International Engineering Safety Management
Overview and what's new

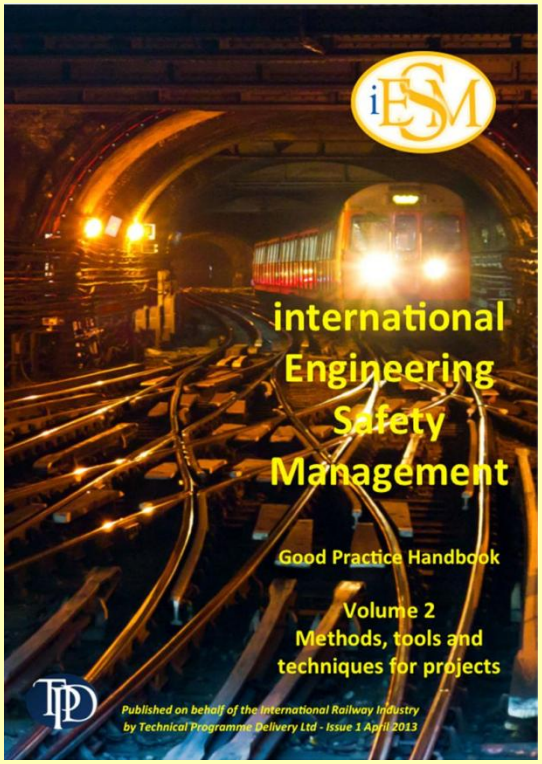
Paul Cheeseman

Technical Program Delivery

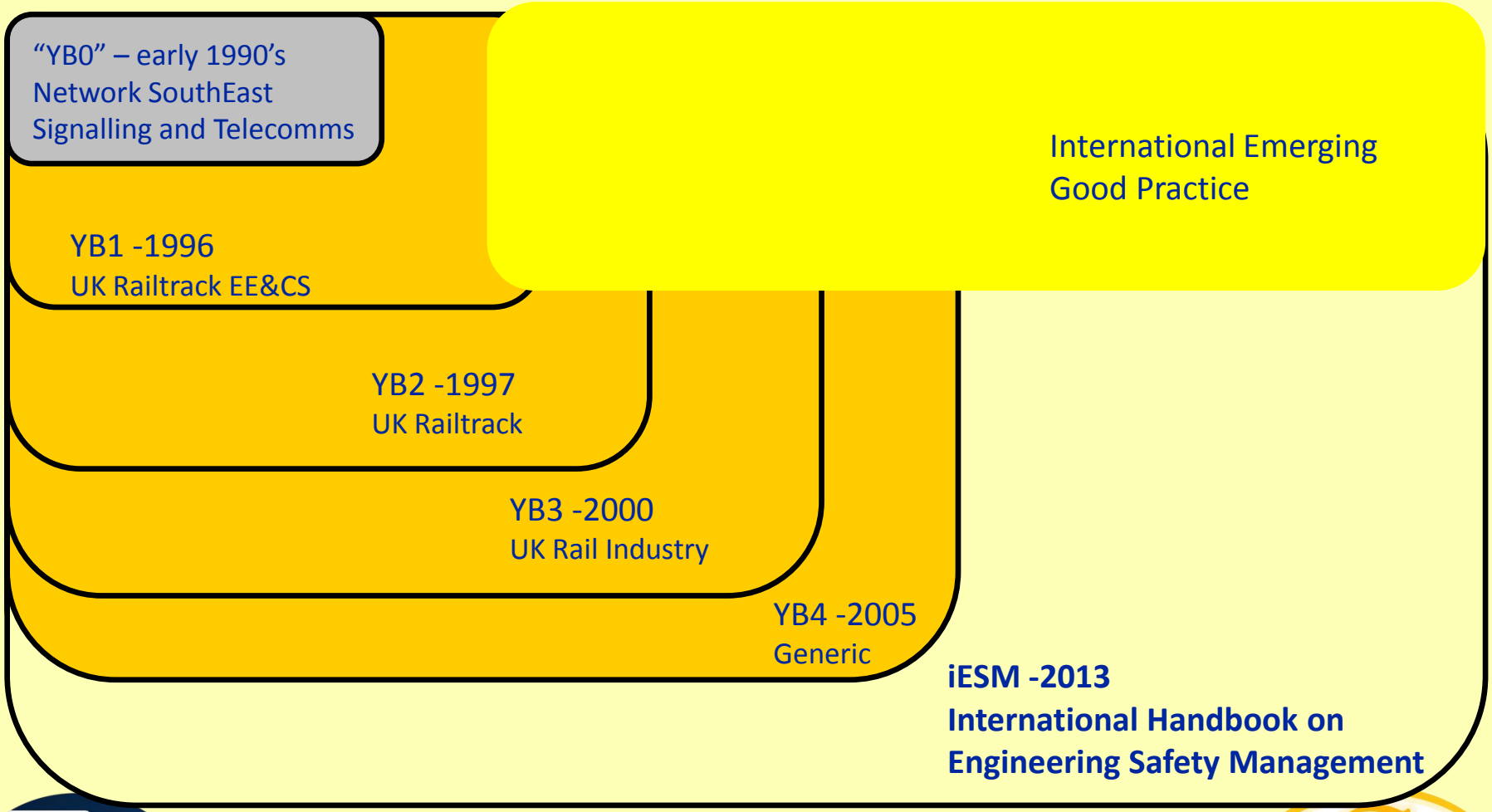
paul.cheeseman@tpd.uk.com

iESM - Aim

- To assist the international railway industry in delivering products/systems with acceptable levels of safety by developing & sharing good practice in railway Engineering Safety Management worldwide.
- Being developed as part of the TPD internal research activities, for the good of the rail industry.

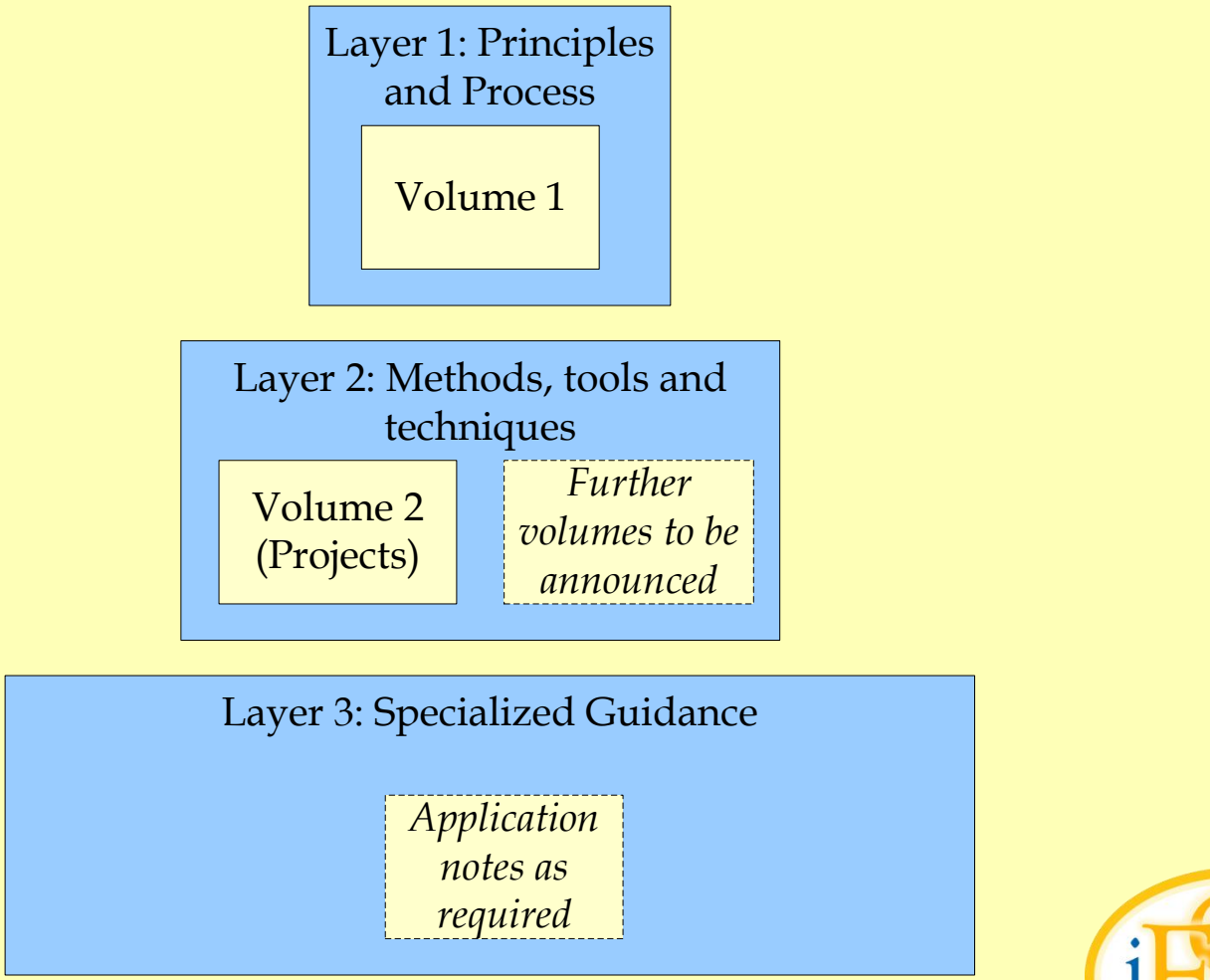


ESM - History


"YB0" – early 1990's
Network SouthEast
Signalling and Telecomms
YB1 -1996
UK Railtrack EE&CS
YB2 -1997
UK Railtrack
YB3 -2000
UK Rail Industry
YB4 -2005
Generic
International Emerging
Good Practice
iESM -2013
International Handbook on
Engineering Safety Management

iESM - Structure

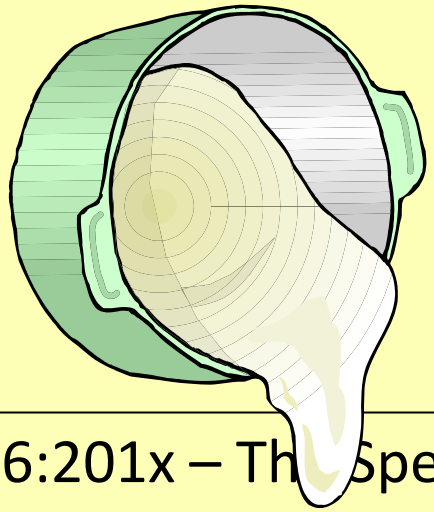
Volume 0



iESM - What's in?
Emerging good practice

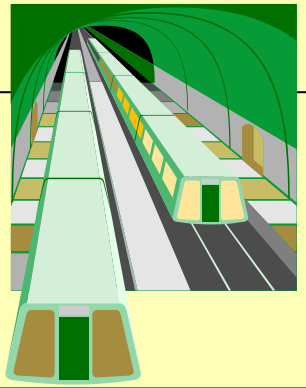
- Common Safety Methods for Risk Assessment have been mandated on parts of the railway by European Directives
- Recent EN50128 with focus on roles and competence
- New CENELEC EN50126 incorporating the former EN50128/9/155
- Guidance from RSSB UK "Taking Safe Decisions"
- Increasing use "Cross Acceptance" fast track
- Increasing awareness and demand for a risk-based approach internationally especially in emerging economies

CENELEC Changes



EN50126
EN50128
EN50129
EN50155
and more

EN50126:201x – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
Part 1 Generic RAMS process
Part 2: Systems Approach to Safety
Part 4:Functional Safety –EEP Electronic Systems
Part 5: Software



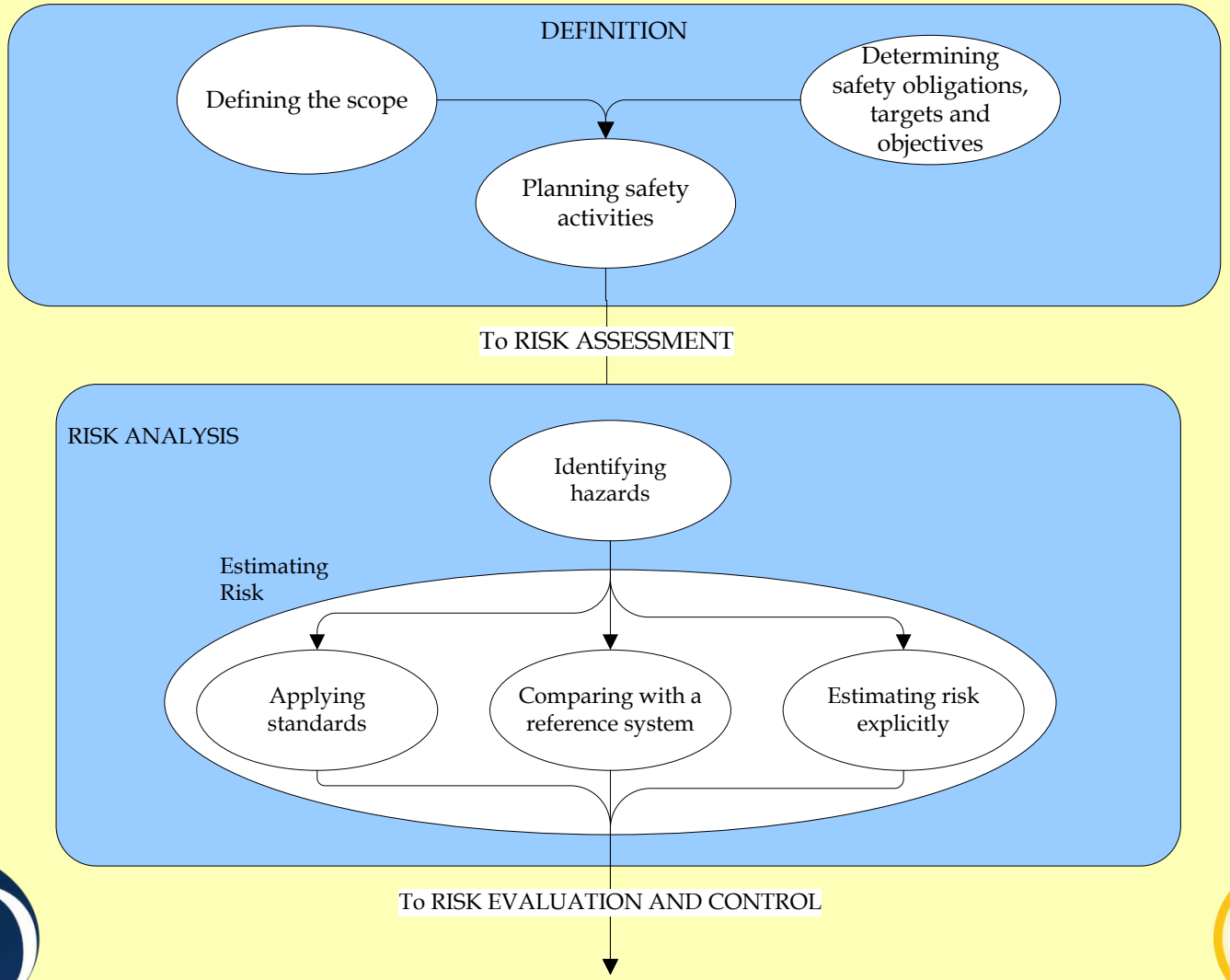
SIL 0 – a new level of safety

- Where the target rate of occurrence of failure is less demanding than 10^{-5} per hour
- Aims to address uncertainty without overkill avoiding unproductive expenditure on low risk functions draining funds from high integrity functions.
- For SIL 0 software demonstration, where a certificate stating compliance with EN ISO 9001 is available, no independent assessment may be required.

iESM - What's out?

- Bias towards any one legal system or regulatory framework (e.g. requirement to reduce risk ALARP)
- Known deficiencies and poor practice e.g. using risk matrices as a sole method for risk acceptance
- Templates, checklists, techniques etc to layer 3
- Explicit consideration of maintenance activities – (temporary)
- English spellings!

iESM - Overview #1



1. Estimating risk by applying standards

- The standard shall at least satisfy following requirements:
  - be widely acknowledged in railway domain. If not the case, the standard will have to be justified;
  - be relevant for control of considered hazards in system under assessment;
  - be publicly available for all who want to use it.

IEEE1474 – thank you

As a minimum, a CBTC system shall address the following critical/catastrophic system hazards through the implementation of the ATP functions defined in 6.1:

a) Train-to-train collisions (rear-end, sideswipe, head-on); hazard to be addressed through train separation assurance (see 6.1.2), rollback protection (see 6.1.4), parted consist protection (see 6.1.6), route interlocking protection (see 6.1.11), and traffic direction reversal interlocks (see 6.1.12)

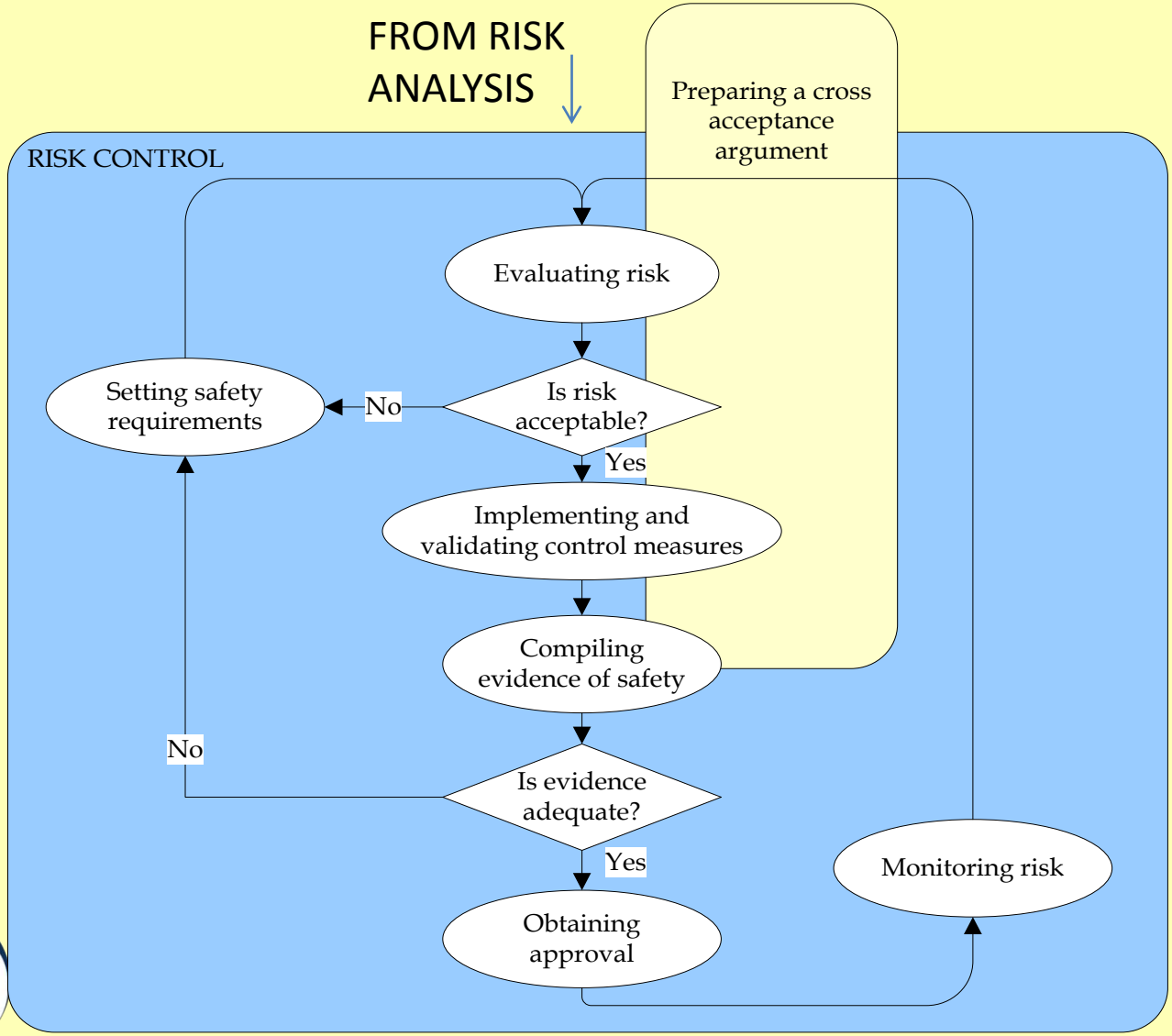
2. Estimating risk by comparing with a reference system

- A Reference System shall at least satisfy following:
  - it has already been proven in-use to have an acceptable safety level and would still qualify for acceptance where change is to be introduced;
  - it has similar functions and interfaces as system under assessment;
  - it is used under similar operational conditions as system under assessment;
  - it is used under similar environmental conditions as system under assessment.

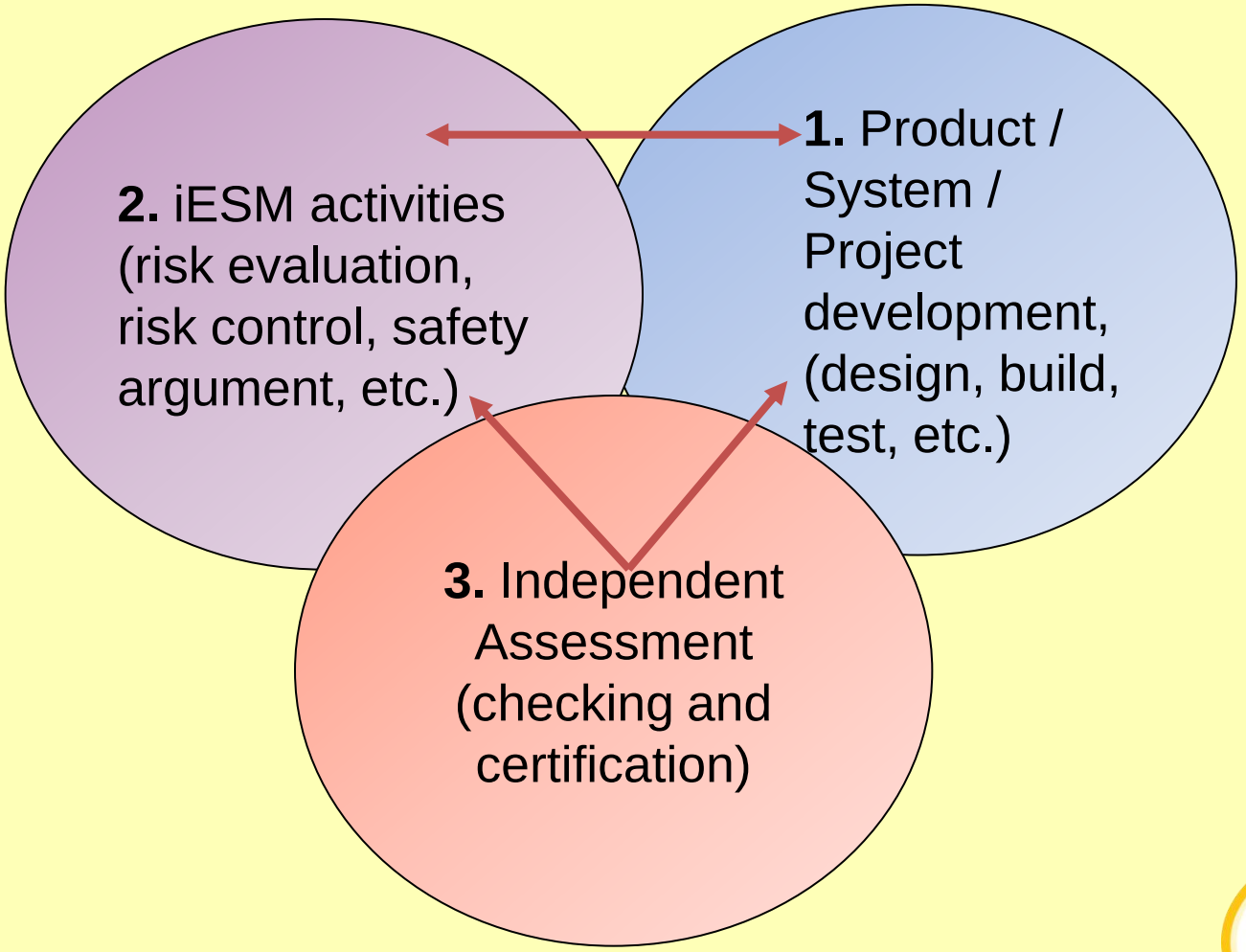
3. Estimating risk by explicit risk estimation

- The need for the use of an explicit risk estimation could typically arise:
  - when the system under assessment is entirely new, OR
  - where there are deviations from a Standard or a Reference System, OR
  - when the chosen design strategy does not allow the usage of a Standard or similar Reference System because e.g. of a wish to produce a more cost effective design that has not been tried before

iESM Overview #2

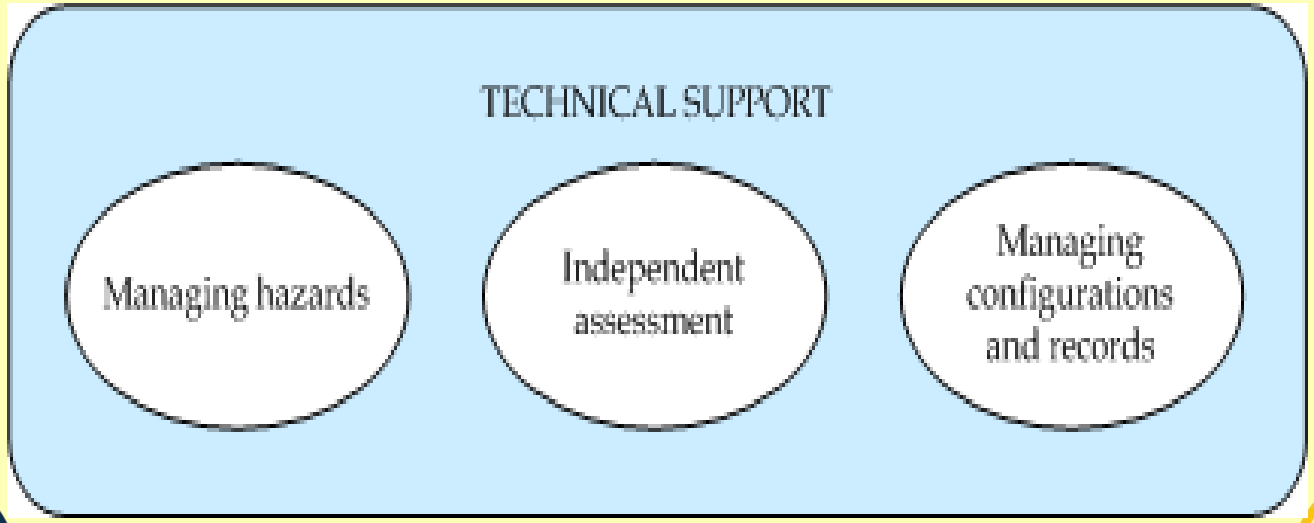


iESM - Risk Control - Summary



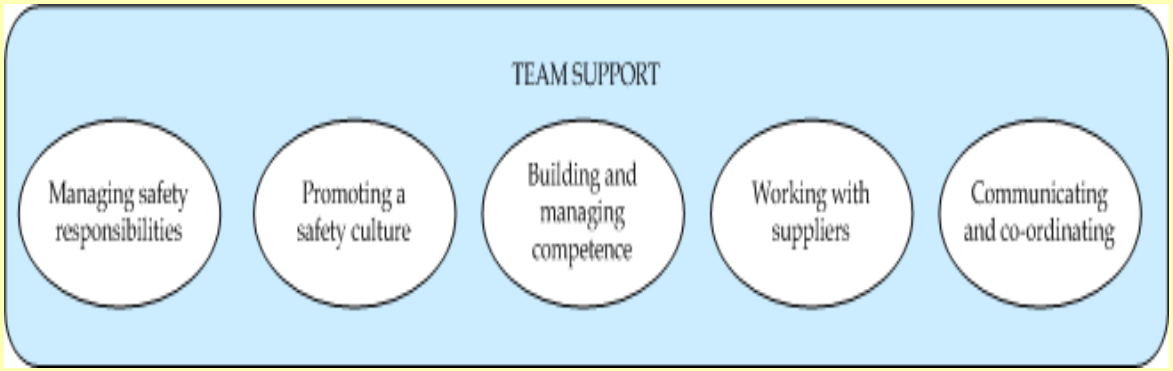
iESM - Technical Support Processes

- Managing hazards
- Independent assessment
- Configuration management & records



iESM - Team Support Processes

- Managing safety responsibilities
- Promoting a good safety culture
- Building & managing competence
- Working with suppliers
- Communicating and co-ordinating



iESM - Business benefits

- Identifying risks early
- Integrated hazard management – three “legs”
- Encouraging consistency and re-use
- Scaling with the problem
- Empowering project managers and supporting users through a common approach and common “language”

iESM - Summary

- Is advisory, not mandatory;
- Provides good practice guidance and will continue to reflect emerging good practice;
- Is applicable in an international market;
- Supports use of CENELEC standards and Common Safety Methods (CSM) for risk assessment, with practical, cost-effective advice;
- Assists in discharging legal & professional obligations;
- Is guided by an international Working Group of practitioners and supporters.

www.intesm.org

A final thought

Absolute safety is not achievable in the real world and therefore success relies on two fundamentals:

1) good processes, and
2) good people;

such that when there is a problem or failure in one, the railway can be sustained by the other.