United States Nuclear Regulatory Commission

Setpoint Allowable Values for Instrument Channels in Safety-Related Service

Paul Rebstock, Hukam Garg, NRC/NRR/DE/EEIB-I&C

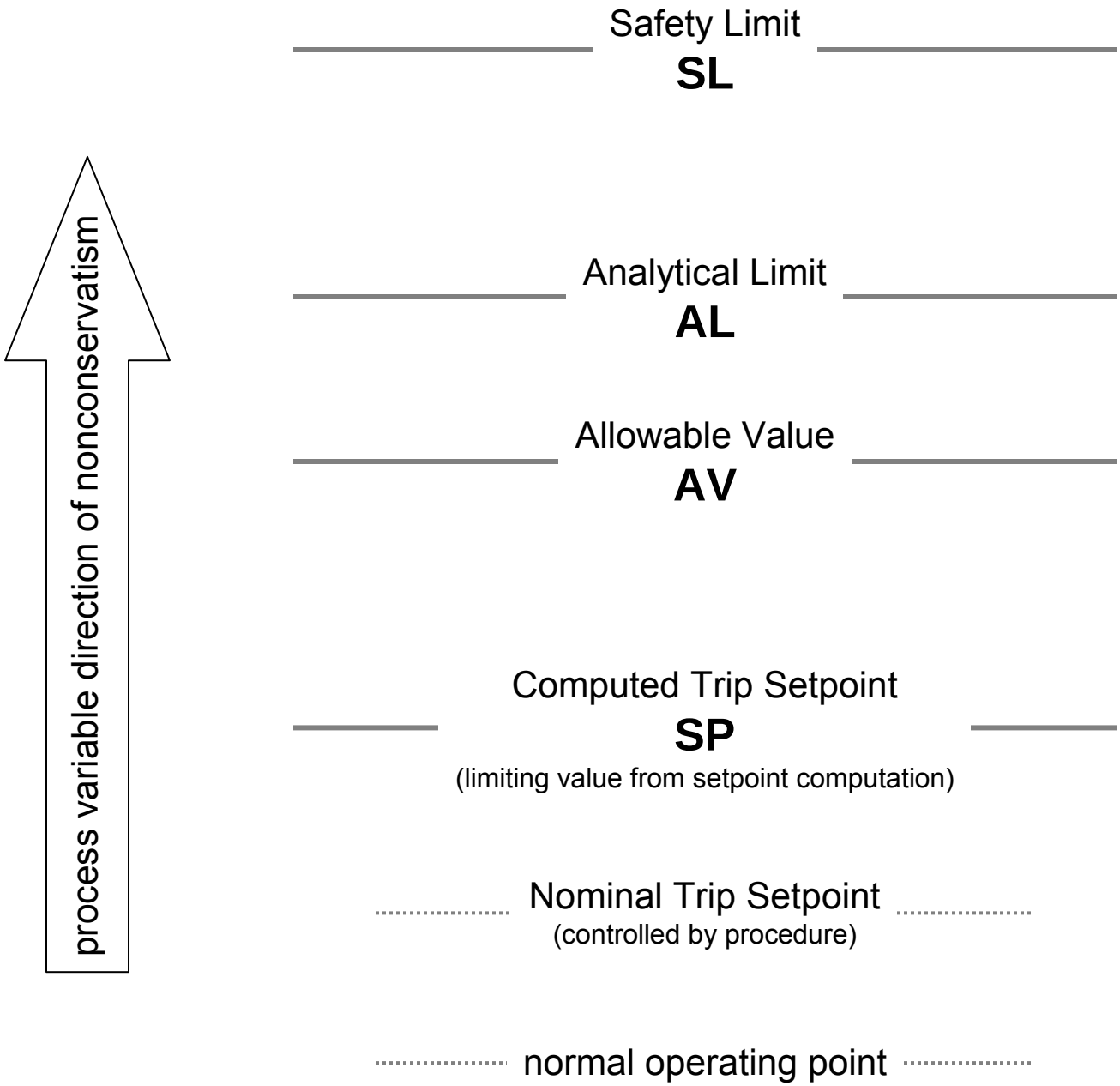
I&C section chief: Evangelos Marinos

Introduction

Everything stems from 10CFR50.36

- present and interpret salient points from 10CFR50.36
- discuss LSSS meaning, selection, and implications
- discuss testing in relation to 10CFR50.36
- discuss channel uncertainty & its impact upon selection of the LSSS
- discuss some non-intuitive effects and consequences

US NRC – Instrument Setpoints and Allowable Values



10CFR50.36

what it says and what it means

<u>LSSS</u> *(c):*

"... Technical specifications will include ... limiting safety system settings ..."

- ***LSSS must be presented in the TS***

10CFR50.36

what it says and what it means

<u>LSSS objective</u> *(c1iiA):*

"...Where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. ... "

- ***LSSS must protect SL***
- ***for most variables, connection to SL is complex and indirect***
- ***Safety analyses show that SL is protected if AL is met***
  - ***therefore AL serves as as surrogate for SL***
    - ***If AL is protected, then SL is protected.***
    - ***If AL is violated, then operation is in an unanalyzed condition and protection of the SL is not assured.***

10CFR50.36

what it says and what it means

operability requirement *(c1iiA):*

"... If, during operation, it is determined that the automatic safety system does not function as required, the licensee shall take appropriate action ... notify the Commission … review the matter … record results … including the cause of the condition and the basis for corrective action taken to preclude recurrence."

- ***take action if channel is found to be nonfunctional***
  - ***take corrective action to preclude recurrence***
- ***incorrect setpoint would prevent function per accident analysis***
  - ***therefore "incorrect setpoint" = "nonfunctional"***
  - ***failure to protect AL could mean failure to protect SL ... therefore nonfunctional***

10CFR50.36

what it says and what it means

surveillance requirement *(c3):*

"... requirements relating to test, calibration, or inspection to assure that ... facility operation will be within safety limits, and that the limiting conditions for operation will be met."

- ***protection of SL (in the guise of AL) must be demonstrated by surveillance testing***
- ***SL is protected by LSSS, therefore testing must demonstrate protection of LSSS***
- ***AsF beyond LSSS indicates potential violation of AL … and therefore of SL***

10CFR50.36

what it says and what it means

reporting requirement *(c8):*

"... submit written reports to the Commission ... for events described in paragraphs (c)(1) ... "

- ***LSSS violation must be reported & remedial action must be taken***

10CFR50.36

summary

- LSSS must be presented in the TS
- LSSS must protect SL by protecting AL
- nonfunctionality includes as-found setpoint that fails to protect AL
- testing must demonstrate protection of SL
  ... therefore of AL
  ... therefore of LSSS
- LSSS violation must be reported & remedial action must be taken

The Significance of the LSSS

- LSSS is a “setting” in that it is concerned with an adjustment
  - Specifically, it governs a setpoint
- LSSS is “limiting” in that it places a limit on the acceptable measured setpoint
  - it is not itself a setpoint
  - must provide adequate assurance that Actual Trip Point is always within AL despite anticipated uncertainty

The Significance of the LSSS

- guidance from RG1.105: should be AV, but alternatives may be proposed & defended
  - if allowable value:
    - must ensure protection of the process
    - will result in what may be incorrectly interpreted as false alarms (we will address this later)
  - some might prefer to use setpoint as LSSS:
    - must specify as limit and add margin to avoid violation at every COT
    - operating margin reduced
- violation of LSSS is undesirable
  - must ensure adequate margin between as-left setting and LSSS
  - AV provides this margin with less impact on operating margin than use of computed SP plus “extra” margin

Protecting the Safety Limit

- few safety limits, many setpoints
- setpoints map to safety limits through complex and indirect relationships
- plant safety analyses evaluate plant behavior relative to safety limits under the assumption that certain events will occur before certain process variables reach certain specified values (Analytical Limits)

Protecting the Safety Limit

- AL serves as surrogate for SL
  - Protection of AL ensures that SL are also protected.
  - Violation of an AL does not necessarily mean that the corresponding SL(s) <u>will</u> be violated, but rather that the plant will be in an unanalyzed condition and SL protection is not ensured.
    - » If it is shown that violation of the AL by some specific amount is tolerable, then, in effect, the AL has been adjusted.

The Role of Testing

confirm the present, protect the future

The Safety Limit, in the guise of its surrogate value, the Analytical Limit, must be shown to be protected:

- at the time of the test
  - AsF must ensure that Actual Trip Point is currently within AL
  - no need to consider drift or uncertainties that have already been resolved in the test
- from the end of the test until the start of the next test
  - AsL must ensure that Actual Trip Point will remain within AL throughout limiting test interval
  - all credible sources of error must be considered

The Role of Testing

Channel Operation Test (COT)

- purpose of COT: show that LCO is met (demonstrate operability)
- practical consideration: can't test everything
  - uncertainty subgroups: COT and nCOT
    - » every element of uncertainty for every instrument component either *is* addressed in the test or *is not* addressed in the test
    - » therefore COT and nCOT together encompass every element of uncertainty for every instrument component with no overlaps
- "as-found" limitation applies to COT per TS test schedule only

Uncertainty and Channel Testing

- "testing" includes adjusting the setpoint
- "uncertainty component:"
  a particular element of uncertainty for a particular device, such as:
  - drift for a bistable
  - temperature effect for a bistable
  - drift for a pressure transmitter
  - flow coefficient uncertainty for a flow measurement venturi

Uncertainty and Channel Testing

uncertainty subgroup "COT"

- composite of the uncertainty components that are addressed in the COT (includes only those devices which are included in the COT), for example:
  - drift over the entire limiting test interval
  - test instrument uncertainties
  - setting tolerances

...used mathematically to represent the statistical combination of all uncertainty components addressed in the COT

Uncertainty and Channel Testing

uncertainty subgroup "nCOT"

- composite of the uncertainty components that are *not* addressed in the COT, for example:
  - devices excluded from the test
  - effects of change in operating environment

...used mathematically to represent the statistical combination of all uncertainty components *not* addressed in the COT

Uncertainty and Channel Testing

- The uncertainty components in COT and in nCOT are generally mutually exclusive
  - all of the uncertainty components for a given instrument channel are in one group or the other
  - therefore the two groups are (nearly) orthogonal and together they make up the entire channel uncertainty.

It is possible that the components of COT and nCOT could be defined in such a manner that some elements might bridge between them and compromise independence.
This possibility, and the consequences of such nonindependence, will be addressed later in this presentation.
It will be shown that this nonindependence, even if significant, will not compromise this discussion.

Measured Setpoint
Actual Trippoint

- "setpoint" is the value of the process variable at which channel trip is measured or expected
  - setpoint is:
    - a specific number (deterministic)
    - a property of the channel
    - a measure of expected channel behavior

Measured Setpoint
Actual Trippoint

- "trippoint" is the *actual* value of the process variable at which the trip *does* occur
  - trippoint is:
    - a random variable
    - a physical realization of the setpoint property
    - a measure of how the channel actually does perform in response to a particular challenge
  - trippoint cannot be known exactly, since any measurement includes error
  - trippoint is imperfectly related to the measured setpoint

Measured Setpoint
Actual Trippoint

- the accident analyses presume a specific trippoint
  - actual point of actuation (trippoint)
  - not measured or target value (setpoint)

The limiting setpoint must be selected so as to give adequate confidence that the actual trippoint will be consistent with the accident analysis.

Measured Setpoint Actual Trippoint

- setpoint is “measured” by injecting a test signal, adjusting the test signal level until a trip is observed, and relating the observation to the corresponding process variable
  - the test signal is typically an analog of the process variable, related to it via the channel scaling function
    - channel scaling function typically includes devices not included in the COT (flow element, pressure transmitter, RTD, etc)
    - channel scaling function is known only with limited accuracy
  - signal generation / measurement equipment has limited accuracy

Measured Setpoint
Actual Trippoint

- "error" is the difference between measured setpoint and actual trippoint
  - error is a random variable with zero mean and with variance depending on loop uncertainty

The Math

The Paradigm

1. The objective is to evaluate a postulated AV.
   - setpoint is assumed to be at that postulated limiting acceptable value
   - need to show that ATP would be suitably constrained
2. ATP is normally distributed about SP.
   - standard deviation is proportional to uncertainty
3. The elements of COT and nCOT together encompass all elements of uncertainty for the channel, with no overlap
   - the union set {COT, nCOT} encompasses the entire population
   - the intersection of sets {COT} and {nCOT} is empty (or nearly so)
     - COT and nCOT are mutually exclusive (for all practical purposes)

95/95 Criterion

- few absolutes in statistics
- RG1.105 Regulatory Position #1:

  "... there is a 95% probability that the constructed limits contain 95% of the population of interest for the surveillance interval selected."

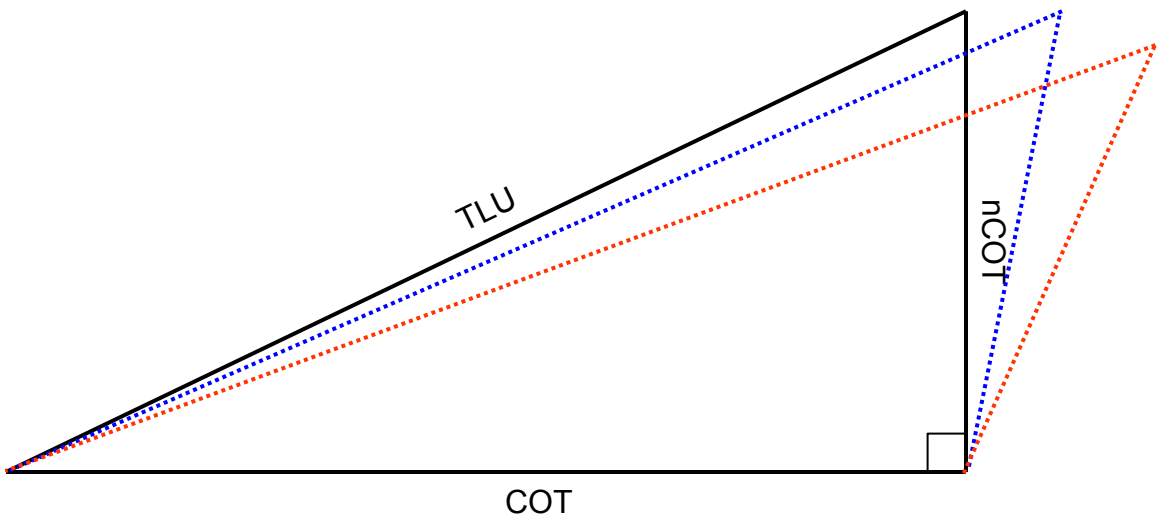
- RG1.105 accepts 95/95 as satisfying the requirements of 10CFR50.36

Total Loop Uncertainty

combining COT and nCOT

- Because COT and nCOT are taken as mutually exclusive, the net channel uncertainty is the SRSS of these two values:

TLU=SRSS(COT, nCOT)



Total Loop Uncertainty

relating COT and nCOT

- for the purposes of this discussion, define a parameter "α" (alpha) as the ratio of nCOT to COT:

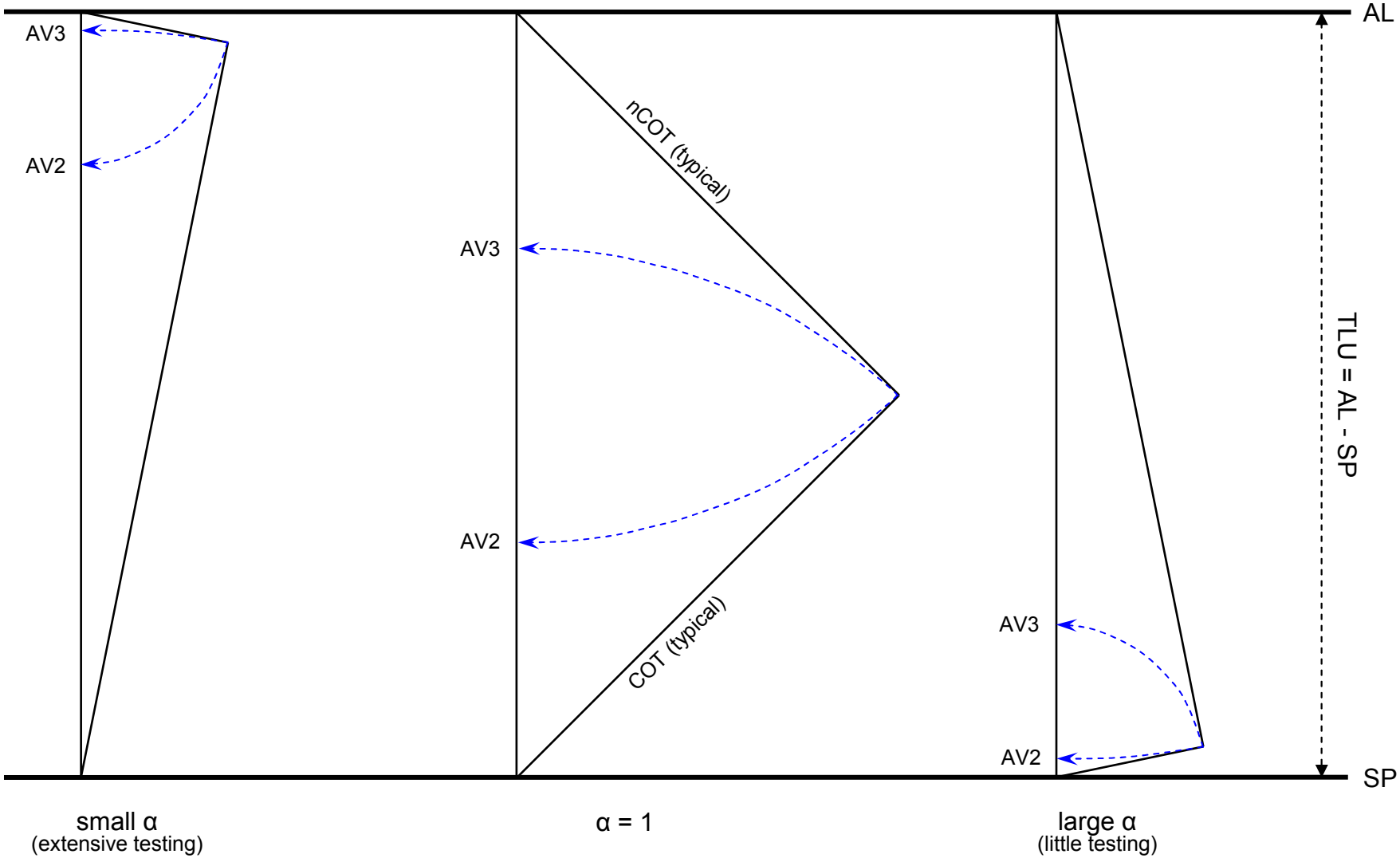
$$\alpha = nCOT / COT$$

... thus α is a measure of the "completeness" of the test
– if everything is included in the test,
then α = 0

US NRC – Instrument Setpoints and Allowable Values

AV2 = AL – nCOT

AV3 = SP + COT

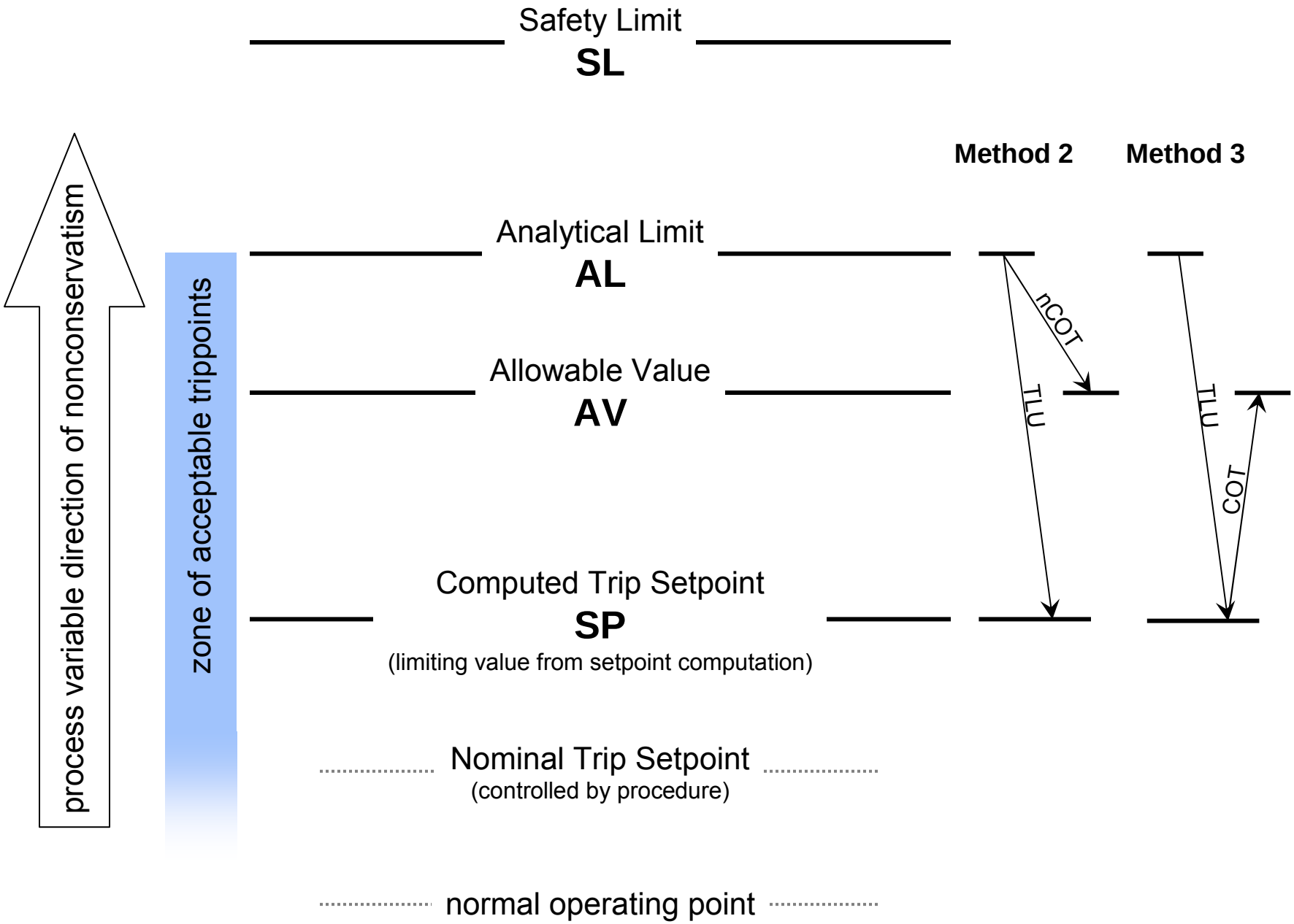


Allowable Value Computation
ISA RP67.04.02 Method 2 vs Method 3

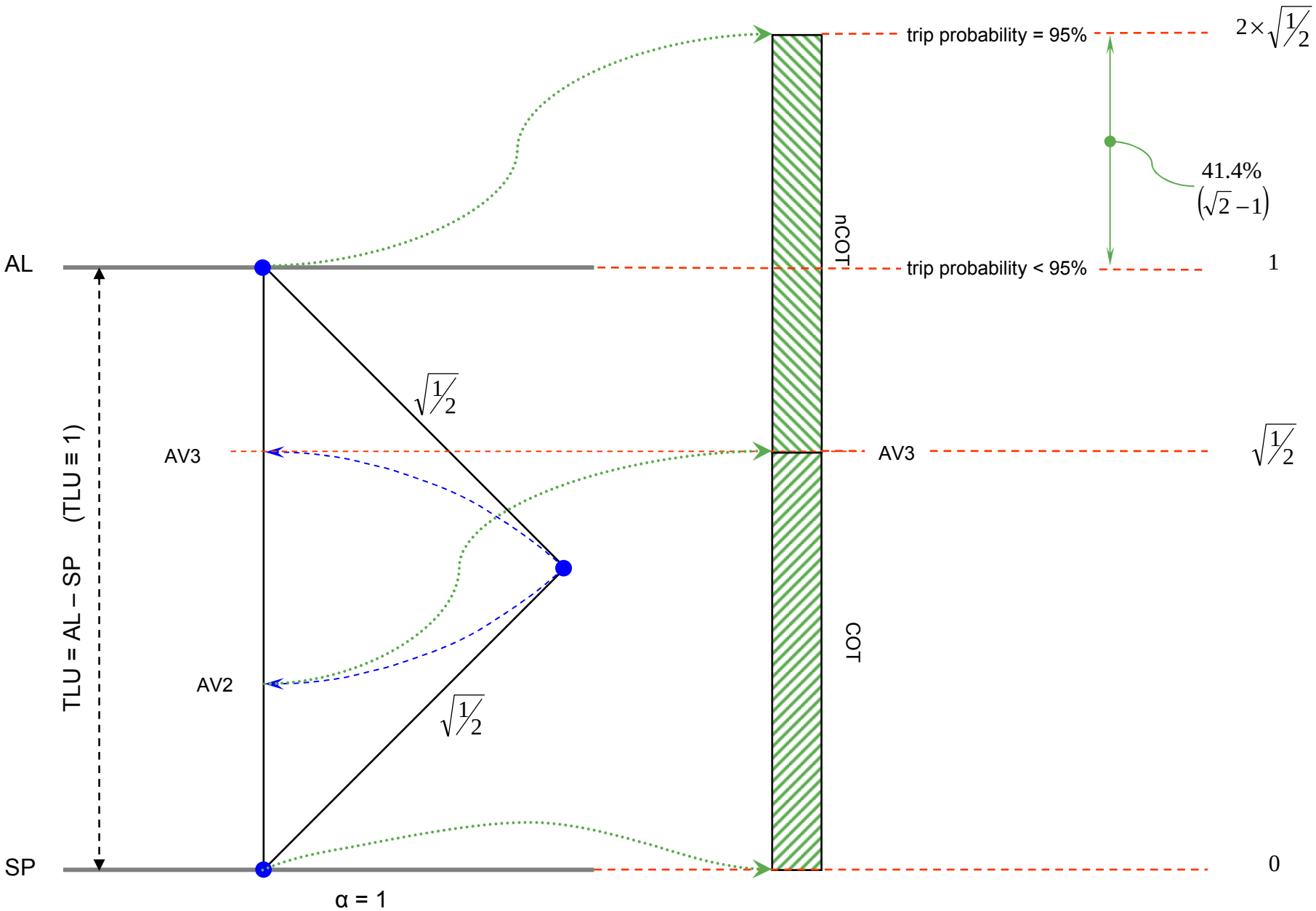
Notes:

1. All graphs assume that standard deviation is corrected to yield 95% probability of trip at TLU.
2. All graphs are normalized to unit TLU (i.e.: TLU=1 unit).
   - ✓ Therefore SP = AL-TLU = AL-1
   - ✓ Therefore AL = 1+SP
   - ✓ Setpoint is arbitrarily set to a large number of TLUs (presentation is relative to SP, so exact value of SP is not important)

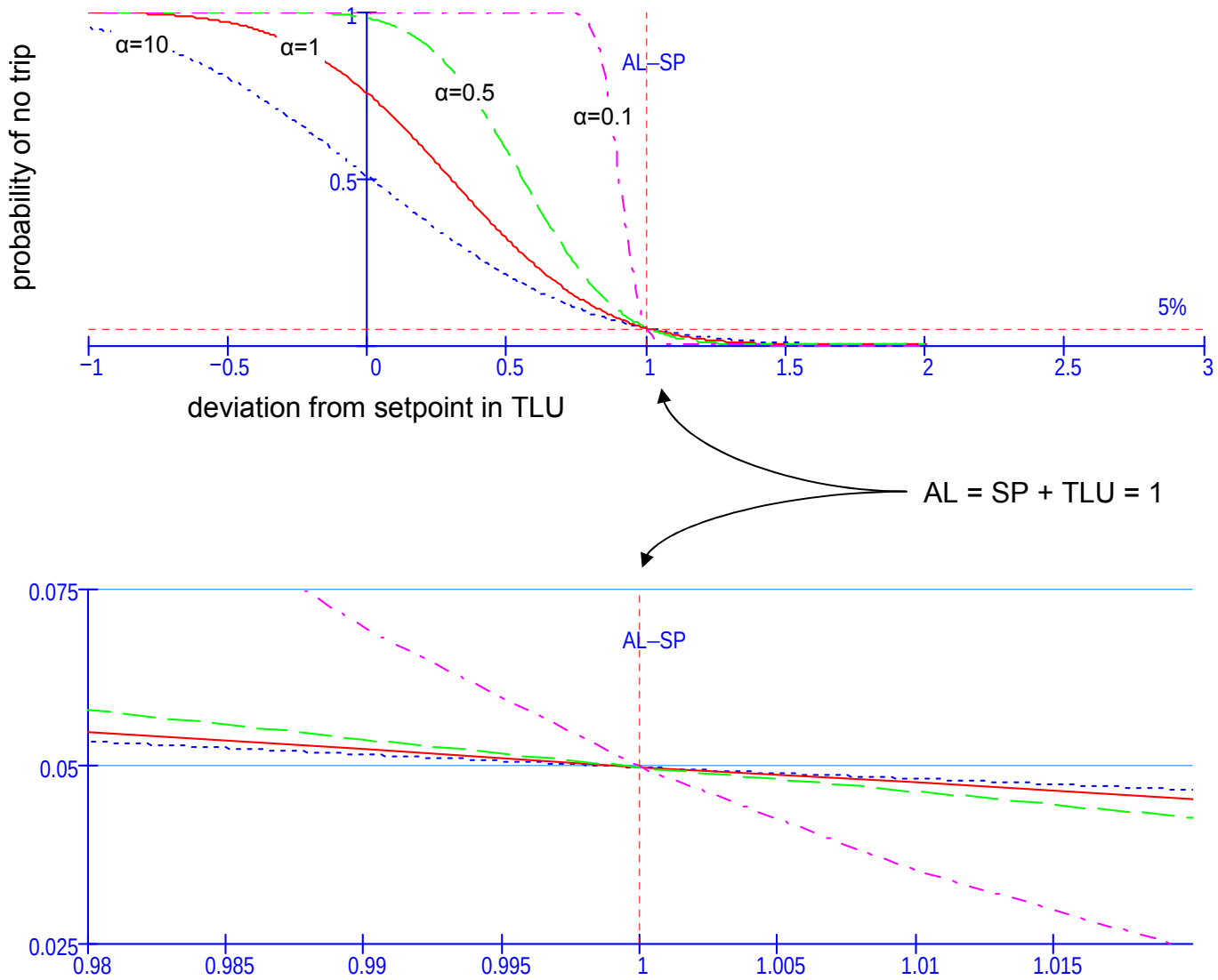
US NRC – Instrument Setpoints and Allowable Values



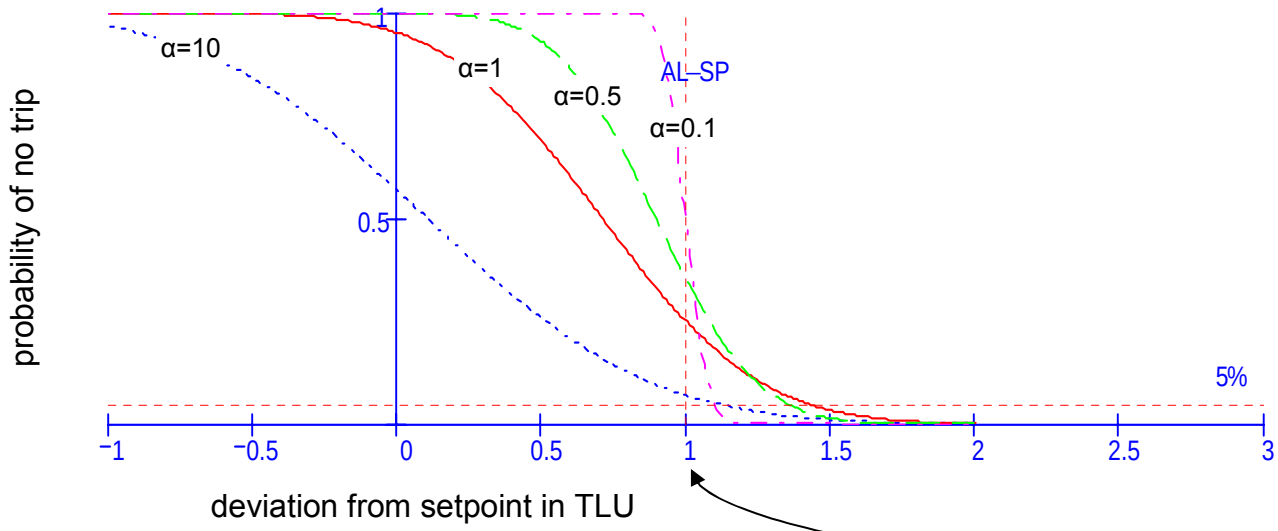
US NRC – Instrument Setpoints and Allowable Values



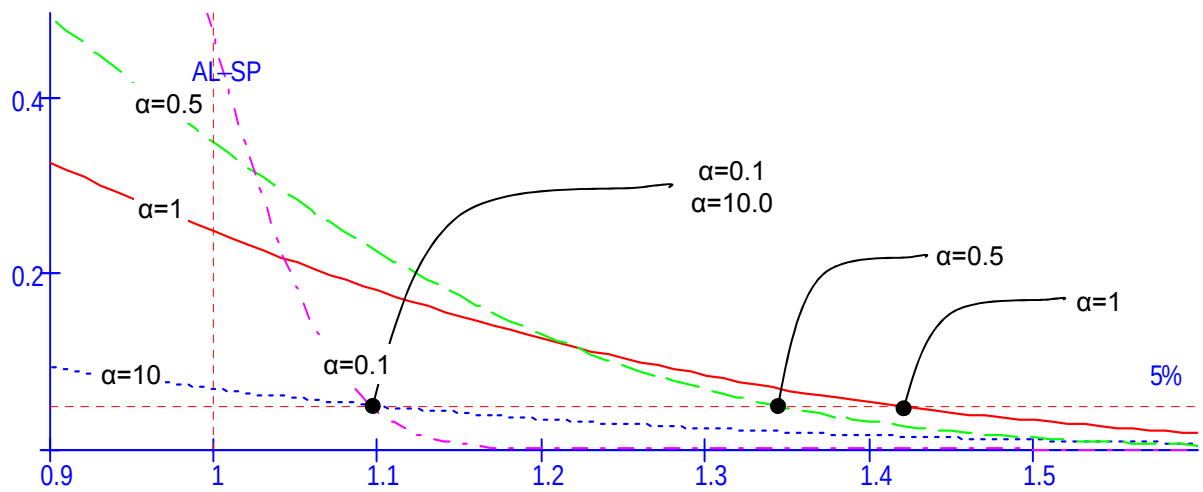
Method 2 NoTrip Probability



Method 3 NoTrip Probability

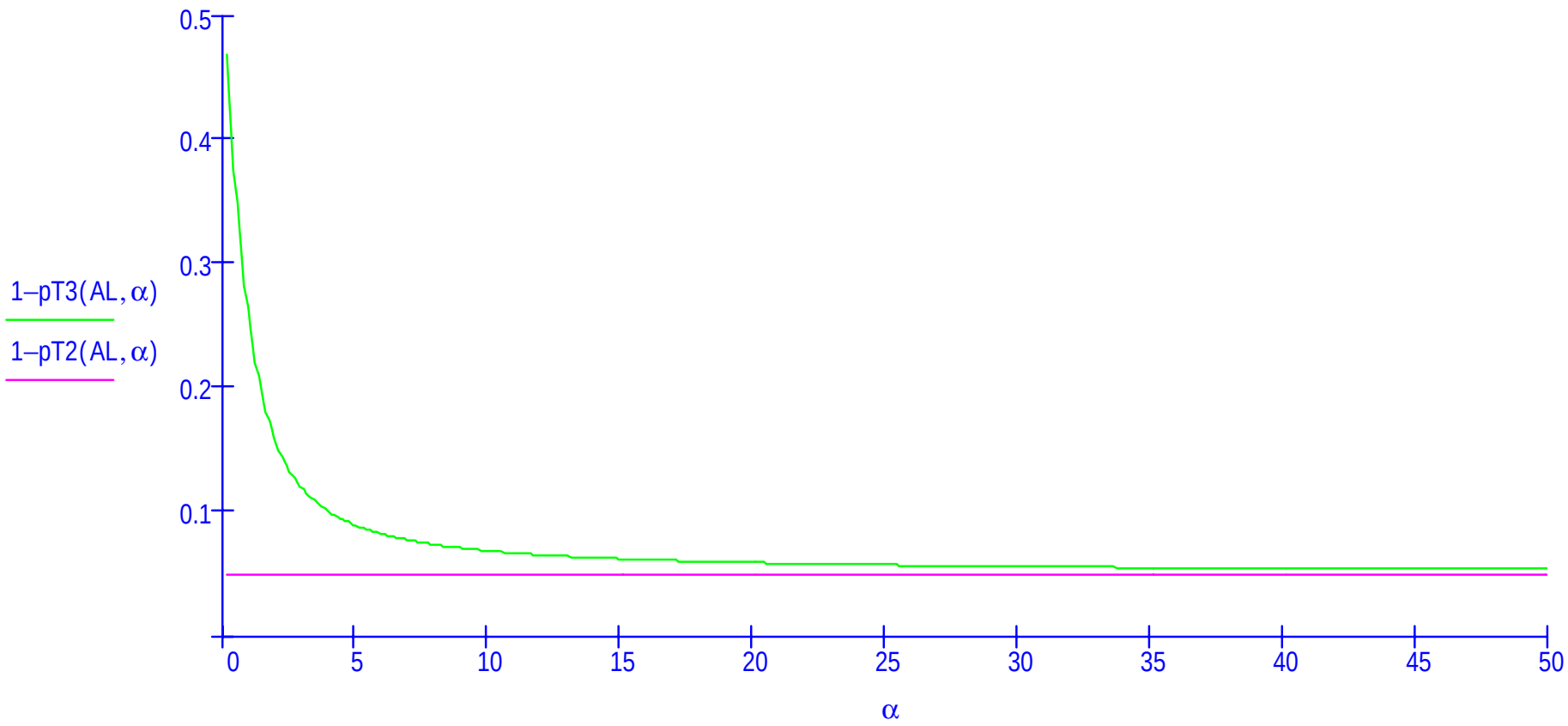


AL = SP + TLU = 1



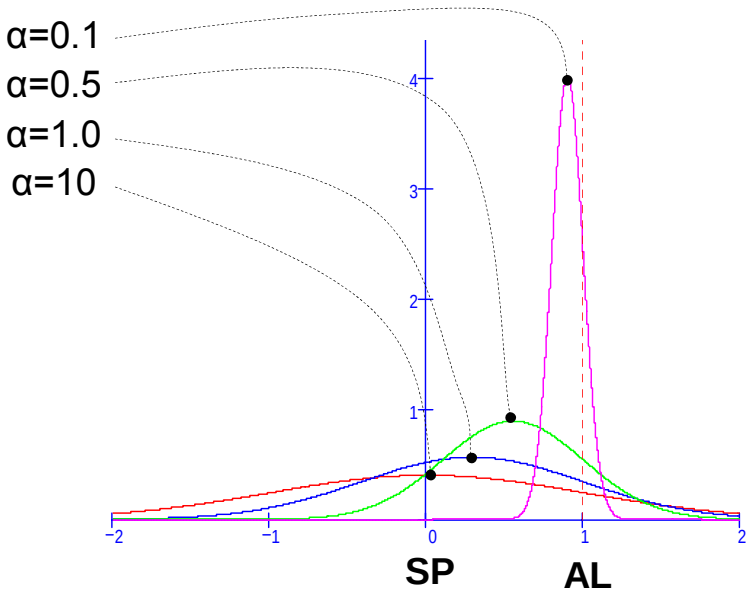
probability of failure to trip at Analytical Limit assuming measured setpoint at the M2 or M3 Allowable Value

as a function of the fraction of the TLU not included in the measurement



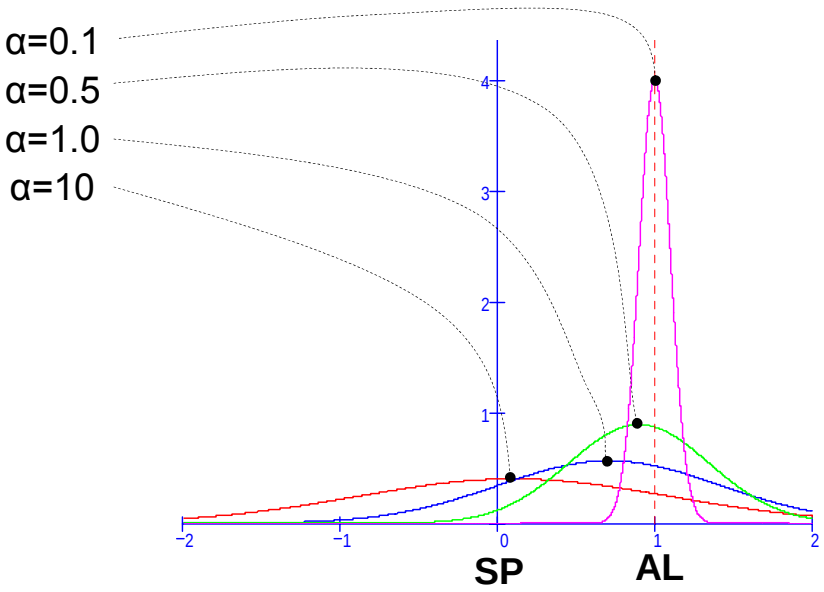
TripPoint pdf for various α

assuming measured setpoint at Allowable Value



deviation from setpoint in units of TLU

Method 2



deviation from setpoint in units of TLU

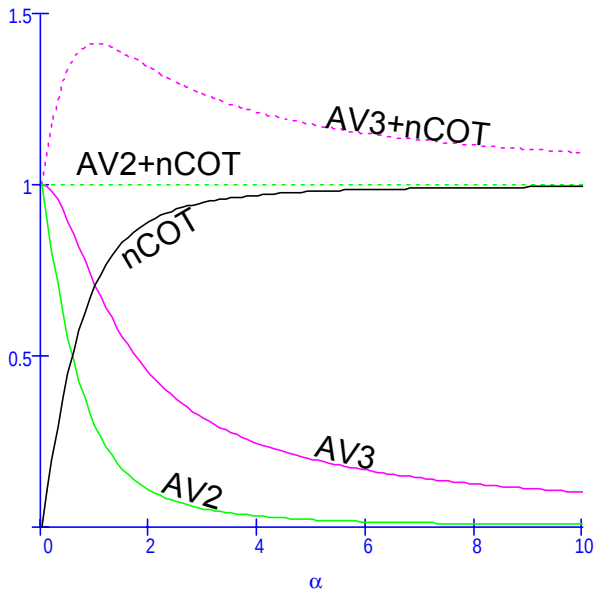
Method 3

Allowable Value and 95% trip probability point vs nCOT ratio

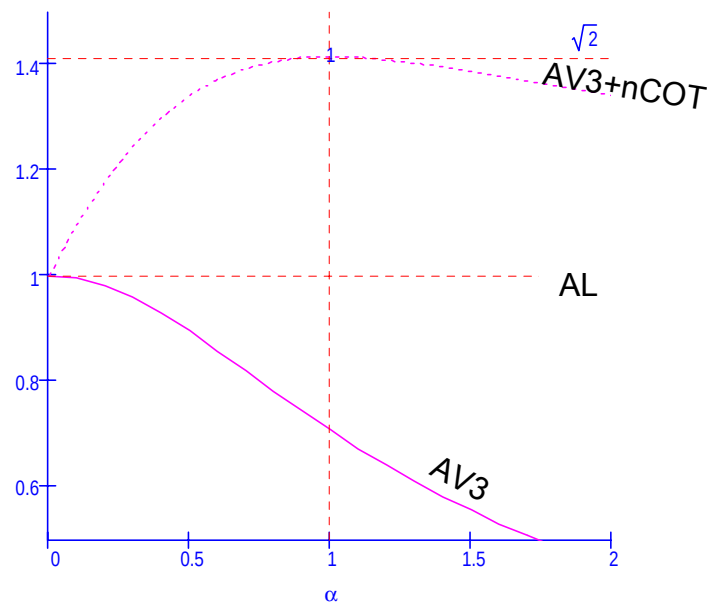
for M2 and M3

(Analytical Limit = 1 TLU)

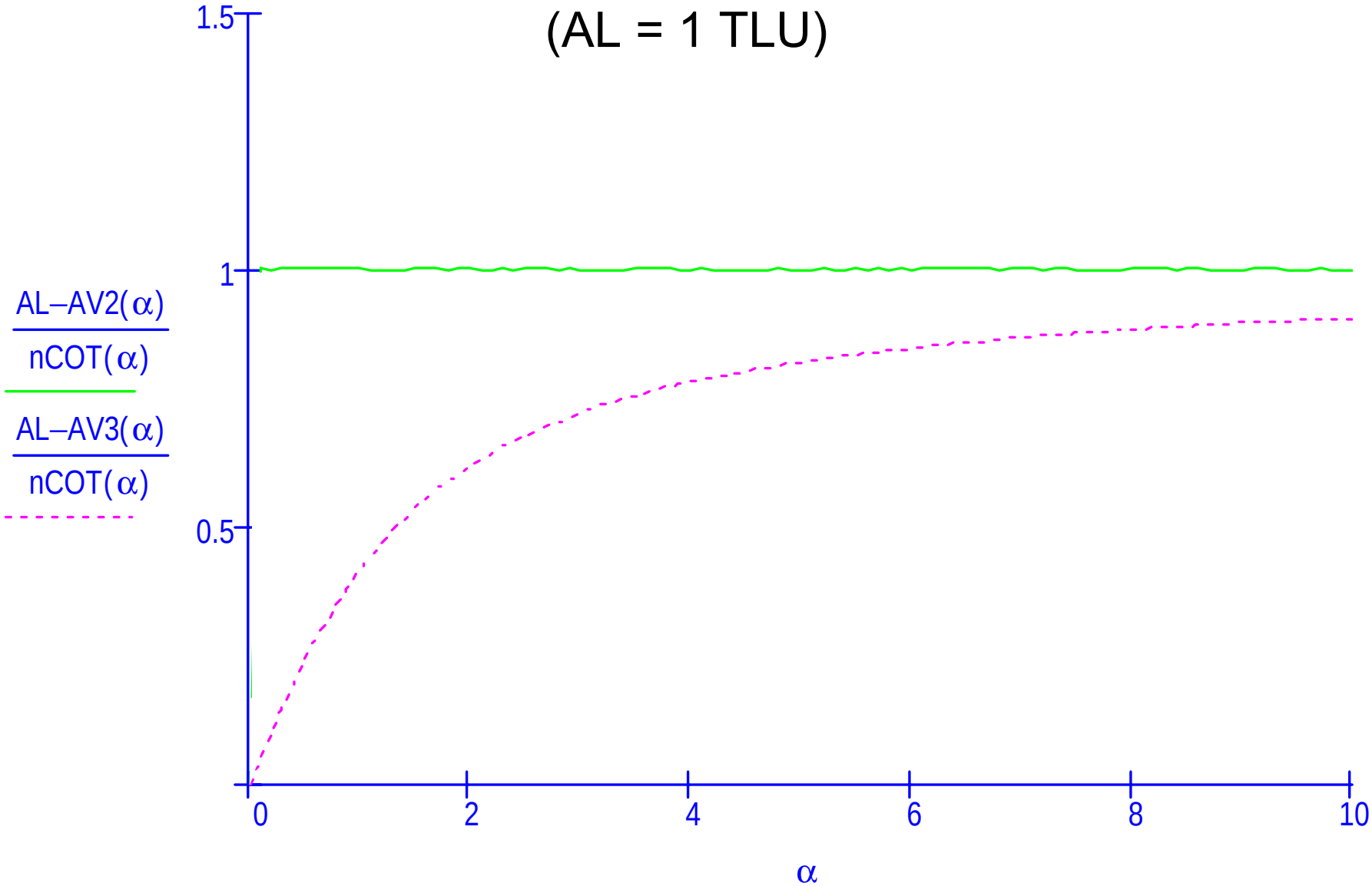
(nCOT is shown for reference)



M3 detail



Offset of AV2 and AV3 from Analytical Limit



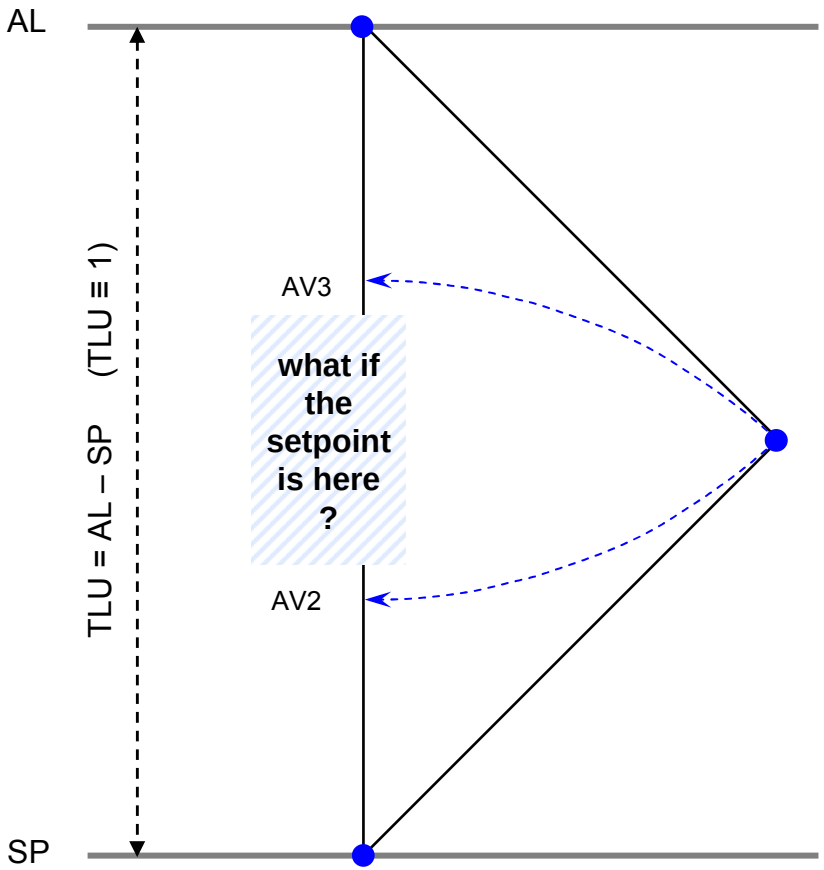
CONCLUSION

Method 3 does not provide adequate safety margin.

probability of failure to trip at AL can approach 50%

process must exceed AL by up to more than 41% TLU to get failure probability down to 5%

Epilogue #1:
Good Channels Gone Bad



Epilogue #1:
Good Channels Gone Bad

- important point is to protect AL
- SP measured within AV3 is expected behavior, but is not sufficient to protect AL
- protection of AL trumps fairness to the channel
- consequence of using SRSS – not enough margin between SP and AL for all possible errors

Epilogue #2:
Built to Fail?

"If Epilog #1 is true, then are we building-in an acceptance of failure?"

- in the absence of other information TP will be within TLU & all will be ok
- knowledge of COT result does not affect nCOT probabilities
- The act of observation changes COT statistics:
  - Once COT observations have been made, stochastic events have already taken place and conditions are more deterministic. The new characteristics are based upon conditions at time of COT and upon chance
  - The statistical characteristics of nCOT elements are not affected by COT.

Epilogue #2: Built to Fail?

- example:
  - Throw two dice: mean sum is 7.
  - Throw & read one die first, and then throw & read the other: mean sum depends on the reading from the first die, ranges from 4½ to 9½.
  - Throw two dice:
    - mean sum is 7
    - $P(\text{sum} \in [2,7]) = P(\text{sum} \in [7,12]) = 6 \div 11 = 55\%$
    - $P(\text{sum} \geq 7) = 55\%$
    - $P(\text{sum} \geq 7 \mid \{\text{first die}=6\}) = 100\%$

Epilogue #3: Resetting the Setpoint in the COT

- if not reset, then next COT may fail
- strong incentive to reset, but procedural rather than TS issue
- not an adequate substitute for proper AV because it does not ensure proper evaluation of present condition

Final Conclusion

AV must ensure that the probability of trip at AL is never less than 95%

- not at the time the setpoint is measured
- not during the interval until the next test

With Method 3, the probability of trip at AL is always less than 95%

Abbreviations and Definitions

SL:	Safety Limit
AL:	Analytical Limit (actuation point used in the plant safety analyses to demonstrate that SL is not violated)
AV:	Allowable Value (the limiting SP value for which the ATP is reasonably sure to be within the AL)
LSSS:	Limiting Safety System Setting described in 10DFR50.36 (must be in TechSpecs; usually expressed as AV)
SP:	SetPoint (the value at which the channel is measured or expected to trip; a mathematically deterministic value)
ATP:	Actual TripPoint (the value at which the trip actually occurs; a random variable composed of SP plus error)
AsF:	As-Found SetPoint (must be within AV)
AsL:	As-Left SetPoint (controlled via procedure; usually not in TechSpecs)
Uncertainty:	a bounding value for channel setpoint error (it is considered reasonable to expect that ATP will differ from SP by no more than “uncertainty”)
COT:	1) Channel Operation Test 2) The uncertainty remaining in the components included in the COT after the COT has been concluded
nCOT:	The uncertainty in the components and conditions not included in the COT
TLU:	Total Loop Uncertainty
SRSS:	Square-Root of the Sum of the Squares