operating parameters on the analysis results. Operational flexibility would be negatively affected.

b) Changing plant design. Potential impacts of this option on the actual and demonstrated safety are the same as with option a) above, depending on the design change. Analysis limits and margins associated with the modified systems would need to be established anew.

c) Modifying the analysis method by reducing conservatism in assumptions or refining the models. In this case the analysis inputs for operating parameters (and the associated margins) may or may not change. The actual plant safety would not change as no material changes to the plant would have been made, but the calculated analysis margin would improve.

It is the licensee's responsibility to justify the selected approach to address impacts of a discovery issue on the safety margins.

5. Safety factors in design practice

A concept of a safety factor is widely used in design of systems, structures and components, most notably in the mechanical design. In that context, the safety factor could designate the ratio of the load leading to failure to the maximum load expected to be experienced by a component: safety factor = failure load / maximum load. Sometimes, the term "safety margin" is also used: safety margin = safety factor – 1.

It is easy to see that the concept of safety analysis margins is quite similar, but its use is extended to any parameter that could be a measure of safety challenge. This includes parameters that are

not direct measures of a challenge but also the parameters that serve as the input to safety analysis.

Summary

Tables 1 and 2 summarize definitions and some key points about limits and margins as discussed above. Table 3 captures some of the highlights of this paper.

Table 1. Limits

Limit	Definition
Failure limit	Separates the zone of essentially no failures of a physical barrier from the zone where failures can occur with non-negligible likelihood
Analysis limit for acceptance parameter (analysis output)	Incorporates a failure margin to account for effects not fully represented in experiments. This limit is the acceptance criterion in performing safety analysis
Analysis limit for operating parameter (analysis input)	The extreme value that an operating parameter may have, when it is indicated to the operator at the operating limit, taking into account instrumentation uncertainties
Operating limit	The allowable indicated value of an operating parameter before immediate corrective action need to be taken
Action limit	The operating parameter value when corrective action would need to be applied to avoid potential non-compliance with the operating limits

Table 2. Summary of safety margin definitions

	Margin	Definition	Regulator's role	Licensee's role	Availability for use
1	Failure margin	Difference* between the failure limit and the analysis limit for the analysis output parameter	Verifies/accepts failure limits. Establishes analysis limits.	Provides supporting data for failure limits. Establishes analysis limits if not already set by the regulator.	Cannot be used if analysis limit is a legal requirement. Otherwise the analysis limit should not be used other than in exceptional circumstances.
2	Analysis margin	Difference between the analysis limit for a given analysis output parameter and the calculated value of this parameter	Verifies/accepts analysis outputs.	Provides safety analysis outputs	Can be used by the licensee if justified.
3	Uncertainty margin	Difference between the safety analysis limit for an input parameter and the operating limit, i.e., the maximum value that this parameter may have during the plant operation without non-compliance with licensing or operating requirements	Verifies/accepts limits for operating parameters	Establishes analysis limits for operating parameters which are used as basis for safety analysis inputs	Can be used by the licensee if justified.

4	Action margin	Difference between the operating limit and the action limit, i.e. the value of the operating parameter when the operator would be required to undertake corrective actions		Establishes action limits using justified uncertainty allowances	Should not be used in routine operation - corrective actions should be undertaken within reasonable time
5	Operating margin	Difference between the action limit and the actual value of the operating parameter		Operates the plant below the action limits	Can be used by the operator in routine plat operation.

(*) Difference here means either difference in absolute physical units, say temperature in degrees C or K, or relative difference in % (as could be used for sheath strain).

Table 3. Highlights of the discussion on establishing safety margins

1	Each physical barrier should have a failure limit and an analysis limit for each mechanism (there may be several failure mechanisms) that could challenge its integrity.
2	The analysis limit (acceptance criterion) should be, in principle, set by the regulator (or another appropriate organization, for example the CSA); if there is no prescribed analysis limit, then the plant designer or licensee should identify analysis limits for each barrier/challenge.
3	Depending on the importance of an SSC failure, the analysis limit may be indicated either as a **requirement** or an **expectation**. Requirements should have the appropriate legal basis (for example through incorporation into regulatory documents referenced in the licence) and thus be enforceable. Expectations, on the other hand, could allow justified exceptions.
4	When the **analysis limit** incorporates adequate margin (the analysis limit set sufficiently far from the failure limit), **only then the analysis predictions could be at the analysis limit and an adequate safety would still be assured**.
5	The margin to the analysis limit as originally accepted for issuing the licence could be decreased without breaking the analysis limit (in other words, be in conformance with regulatory requirements) but this would be considered as decrease in safety and thus should be avoided to extent reasonable (for example through compensating by changes in design or operation).

References

1. Implications of Power Uprates on Safety Margins of Nuclear Power Plants, IAEA TECDOC Series No. 1418, 2004.
2. Task Group on Safety Margins Action Plan (SMAP) Safety Margins Action Plan - Final Report, NEA/CSNI/R(2007)9.
3. CSA N290.15 “Requirements for the safe operating envelope of nuclear power plants”, 2010, draft.
4. Principles and Guidelines for Deterministic Safety Analysis used in Licensing of Current CANDU Nuclear Power Plants in Canada, COG 09-9030, March 2010.
5. COG-JP-4290-V02 “CNSC-Industry Working Group on Positive Reactivity Feedback and Large Break LOCA Safety Margins”, December 2009.
6. COG –JP-09-4367-V01, ‘Large LOCA Analytical Solution – Project Execution Plan``, March 2010.
7. COG WP 20326, Fuel & Fuel Channel Integrity Independent Technical Panel Framework, November 28, 2010.

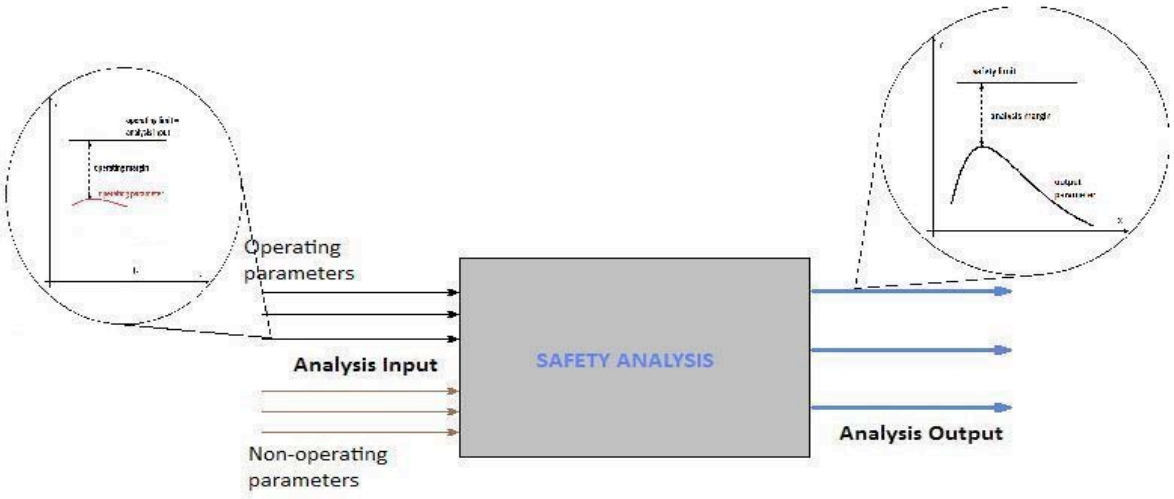
Operating parameters
Analysis Input
Non-operating parameters
SAFETY ANALYSIS
Analysis Output

Figure 1

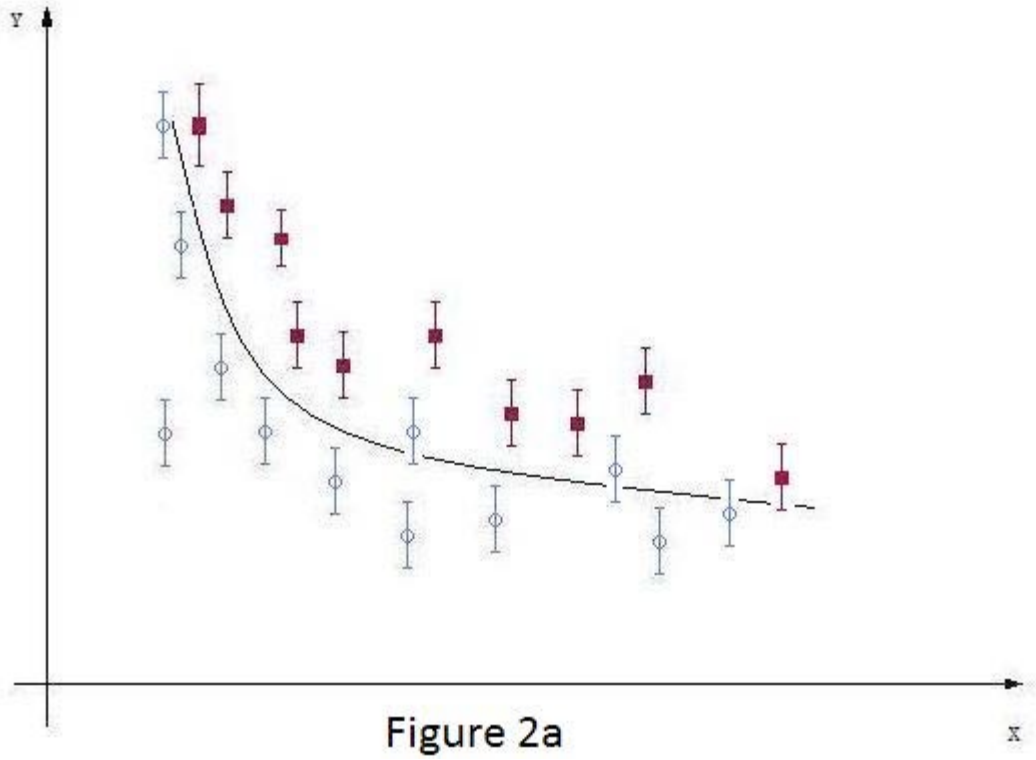

Figure 2a

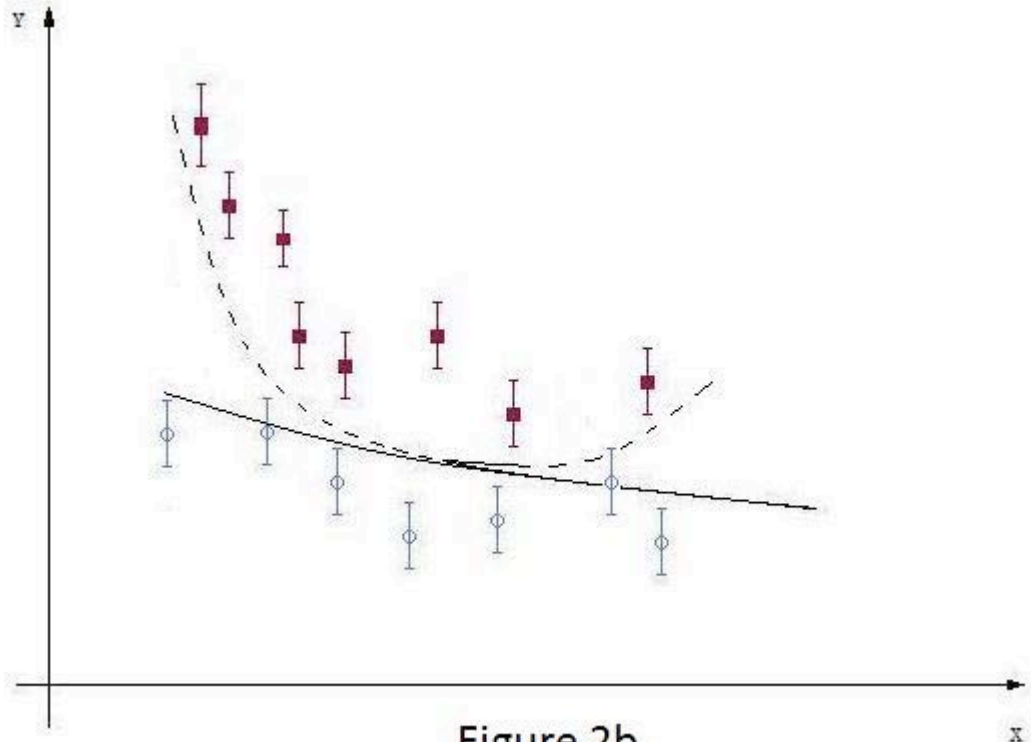

Figure 2b

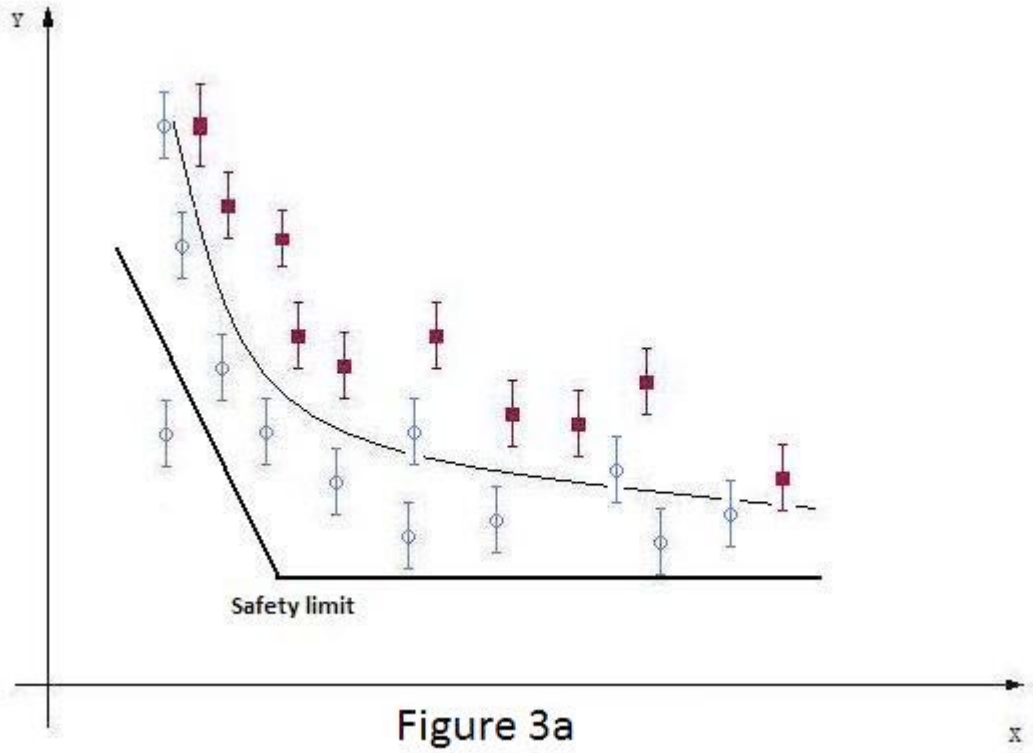

Figure 3a

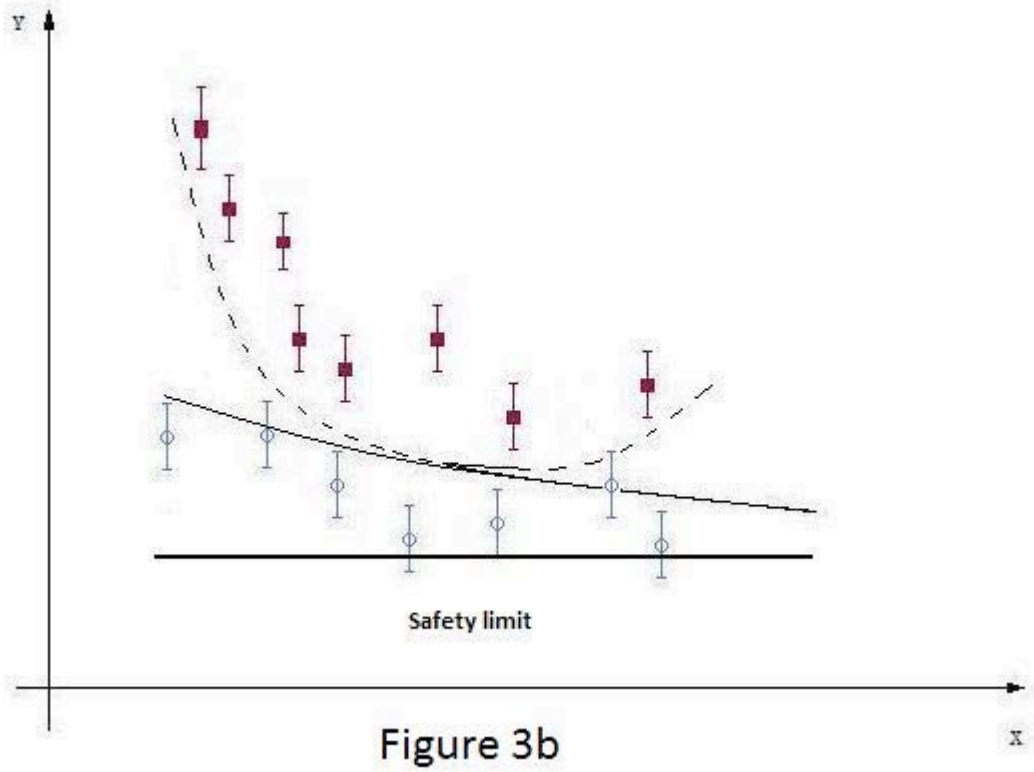

Figure 3b

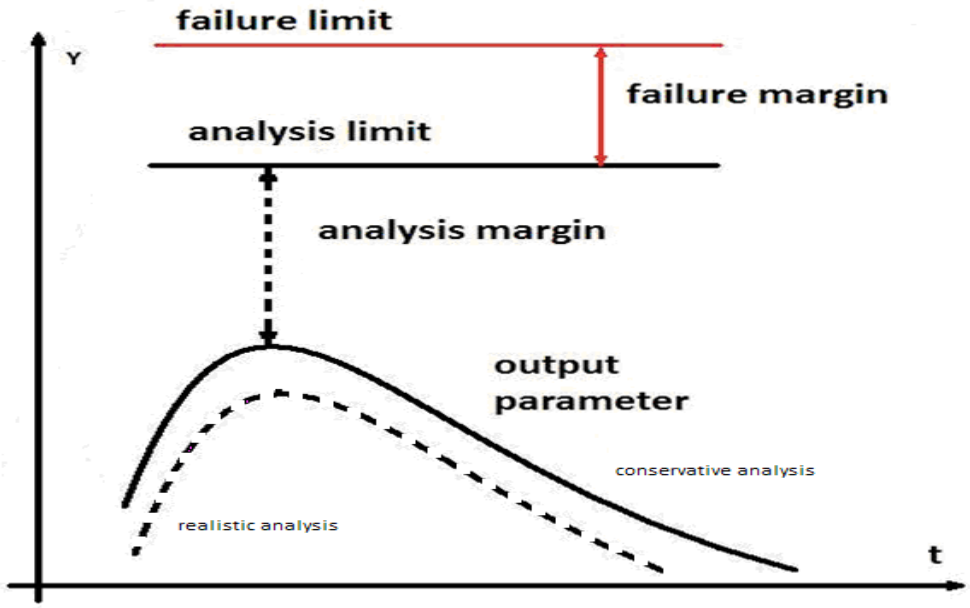

Figure 4

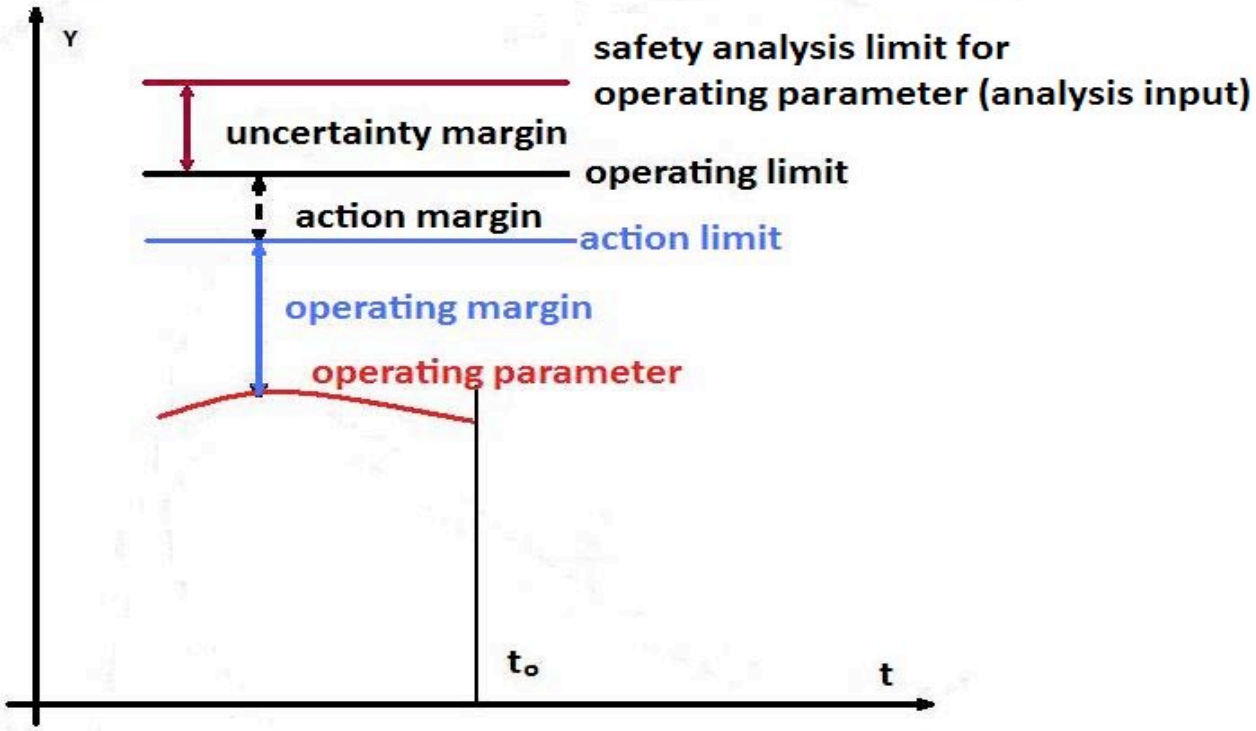

Figure 5