Quantifying the Unimaginable

Human Performance Limiting Values

What is the maximum human reliability of a single human operator? 10^{-3}? 10^{-4}? 10^{-5}?

Barry Kirwan, Eurocontrol

Ian Umbers (BEGL), Jim Edmunds (CRA), Huw Gibson (University of Birmingham)

Overview

- The Problem Area
- HPLVs
- Guidance

Scenario

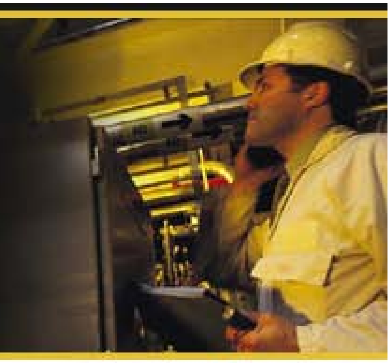
- Nuclear Power Plant
- Loss of feedwater
- Operating team fail to recognise need to commission boiler feed for post-trip cooling (1.5hrs after trip)
- Continues to fail for further 8 hrs
- What is the failure probability?
- What is the failure mechanism, anyway?

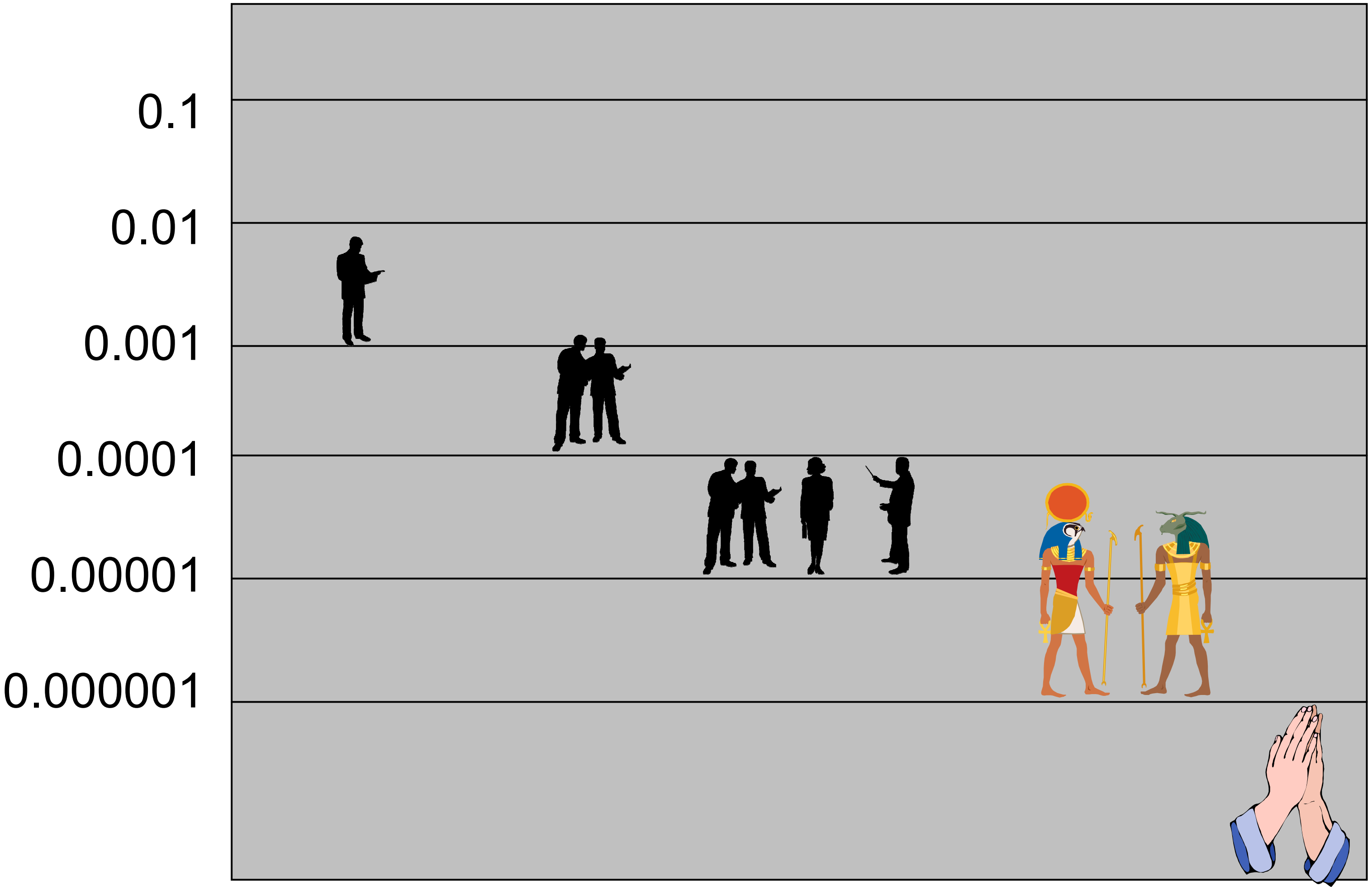
Human Error Probabilities in Cutsets

- Operator 1 fails to do it right
- Operator 2 fails to check operator 1
- Supervisor fails to detect error
- Operator 3 fails to re[illegible] correctly
- Operator 4 fails to co[illegible]
- Supervisor fails to ov[illegible]d

Whoa !!!

The Problem – human performance limits





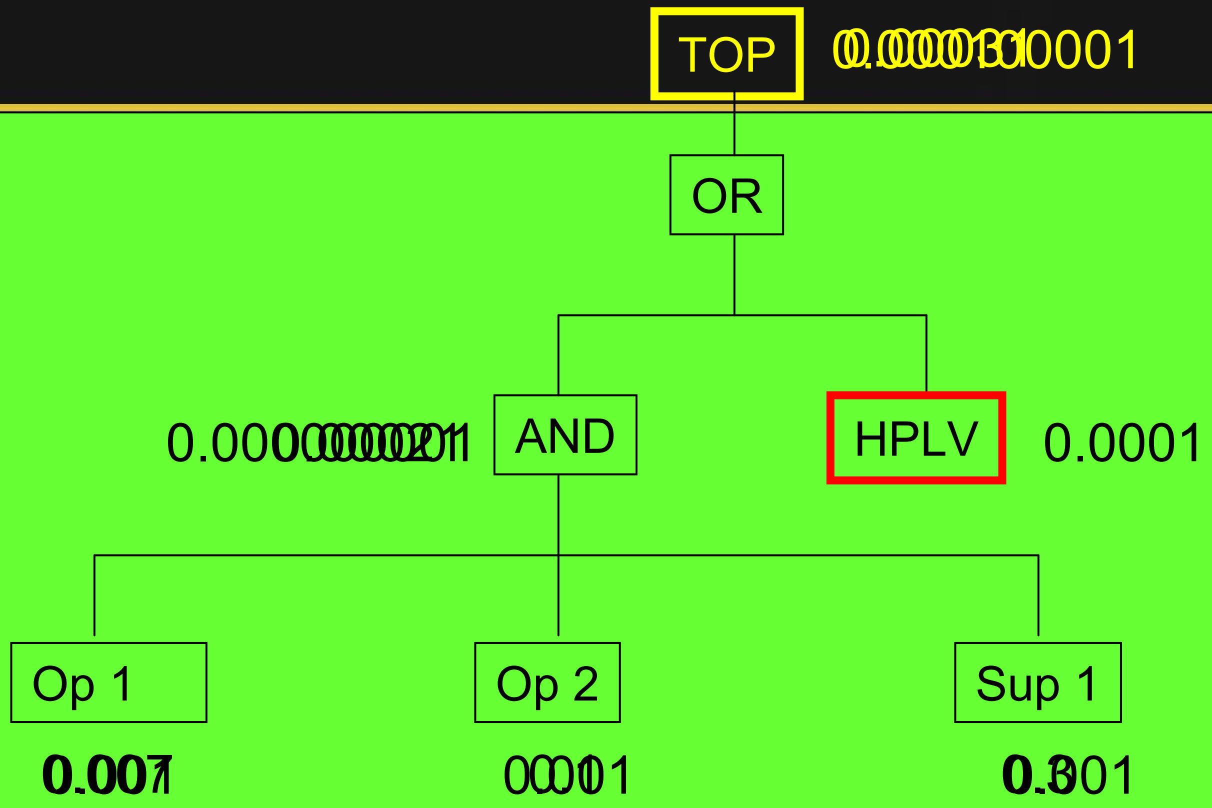
Nureg1792

Human Performance Limiting Values (HPLCs) cutset ‘cut-off’ values

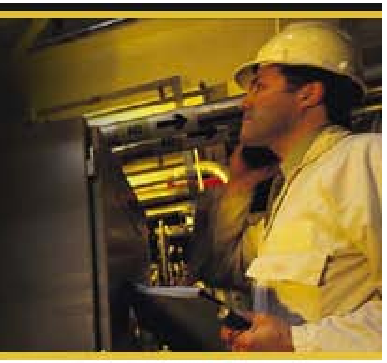
- Circa 1990, BNFL THORP Safety Case Methodology
- Reviewed human error data < 10^{-5}
- Concerned over optimism
- 3 HPLVs:
  - – 10^{-4} Single operator
  - – 10^{-5} One operator team in plant / Central Control Room
  - – 10^{-6} Rare usage – exceptional CCR conditions
- Some other utilities use them (e.g. PSI)

A HPLV is NOT a HEP

Example


TOP
0.0000310001
OR
0.00000000201
AND
HPLV
0.0001
Op 1
0.007
Op 2
00001
Sup 1
0.301

Utility of HPLVs: BNFL experience



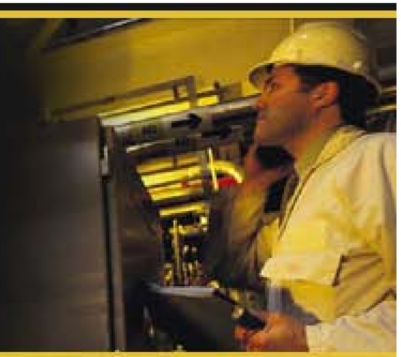
- Checked optimism
- Straightforward for assessors
- BNFL interpretation of NII SAPs discontinued use of 10^{-6}
- HPLV Sheets & Review by HF Team
- Highlight issues to internal Safety Committee
- Use of ‘Non-credible’ argument in some cases
- If have data (e.g. $<10^{-5}$) then use data
- Approach allows focus of safety effort where needed

UK Nuclear Industry Workshop on HPLVs (2007)

British Energy; British Nuclear Fuels; Atomic Weapons Research Establishment; Nuclear Installations Inspectorate

NARA Project Team

Usage of HPLVs in UK



- **Reprocessing**
- Less diagnosis; many small fault trees; assessors have HF training; **HPLV process clear to assessors**
- Some events not modelled if HD or CD
- Assessors model and choose value of HPLV in (small) FT
- Justification sheets (HPLV)
- HF Review – if 10^{-5} consider task analysis; determine impact on risk target; consider pessimisms; identify improvements (ALARP)
- Can designate ‘non-credible’ argument

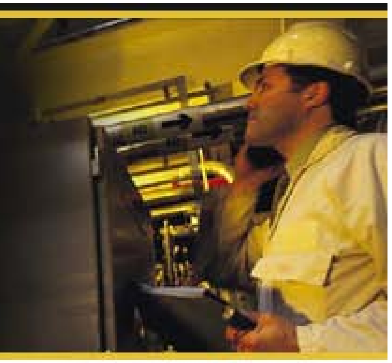
- **Defence**
- [No diagnosis; very many very short fault sequences; criticality]; long FT under an OR gate; focus on initiating events
- Quantify using THERP or historical data
- Consider direct dependence (THERP)
- **If < 10^{-5} then apply HPLV cut-off 10^{-5} for group or 10^{-4} for single person**
- If risk sensitive try qualitative approach / ALARP

Process

- **Gas-Cooled Reactors**
- Initiating events give auto trips (high level of redundancy): focus on post-trip – need operator support after 1-2 hrs; massive fault trees; some latent failures; SRV lift is major milestone
- Identify required actions – focus on key actions (do task analysis)
- 2 periods – initial and long timeframe: assumptions of different shifts, continued need for action
- Raise all HEPs to 0.9 and review cutsets

- **PWR**
- Some long timeframe actions – assumption about shift changes; PWR has a shutdown PSA where more dependent on operator diagnosis/action
- No HPLV usage
- Latent errors are in – do not see need for dependency across latent/active boundary
- THERP & Direct dependence using modified formula – slightly less pessimistic
- Raise all HEPs to 0.9 (prioritisation analysis)

Workshop Approach



- Scenarios considered by all parties
- Usage & non-usage of HPLVs discussed
- Frank & honest discussion, regulator present
- Differences in plant type, and assessment approach has an effect
- Idealised process evolved after the workshop

Scenario

- Ops fail to recognise need to secure continuous boiler feed for post-trip cooling within 2.5 hrs of reactor trip
- Fail to respond to a break in boiler feed and issue instructions to re-instate boiler feed within *a further 12.5 hrs*
- Various alarms; SRV lifts 4.5 hrs into scenario; change of shift; Symptom-Based Emergency Response Guidance

Scenario 3 - Glove-box Scenario

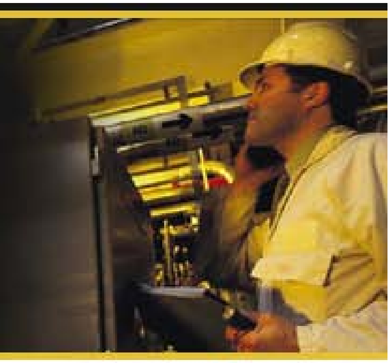
- Build up of powder – fail to detect in one month
- Process related check (2)
- Weekly check (3)

- 2 different people
- Same check
- Administrative control
- HPLV 10^{-4}

Principles

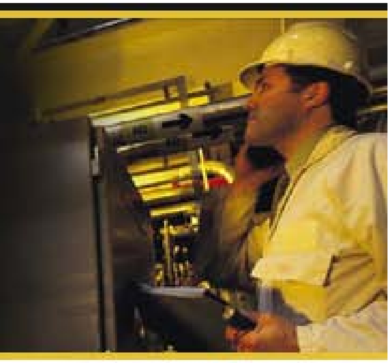
- An HPLV is not a Human Error Probability (HEP), and is only used to bound a cutset, preventing optimism
- Direct dependence should be modelled before HPLV application – HPLVs should not be a short-cut for modelling or understanding
- An HPLV acts as a ‘flag’ to assessors that a deeper look needs to be taken to determine risk significance
- Indiscriminate use of HPLVs distorts the risk picture
- A utility’s Risk Management processes should include dependence counter-measures
- HPLVs are not a solution to errors of commission – separate searches for EOCs (latent and post-trip) should occur
- Whatever the approach taken for dependence, it needs to be transparent and defensible
- The lowest credible HPLV appears to be 10^{-6}
- Positive Safety Culture must also be assured separately

Guidance



- Model direct dependence, including cognitive dependencies
- Apply HPLVs as appropriate
- Consider impact on risk target
- If risk sensitive:
  - If single personnel consider centralising / adding personnel
  - If new plant, consider design change to improve human-system reliance balance
  - Work on ‘optimising factors’, countering ‘mechanisms’
  - Deem ‘non-credible’ go to peer review
  - Use 10^{-6} if long timescale
  - Make As Low As Reasonably Practicable (ALARP) case
  - Re-design task

Conclusions



- Two of the four companies make regular use for HPLVs – most of the time they don’t matter; but occasionally they help assessors see ‘the wood for the trees’, and they know they have to dig deeper

- In new plant, the ideal would be to have a better balance between technology and human, such that there was less need to resort to HPLVs. However, outage PSAs etc. may remain a different story

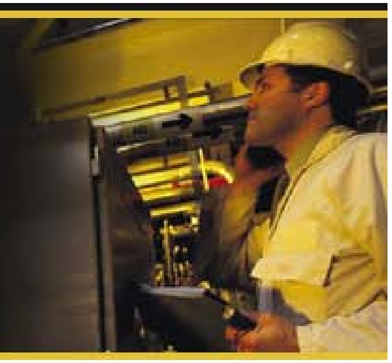
- As ever, the numbers are less important than the search for vulnerabilities and the attempts to defend against them, and maintaining transparency throughout this process. HPLVs are ‘blunt’ but clear.

Closing statements (from the Workshop)

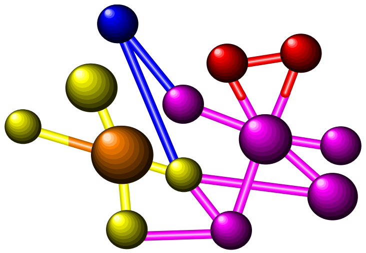
- Balance between human and hardware reliability
- HPLVs covering ‘residual’ (epistemic) uncertainty
- Regulator – no expectation for licensees to use HPLVs – but can see that direct dependence will not capture everything, and you can get excessively optimistic cutsets – there is a case for using HPLVs – though not as a substitute of direct dependence modelling

Questions?

INDIRECT DEPENDENCE



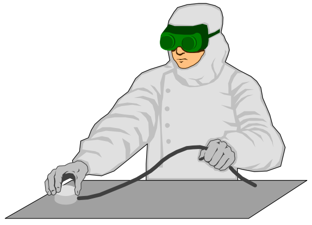
- Equivalent of CMF or Beta factors
- Allowing for unforeseen dependencies – interactions less understood
- Incident & accident experience tells us we are not so reliable
- Accounting for (partially) errors of commission
- Limits of human performance
- Limits of prediction



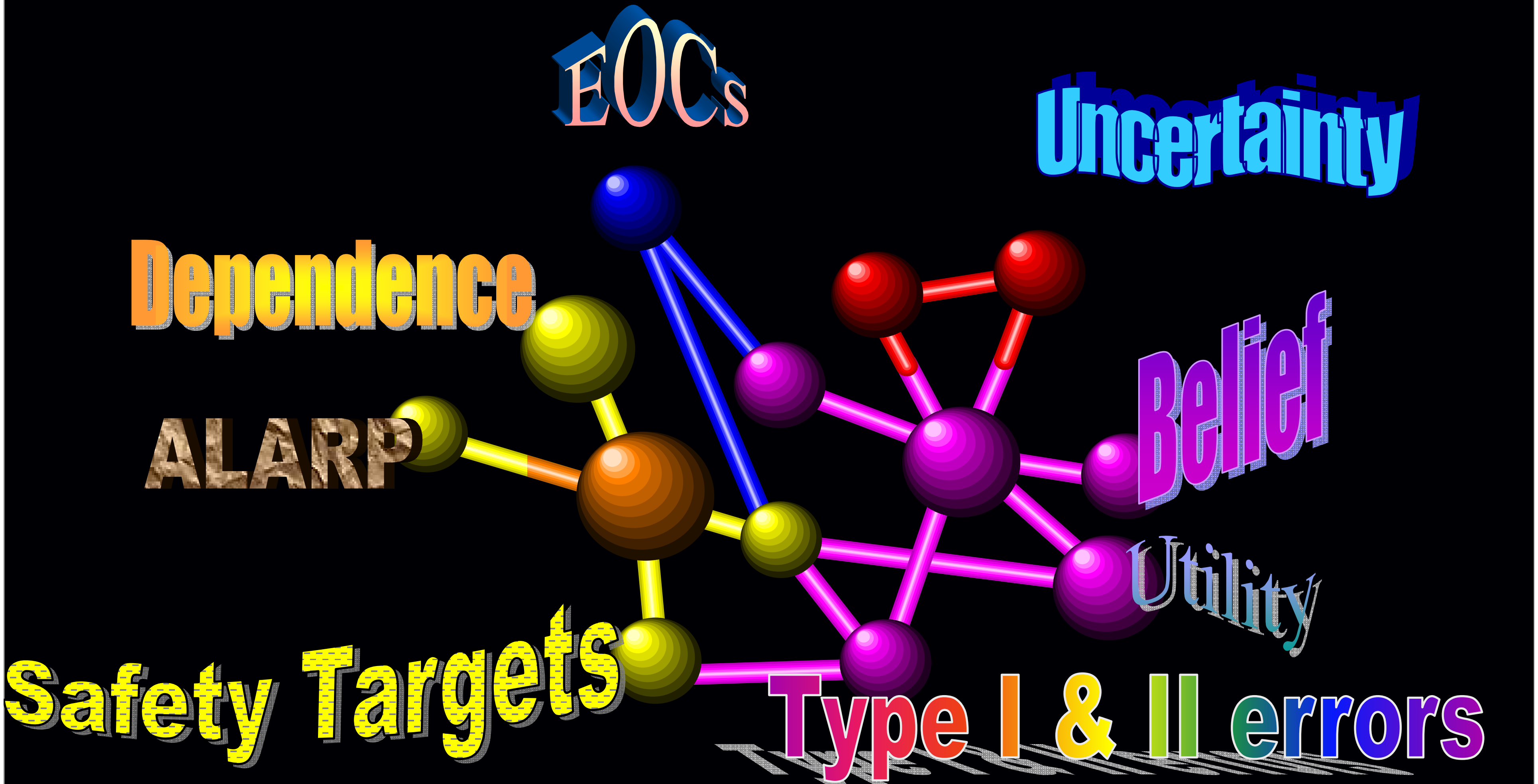
Epistemic Uncertainty

HPLV Issues

- DIRECT DEPENDENCE
- Clear mechanism of dependence
- Swain/HSE factors apply – same people, task, timeframe, etc.
- Use of THERP adjustment factors, conditional probabilities, judgement, etc.



Multiple perspectives



EOCs

Uncertainty

Dependence

Belief

ALARP

Utility

Safety Targets

Type I & II errors