Office for Nuclear Regulation

PSA expectations – a regulator's perspective

Shane Turner

Content

- Overview of ONR's expectation for PSA
- Changes in expectations post Fukushima
- The revision to the PSA aspects of the ONR Safety Assessment Principles
- What the numbers mean to ONR
- Conclusions

ONR's expectation for PSA

- PSA is a fundamental and integral part of the safety case
- LC 23 requires an adequate safety case
- ONR's expectation
  - Three legs to fault analysis
    - Design basis analysis
    - PSA
    - Severe accident analysis
  - Adequacy of PSA
    - ONR Safety Assessment Principles FA.10 to FA.14
    - ONR Technical Assessment Guide (TAG) 030 for PSA
    - Informed by international standards, guidance and practice
  - ALARP should not be used as an argument for not doing adequate analysis

Changes post Fukushima

- No significant changes to ONR expectations
  - Small changes to PSA related SAPs proposed (more later)
  - TAG 030 remains fit-for-purpose
- Emphasised the importance of comprehensive PSA
- Greater focus on hazards PSA
- Emphasised the importance of an adequate level 2 PSA
  - Magnox level 2 PSA
  - AGR level 2 PSA
  - Sizewell B level 2 PSA
  - New build level 2 PSA
    - Hinkley Point C
    - Generic Design Assessment

Chief Inspector's recommendation post Fukushima

- Recommendation FR-4 concerned the need for level 2 PSA
- Includes consideration of external hazards
- Includes extended mission times
  - *Long duration faults*
    - *Loss of offsite power (LOOP)*
    - *Loss of ultimate heat sink (LUHS)*
  - *Long duration safety system requirements*

Consensus on need for consideration of extended mission times

- IAEA – SSG3
  - Success criteria should specify the mission time to reach safe stable shutdown state … and for long term recovery actions to be established
- WENRA – Issue 0 (2013 rev)
  - Mission times in the PSA shall be justified
- ONR SAPs (2014 consultation version)
  - The mission time for PSA should be justified…. Where repair and/or recovery actions are needed to achieve a safe stable state, these should be modelled

Extended mission times – ONR expectations

- For duty holder to propose and justify
- Not prescribing either times or modelling methodologies
- Realistic best-estimate data and assumptions preferred
- Repair and recovery actions justified (task analysis, training etc)

SAPs (2014 consultation version)

- Need for PSA
  - New paragraph to emphasise the expectation for a level 2 PSA

    “Where the off site accident consequences are potentially significant, such as for an operating power reactor, the PSA should be at least to level 2 (i.e. provide information on the frequencies and characteristics of different fission product releases to the environment) and include analysis of all external events (including “beyond design basis” events) that could realistically lead to a significant off-site release.”

SAPs (2014 consultation version)

- PSA validity
  - New text to emphasise the expectation for PSA to be living

    “The PSA should be updated regularly, which for power reactors should mean adopting a “living PSA”. Where the PSA is in support of a design under development, the guidance set out in para # should be followed”

SAPs (2014 consultation version)

- Scope and extent
  - Principle FA.12 changed to emphasise the expectation that PSA should be comprehensive:

    "PSA should cover all significant sources of radioactivity, ***all permitted operating states*** and all relevant initiating faults"

  - External hazards initiating frequency no longer constrained:

    "Screening criteria used to exclude low frequency faults should be justified."

  - New text as a result of learning from Fukushima:

    "The identification of initiating faults should consider the potential for combinations of hazards. At multi facility sites, the analysis should also consider the potential for specific initiating faults giving rise to simultaneous impacts on several facilities."

SAPs (2014 consultation version)

- Adequate representation
  - New text as a result of learning from Fukushima:

    “The sequences used for the PSA should each be modelled until a stable safe state (for example on reactors, a cold shutdown state) is reached. The “mission time” (i.e. the duration over which the PSA is applied) for PSA should be justified accordingly. Where repair and/or recovery actions are needed to achieve a stable safe state, these should be modelled.”

SAPs (2014 consultation version)

- Adequate representation
  - Text clarified relating to best-estimate methods and data:

    "Best-estimate methods and data should be used as far as possible within the PSA and in particular for determining initiating event frequencies and in the supporting transient, accident progression, source term and radiological analyses. … Notwithstanding principle FA.5, an adequately justified best-estimate frequency should be used for naturally occurring hazards."

SAPs (2014 consultation version)

- Use of PSA
  - Further applications of PSA have been included:
    - supporting the demonstration that risks are tolerable and ALARP;
    - informing the selection of safety function categories or the safety class of structures, systems and components (see paras 150 and 153);
    - setting operating rules;
    - informing arrangements for examination, maintenance inspection and testing (e.g. the frequencies of these activities);
    - plant configuration control (including maintenance planning), which for power reactors is normally through the use of risk monitors;
    - event analysis and investigating significant incidents and events;
    - helping to determine initiating event frequencies for DBA; and
    - providing an input to SAA and to analyses performed under REPPIR

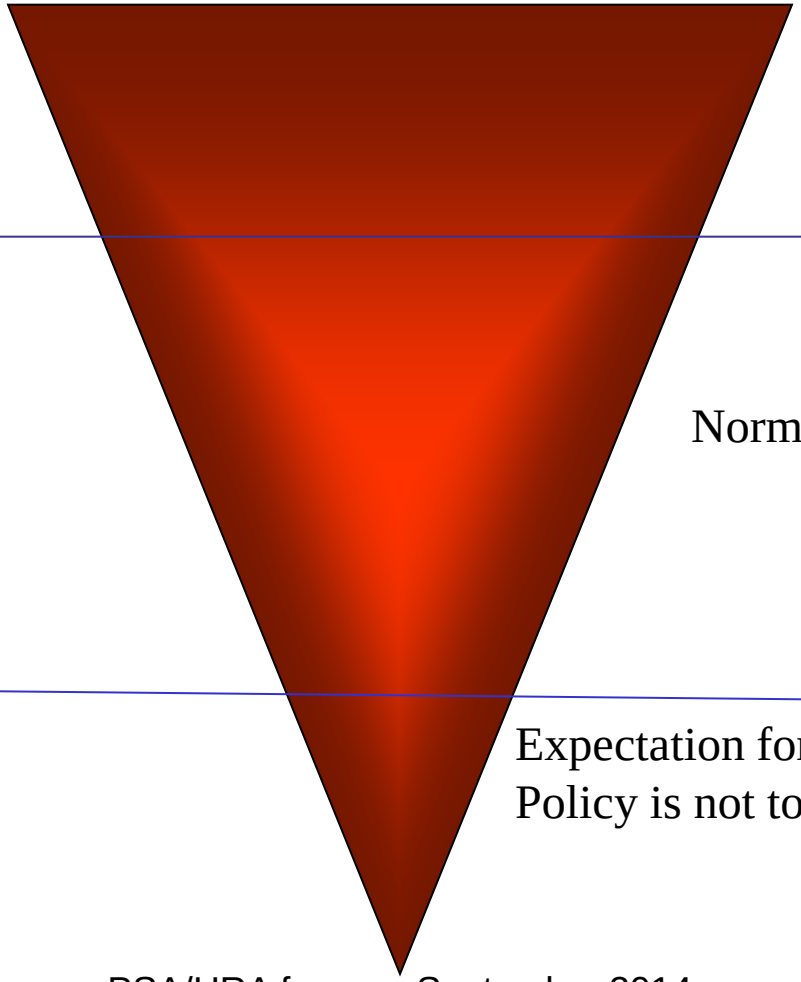
What the numbers mean to ONR

- Overview
- PSA and tolerability of risk
- PSA risk versus real risk
- CCFs
- Zero failures
- Digital C&I
- Approach to PSA data

What the numbers mean to ONR

- **PSA is not just a bunch of numbers!**
  - **To demonstrate that a balanced design has been achieved, such that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk**
  - **To help demonstrate that the risk associated with the design and operation of the facility is and remains ALARP**
  - **To enable a judgement to be made as to the acceptability of the overall risk of the facility**
- **Numbers should be the last thing that are assigned**
  - **Main element of PSA is the logic**
  - **What it tells you about the architecture of the safety claims**
  - **How they link to the complex underlying engineered systems and human claims**

PSA and tolerability of risk



New facilities must meet BSLs
High gross disproportion
Long term plan needed

Unacceptable region

Tolerable Region

Normal regulatory business

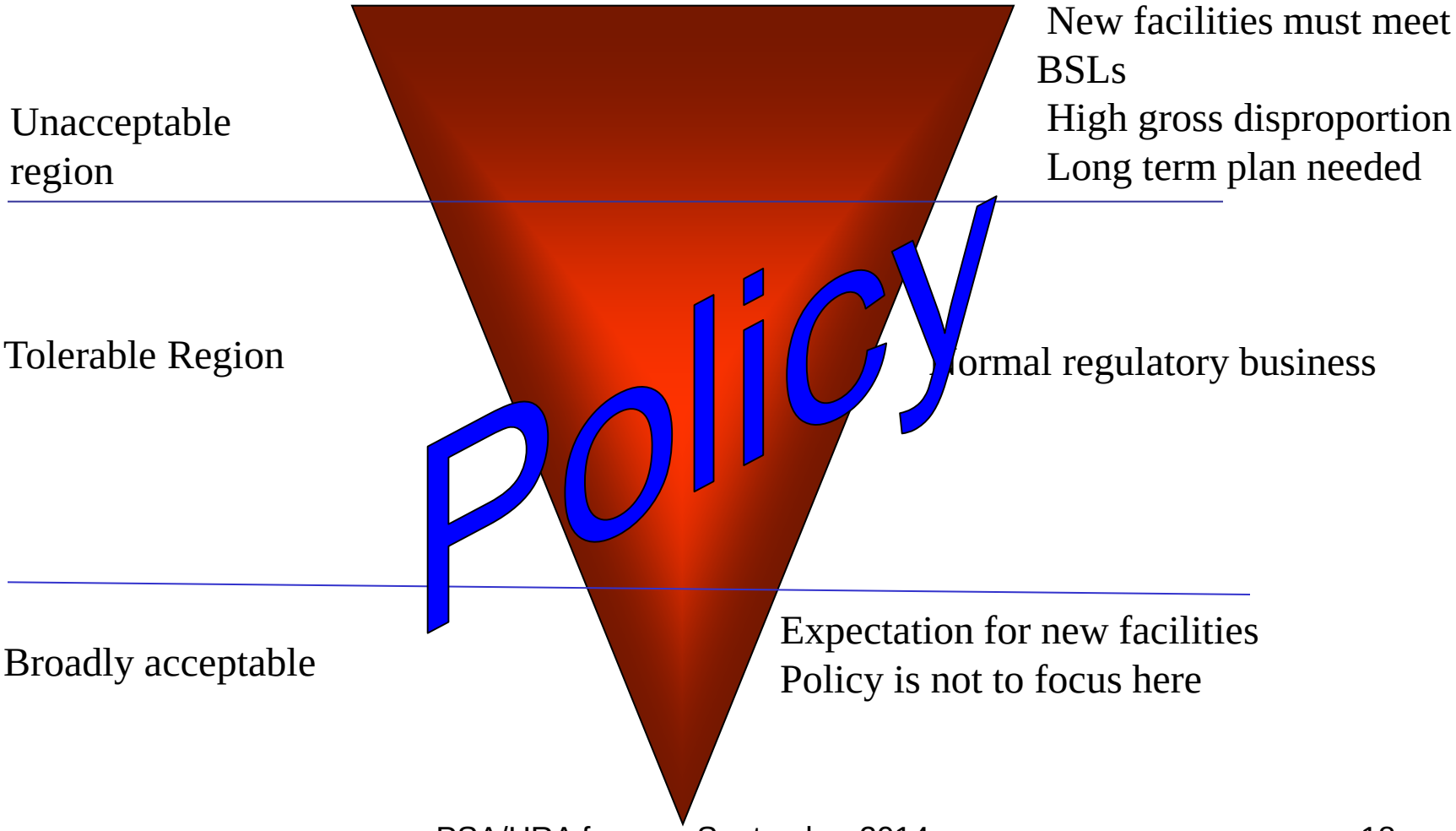
Expectation for new facilities
Policy is not to focus here

Broadly acceptable

PSA and tolerability of risk

- Frequent misunderstanding
  - ALARP is **NOT** simply a matter of numbers
  - ALARP is rarely even numerical!
  - Numbers can inform the ALARP decision but should "guide rather than decide"
- PSA myth
  - Risk is broadly acceptable and therefore ALARP, which equates to do nothing

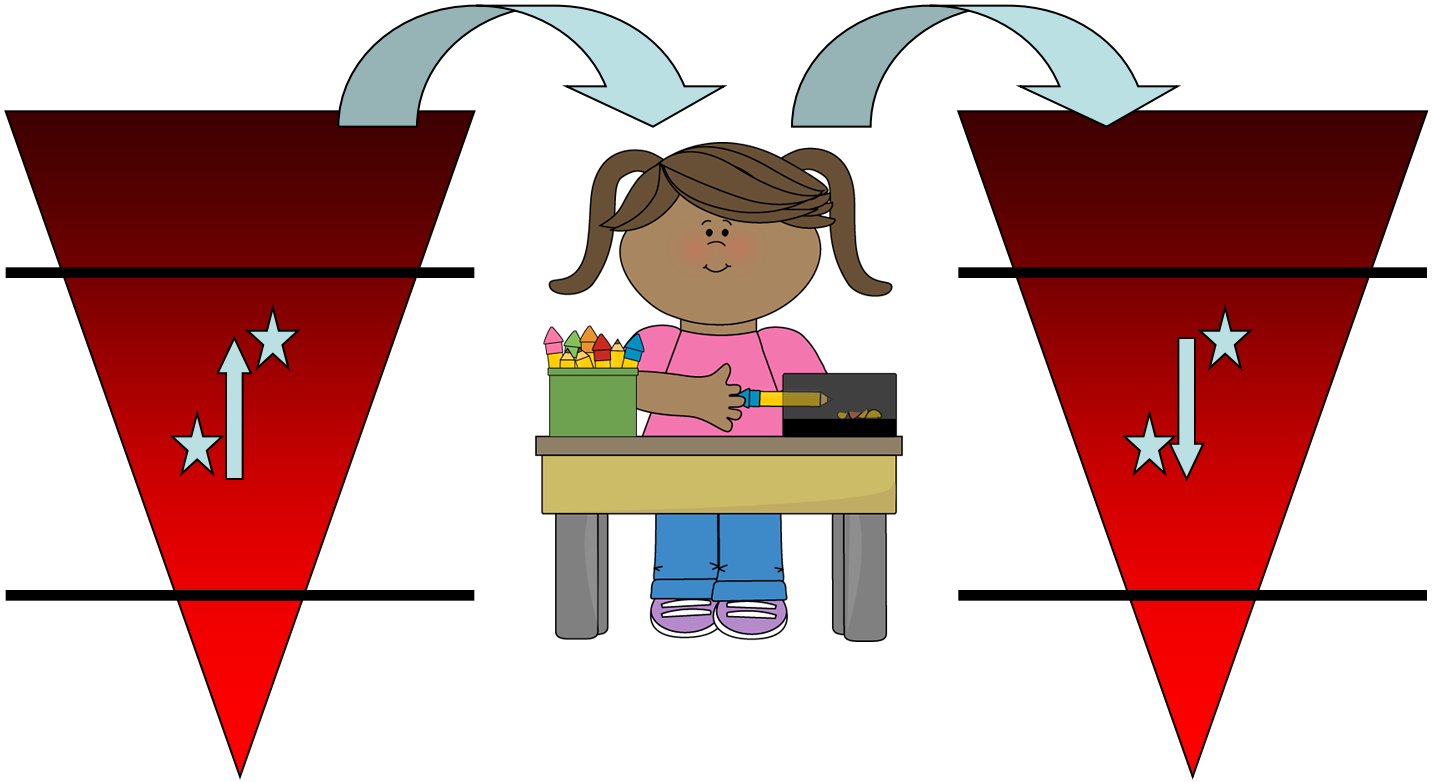
PSA and tolerability of risk



Key focus of PSA

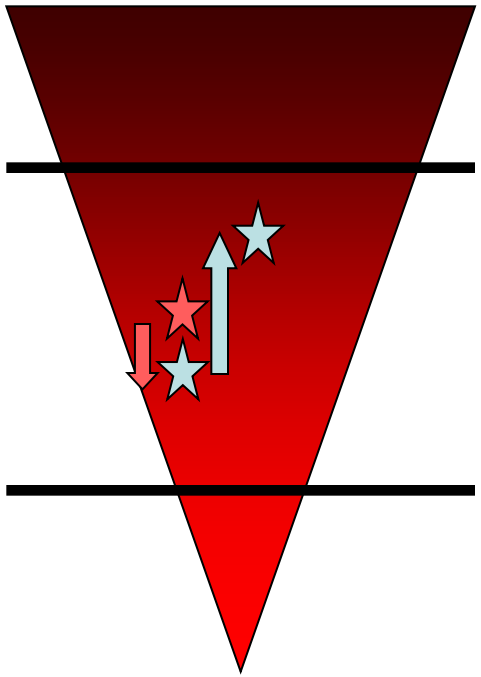
- Structured and systematic thinking process
- Qualitative insights
  - Cut-sets
- Quantitative insights
  - Dominant sequences
  - Importance
  - Sensitivity
  - Balance of risk
  - Level of risk (last and least important!)
- Appropriate fidelity
- Comprehensive – events and modes of operation
- Best-estimate representation of risk
- Numbers have a role …

PSA risk versus real risk



PSA risk unchanged, therefore ALARP?

PSA risk versus real risk



- Consider changes to PSA insights
- Remove conservatisms from base case first
- What more could be done?
- Why aren't you doing it?

- Interested in whether there are any reasonably practicable enhancements to manage the change in 'real' risk

CCFs

- Is a CCF cut-off in PSA reasonable?
- ONR expectation:
  - $1x10^{-5}$ pfd for a simple system
  - $1x10^{-4}$ or $1x10^{-3}$ pfd for complex / novel system
- Is there sufficient experience to substantiate better claims?
- Substantiation key
- Robust sensitivity analyses would be required for better claims
- Cut-off values lower than $1x10^{-5}$ should be exceptional and will require a very high level of justification
  - Insufficient diversity in the design

Zero failures

- What approach should be used?
  - Bayesian – 0.55 failures
  - Chi squared – 0.7 failures
  - Assume 0.5 or 1 failure
- Does it matter?
- ONR will not dictate the approach used
  - Will look for sufficient justification
- Salami slicing zero failures …
  - Initiating event x component failure x CCF
  - Zero failures to the power of 3
  - Is this appropriate?

Digital C&I

- PSA should not blindly use safety case targets as basis of pfd
  - PSA is a best-estimate tool
  - Is there a difference between reliability to meet IEC 61508 and that assumed in PSA?
- Example
  - Statistical tests to demonstrate 10^{-4} pfd with 99% confidence
  - 50,000 fault free tests
  - Best-estimate assumption 10^{-5} pfd
- Robust sensitivity study

Approach to PSA data

- PSA is not just a bunch of numbers
- But, numbers are important
- PSA should be site specific
  - Fidelity
  - Data
- Consistent hierarchy to use data should be applied
- Robust data processes
- Bayesian updating – is this always necessary?
- Best use of plant data

Conclusions

- PSA is a fundamental and integral part of the safety case
- PSA needs to be comprehensive and representative of the plant
- PSA is not just a bunch of numbers
- Data should be best-estimate
- Cut-offs should be used with care
  - Sensitivity analyses
  - Low claims need strong justification
- In a safety argument, interested in change in real risk

Questions?