

**Risk Management & Safety
Asia Pacific Conference**

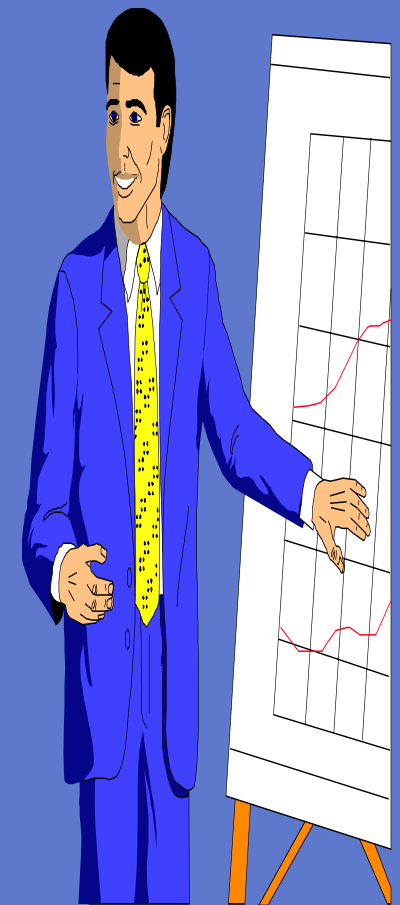
Risk, is there no Reward ?

A G Hessami
Professor of Systems Assurance
Atkins Rail

1-2 Dec. 2005, Hong Kong

Contents & Structure

- ◆ *Definitions*
- ◆ *Systems Safety Concepts*
 - The Legal Requirements
 - International & European Standards
 - The Evolution of CENELEC Standards
- ◆ *Safety Approval Principles*
- ◆ *A Critique of the Current Approaches*
- ◆ *A New Paradigm*
- ◆ *The Way Forward*



Key Definitions





Hazard

A dangerous event, act or state which in the absence of adequate detection, mitigation or control would result in an accident



LOSS

Physical Harm to people, Detriment to a Business or Damage to the Natural Habitat or a combination of



Risk

A forecast for a Future Accident or Loss



Reward

A forecast for a Future Accident or Loss avoided/prevented



Assurance

Increasing Confidence and Certainty



Definitions - 2



Safety

Freedom of people from Harm



System

An inter-related set of Parts / Elements Working to generate a Desired Output



Systems Safety

The Art, Science and Technology of ensuring that a System does not lead to Unacceptable Levels of Harm to people



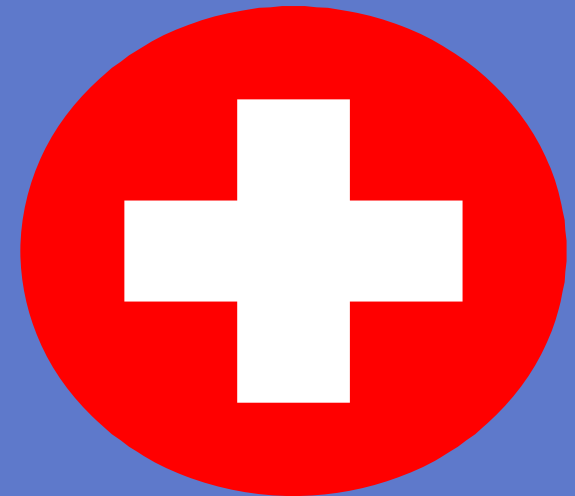
Definitions - 3

Principle :

- ◆ Fundamental Truth or proposition on which many others depend
- ◆ A Fundamental Assumption forming the basis of a chain of reasoning

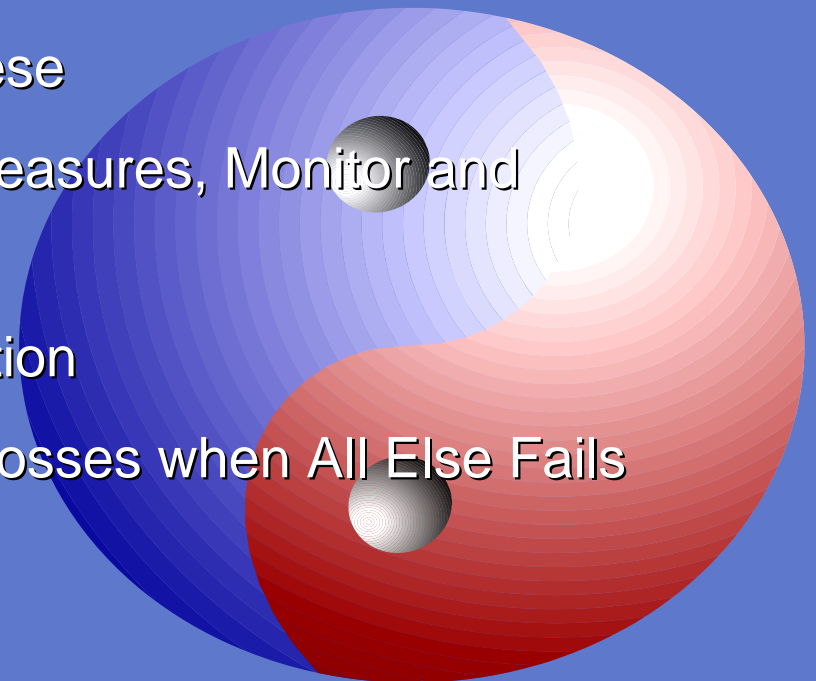


Systems Safety Concepts



Principles :

- ◆ Identify What May Foreseeably Go Wrong
- ◆ Identify Measures to; Eliminate, Reduce, Mitigate or Control the Significant Risks
- ◆ Identify Key Opportunities and Exploit these
- ◆ Plan and Implement the Cost Effective Measures, Monitor and Review Assumptions & Performance
- ◆ Ensure Sufficient & Competent Organisation
- ◆ Develop Contingency Measures to limit Losses when All Else Fails



Facets of Performance

- ◆ Functional/Technical
- ◆ Commercial
- ◆ Environmental
- ◆ Integrity (RAM)
- ◆ Safety & Security
- ◆ Quality &
- ◆ Perceived Value



European & International Safety Standards

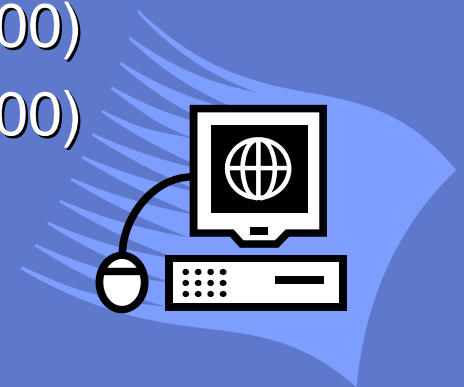


Safety Standards - International

IEC 61508, E/E/PES Functional Safety

◆ Comprises 7 Key Parts

- | | |
|--|--------|
| 1 - General Requirements | (98) |
| 2 - Requirements for E/E/PES | (2000) |
| 3 - Software Requirements | (98) |
| 4 - Definitions and Abbreviations | (98) |
| 5 - Examples of Methods for SIL Allocation | (98) |
| 6 - Guidelines on Application | (2000) |
| 7 - Bibliography | (2000) |



CENELEC Standards - 1

◆ EN50126 (IEC62278)

Railway Applications - Reliability, Availability, Maintainability and Safety

◆ EN50128 (IEC62279)

Railway Applications – Communications, Signalling & Processing Systems, Software for Railway Control & Protection

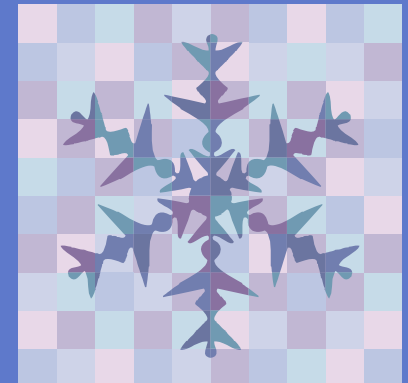
◆ EN50129

Railway Applications - Safety Related Electronic Systems for Signalling



EN50126 – System Life Cycle

1. **Concept**
2. **System Definition and Application Conditions**
3. **Risk Analysis**
4. **System Requirements**
5. **Apportionment of System Requirements**
6. **Design and Implementation**
7. **Manufacture**
8. **Installation**
9. **System Validation (Including Safety Acceptance and Commissioning)**
10. **System Acceptance**
11. **Operation and Maintenance**
12. **Performance Monitoring**
13. **Modification and Retrofit**
14. **De-commissioning and Disposal**



EN50126 Activities

- ◆ A Working Group WG8 set up Dec. 2002
- ◆ Aimed at developing guidance for application
- ◆ Three areas being addressed
 - ◆ Requirements & Apportionment
 - ◆ Modelling & Assessment
 - ◆ Compliance & Certification



TC9XA – WG8 Structure

- ◆ WP1: Leader Richard Imhoff
- ◆ Items in the WP 4, 5 & 6
- ◆ Members: Wouter (BE), Dupoux (FR), Reif (DE), Carpignano (IT), Impallomeni (IT)

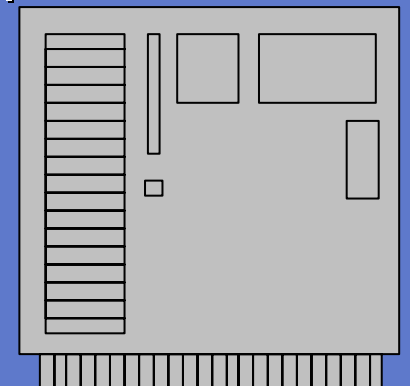
- ◆ WP2: Leader Ali Hessami
- ◆ Items in the WP 1, 2, 7 & 9
- ◆ Members: Møller (DK), Garnier (FR), Shult (DE), Sundvall (SE), Halbritter

- ◆ WP3: Leader Gunhild Halvosrud
- ◆ Items in the WP 3 & 8
- ◆ Members: Alran (FR), Foschi (IT), de Graaf (NL), Kwasnicki (CH)



EN50129 Activities

- ◆ A Working Group WGA2-3 set up Nov. 2003
- ◆ Mainly aimed at developing process for Cross-Acceptance
- ◆ Held many sessions with 3 workpackages
 - ◆ WP1- Cross Acceptance Process
 - ◆ WP2 – Technical Safety Report
 - ◆ WP3 – General Guidance of Qualitative vs Quantitative etc.
- ◆ Developing general guidance on 129 Application areas



EN50128 Activities

- ◆ A Working Group WGA11 set up by SC9XA June 2005
- ◆ Mainly aimed at Review & Update
- ◆ Convenor Ali Hessami/UK
- ◆ Planned to Hold Preliminary Session in Q4 2005
- ◆ Developing general guidance on 128 Application areas



EU regulatory structure

- ◆ Defining the responsibilities of the actors
 - Infrastructure managers
 - Railway undertakings
- ◆ Establishing National Authorities for regulation and supervision of safety
- ◆ Migration strategy for safety rules



EU - A Common Approach

- ◆ New provisions for safety certification
 - a Community valid part
 - a National part
- ◆ Requirements on Safety Management Systems
 - Article 9 of Safety Directive
 - Future European standard on railway SMS?
- ◆ Common Safety Targets (CST),
- ◆ Common Safety Methods (CSM)
- ◆ Common Safety Indicators (CSI)



EU - Safety Performance

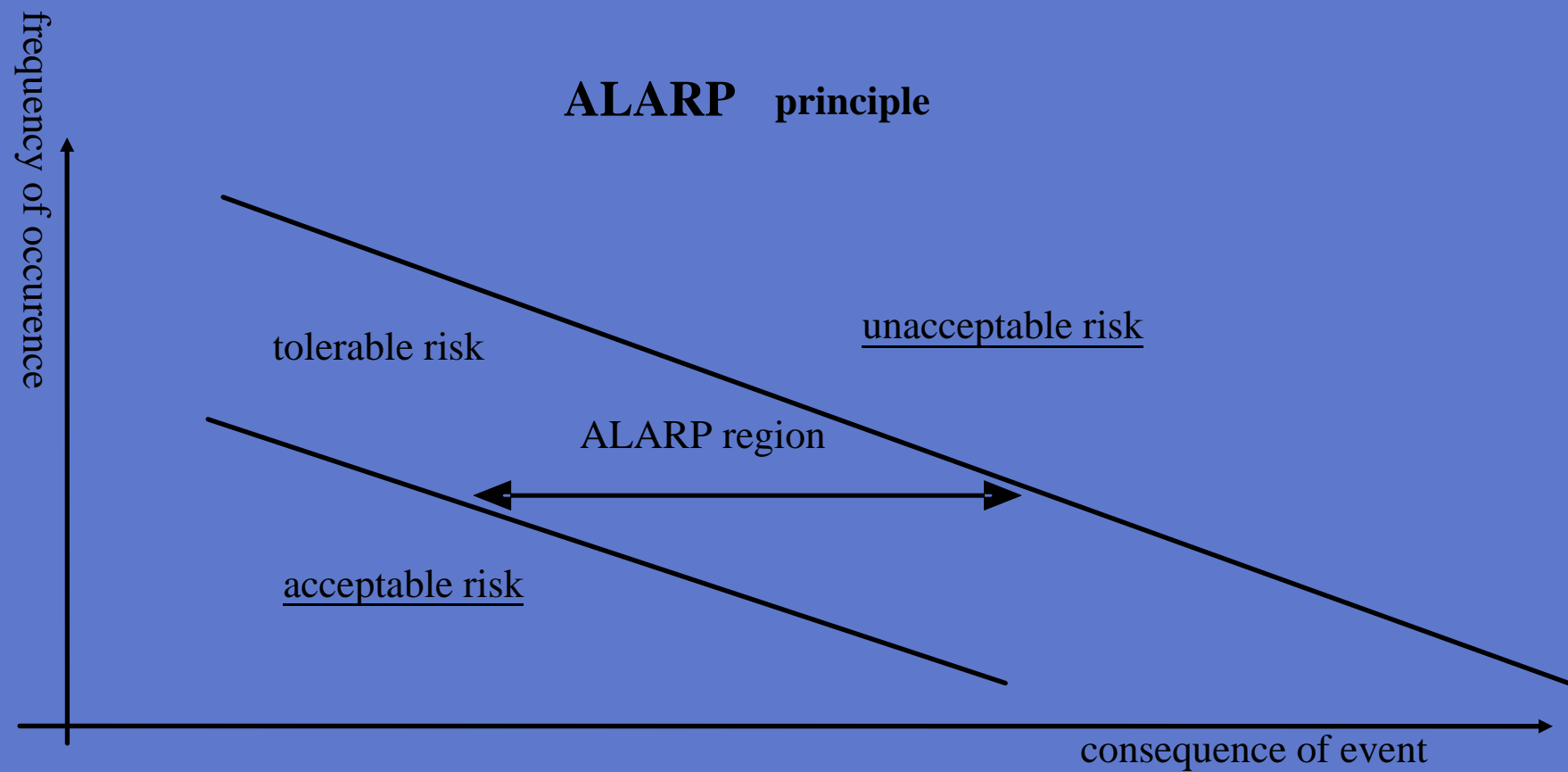
- ◆ CST and CSM gradually introduced to ensure;
 - a high level of safety is maintained
 - when & where necessary and reasonably practicable, improved.
- ◆ They should provide tools for
 - assessment of the safety level &
 - the performance of the operators
- ◆ Focus at European level & Member States.



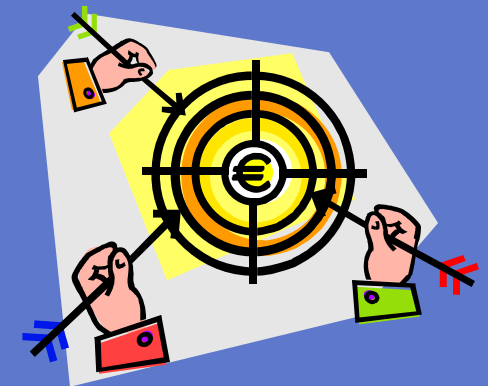
Safety Principles & Compliance



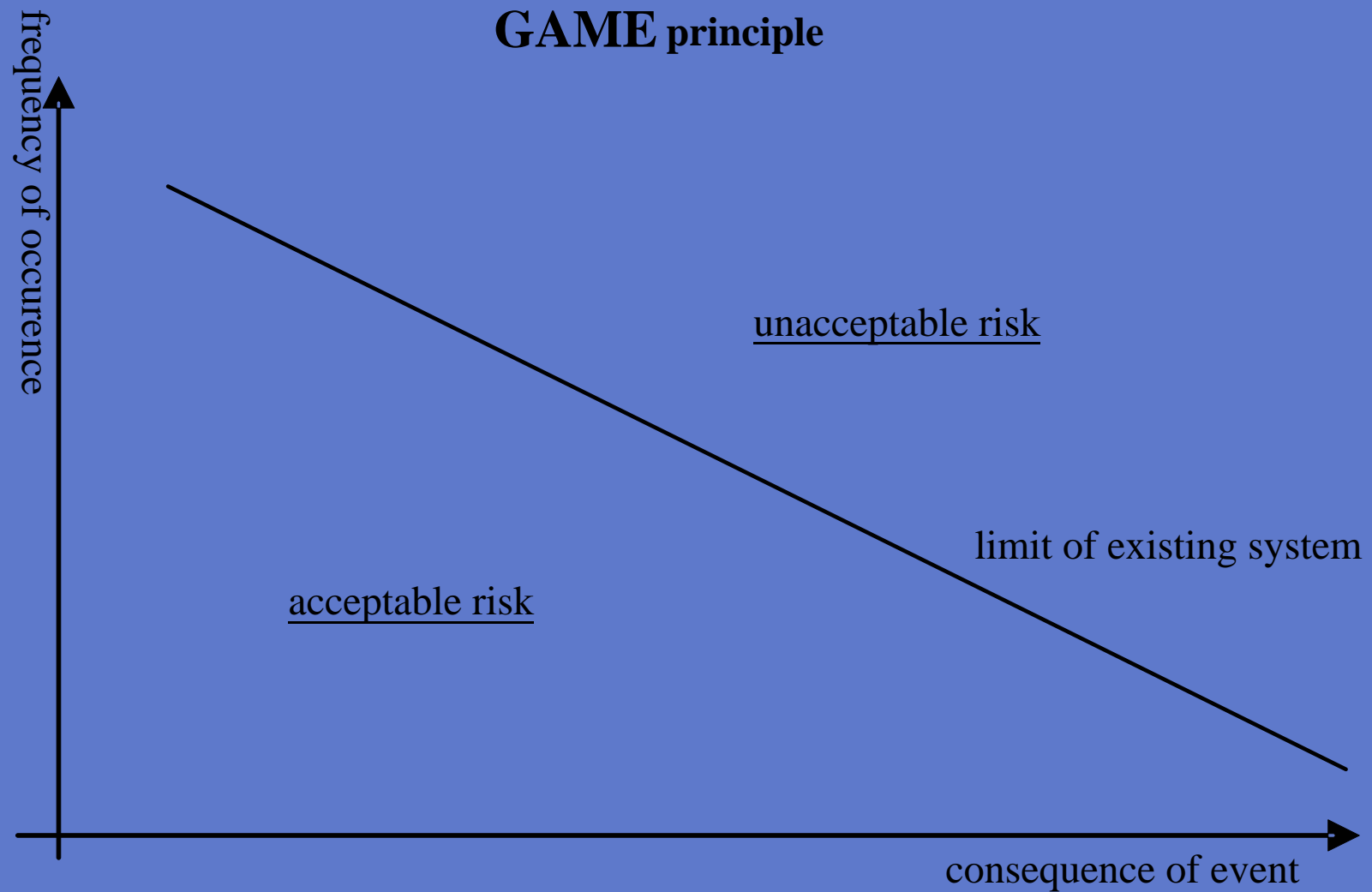
Compliance Frameworks - UK



- ◆ The upper risk domain where mitigation actions must be taken.
- ◆ The middle risk domain where mitigation actions are evaluated using cost/benefit analyses with a view to reduce or maintain risk levels.
- ◆ The lower risk domain where the risks are accepted with no further reduction required other than maintaining risk levels.
- ◆ The Concept of Gross-disproportionality for justification

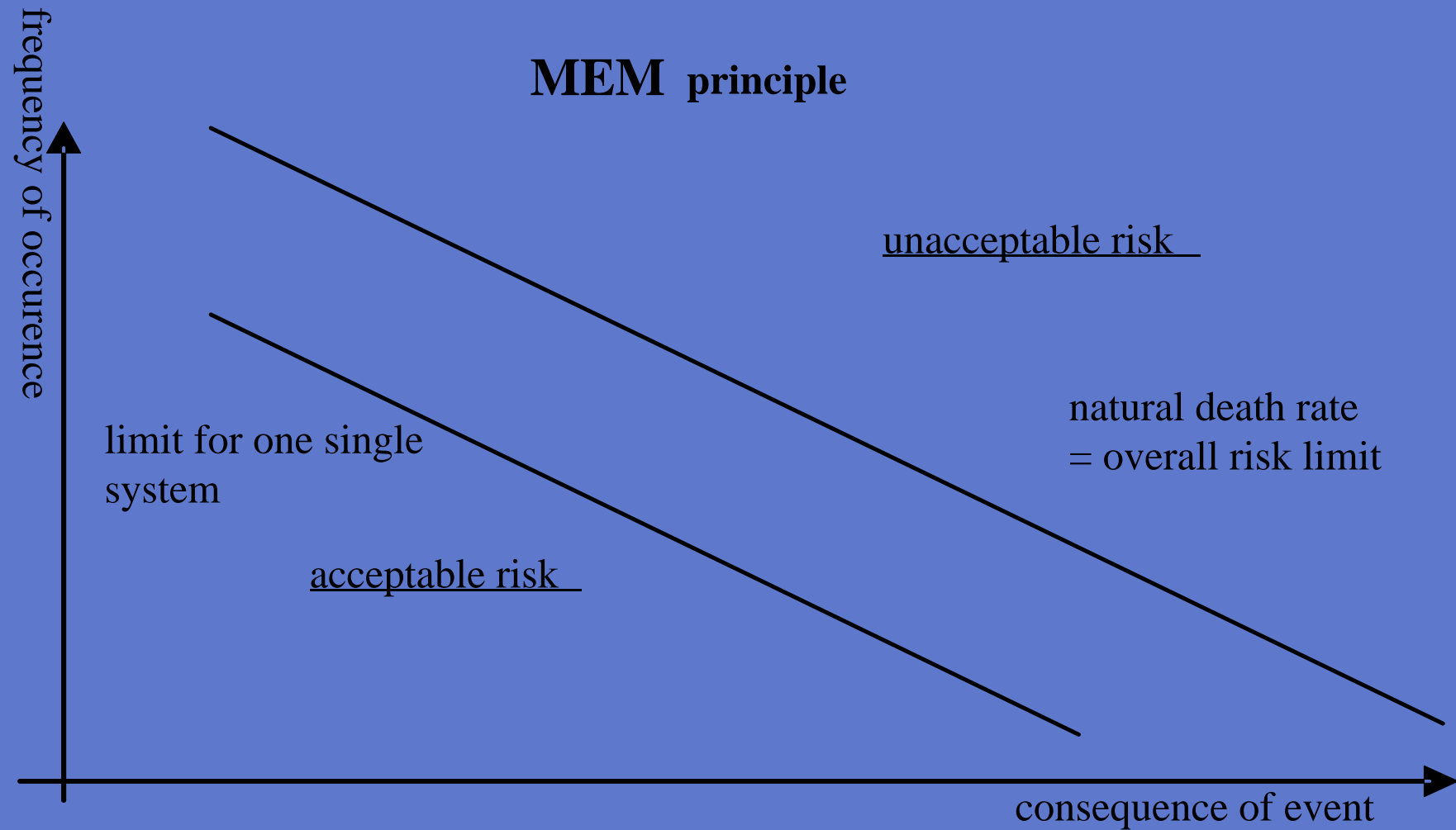


Compliance Frameworks - France



- ◆ *The system under consideration can be compared to an equivalent reference system.*
- ◆ *A clear system boundary can be defined for both new and reference system.*
- ◆ *The properties relevant to the risks considered are known for both the new as for the reference system.*
- ◆ *Any differences in properties need to be compensated for in the setting of risk targets or demonstration of compliance.*





- ◆ In the range 5 - 15 years the natural death rate (R_m) reaches a minimum for individuals:

$$R_m = 2 * 10^{-4} \text{ fatalities/person*year}$$

- ◆ Additional overall hazard death rate caused by technical systems (R_t) shall not exceed this limit

- ◆ Each single system shall not contribute more than 5%

- ◆ Each individual is endangered by n different technical systems in parallel; the assumption in the MEM principle is: $n \leq 20$

- ◆ A single technical system shall not lead to a risk of fatality (R) of a single person with a rate of:

$$R \leq 10^{-5} \text{ fatality/person*year}$$

- ◆ A railway system can be considered as such a technical system.



1) Consideration of correct duration time

- ◆ Exposure time to each possible hazard in reality.

2) Consideration of correct number of persons

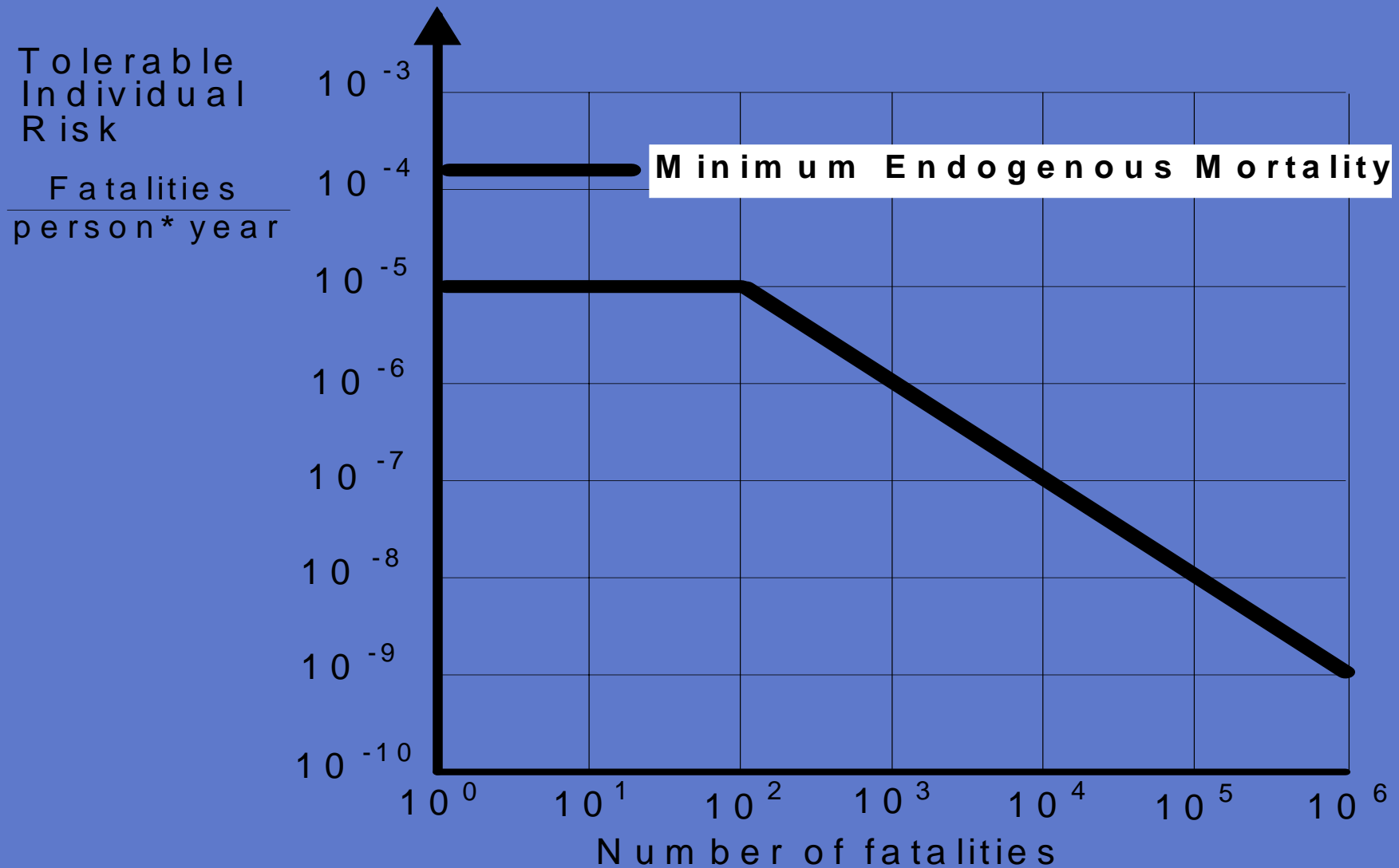
- ◆ For each hazard the number of persons exposed

3) Consideration of correct number of fatalities

- ◆ All fatalities arising from accident/incidents of the system



MEM – Differential Risk Aversion



Safety Principles A Critique



A Critique

- ◆ Focused on Risk
- ◆ Adversarial - only Degrees of Guilt
- ◆ Non-Systemic with Application Difficulties
- ◆ Not based on Fair Balance of Good & Harm
- ◆ Blindly Adopted & Followed by others
- ◆ Misapplied by Many
- ◆ Often Employed as an Excuse for Inaction
- ◆ Misunderstood/Abused in IEC & CENELEC in Matrices
- ◆ Cost used as the Key Measure of Sacrifice



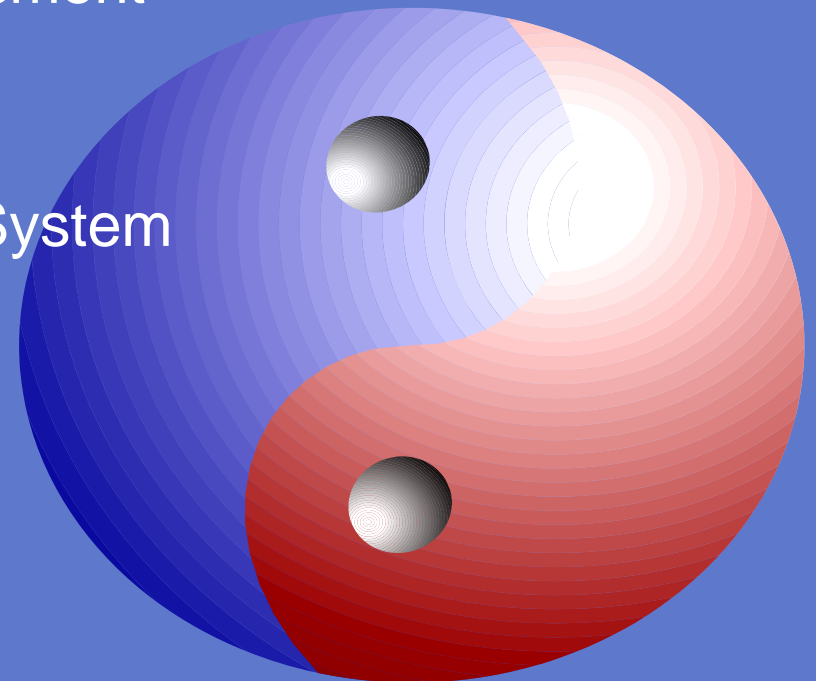
A New Paradigm ?

ATKINS

General Characteristics

- ◆ Systemic & Holistic
- ◆ Fair Balance of Impact
- ◆ Clarity of Satisfaction Criteria
- ◆ Empathic with Ease of Application
- ◆ An Advanced Framework for Assessment
- ◆ Requires A Responsive SMS
- ◆ Overhaul of the Legal Framework ?
- ◆ Better Assessment of a Reference System

- ◆ Are we Up for it?



Safety Cases



EN50129 Requirements



Conditions for Safety Acceptance & Approval:

◆ A Safety Case comprising

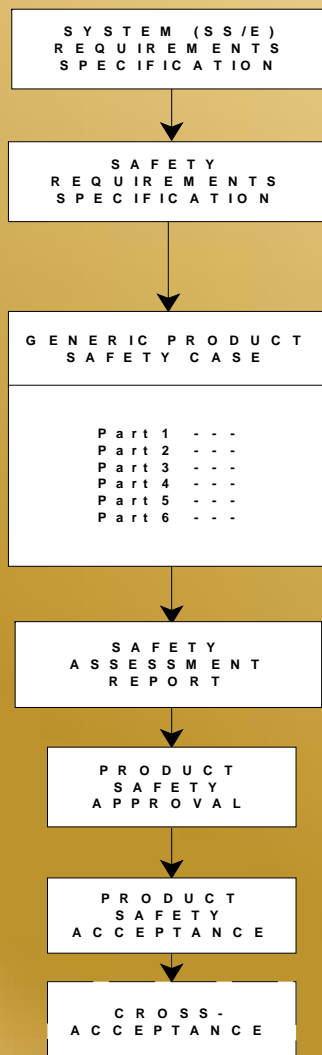
- ◆ *System Definition & Scope*
- ◆ *Evidence of Quality Management*
- ◆ *Evidence of Safety Management*
- ◆ *Evidence of Functional and Technical Safety*
- ◆ *Supporting Safety Cases*
- ◆ *Conclusions*



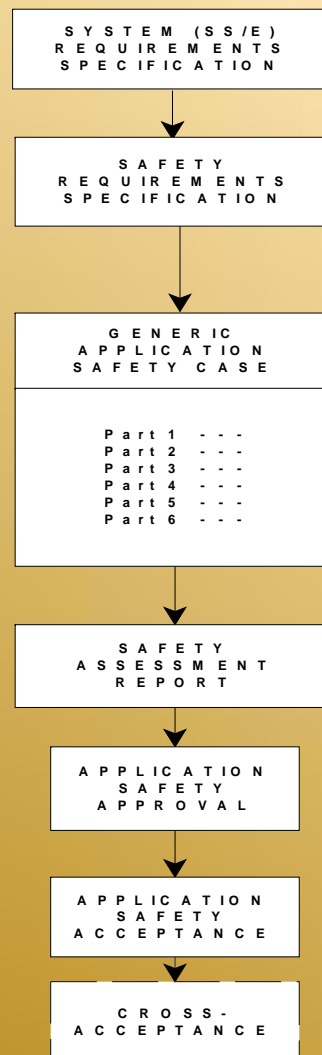
Safety Acceptance & Approval



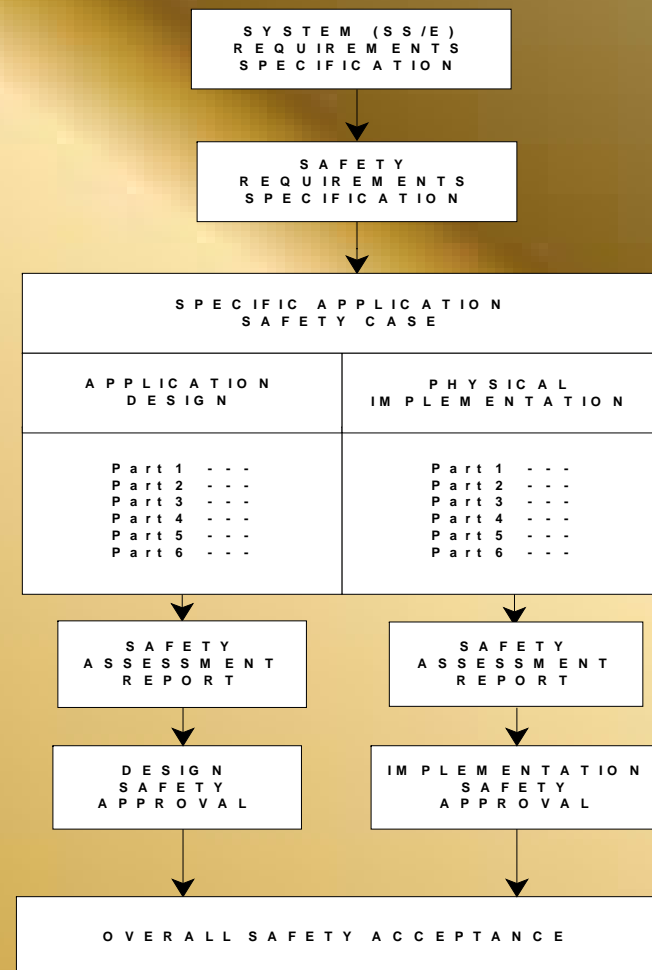
GENERIC PRODUCT (Independent of Application)



GENERIC APPLICATION (Class of Application)



SPECIFIC APPLICATION



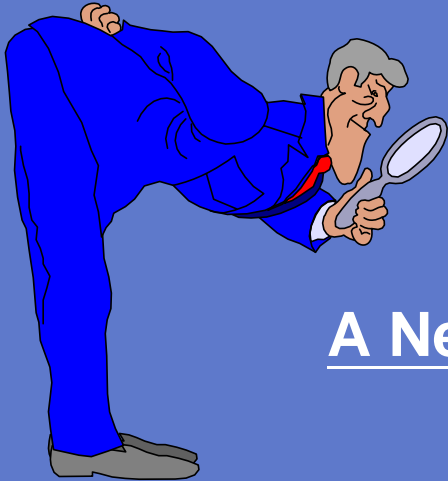
Safety Principles A New Approach ?



Basic Premise

- ◆ Most Endeavours are Purposeful
- ◆ Majority aim for betterment
- ◆ Could introduce new Hazards
- ◆ Safety Approach fundamentally Adversarial
- ◆ Most Products & Systems Improve Aspects of Performance
- ◆ Need a New Balanced Approach to Safety





A New Paradigm is Called for

- ◆ Improving Safety Approvals
- ◆ Enhancing Consistency of Approach
- ◆ Establishing Beneficial & Detrimental Facets
- ◆ Forecasting a Total Behavioural Risk Profile

Risk & Reward Analysis (RaRA)

- ◆ Define the product, system
- ◆ Identify Problems associated with its application
- ◆ Derive Safety Hazards arising from the Problems
- ◆ Assess the risks from Hazards

- ◆ Identify the Benefits associated with its Application
- ◆ Derive Safety Opportunities arising from the Benefits
- ◆ Assess the Rewards from Opportunities

- ◆ Assess total Risk and Reward contributions
- ◆ Establish the Total Profile

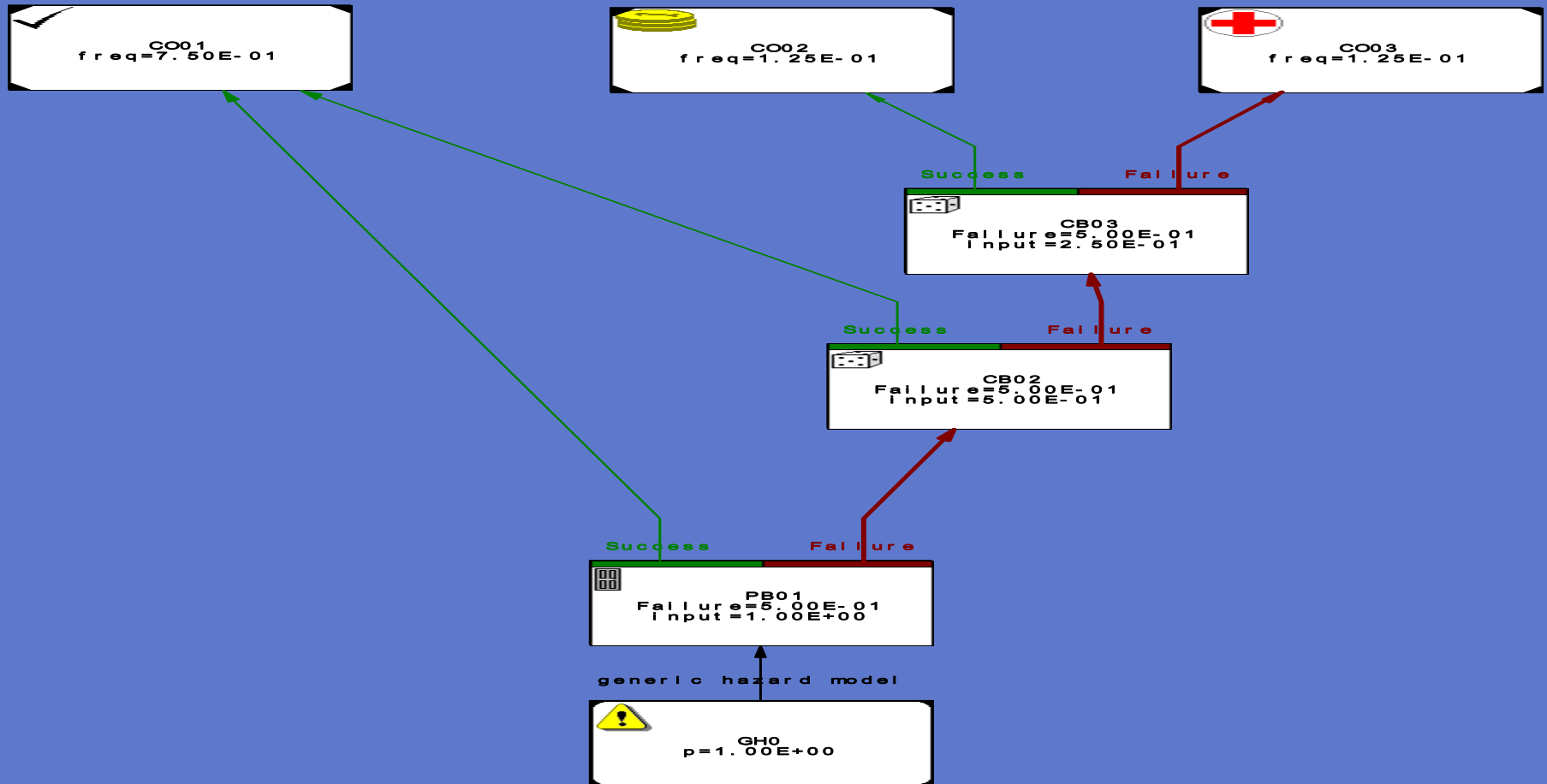


RaRA Constituents - 1

ISAE V07.07.003
Consequence (1/2)
Worksheet 1
Created On: 26/10/2002
Last Accessed On: 15/05/2003
Issue/Draft: 1.0

Hazard: SDOGH0 : Generic hazard model for qualitative eval
Project: MSCIP-SDO : Ansaldo SDO Signal Problem
Author: THE ADMINISTRATOR
Last Accessed by: THE ADMINISTRATOR
Panel:

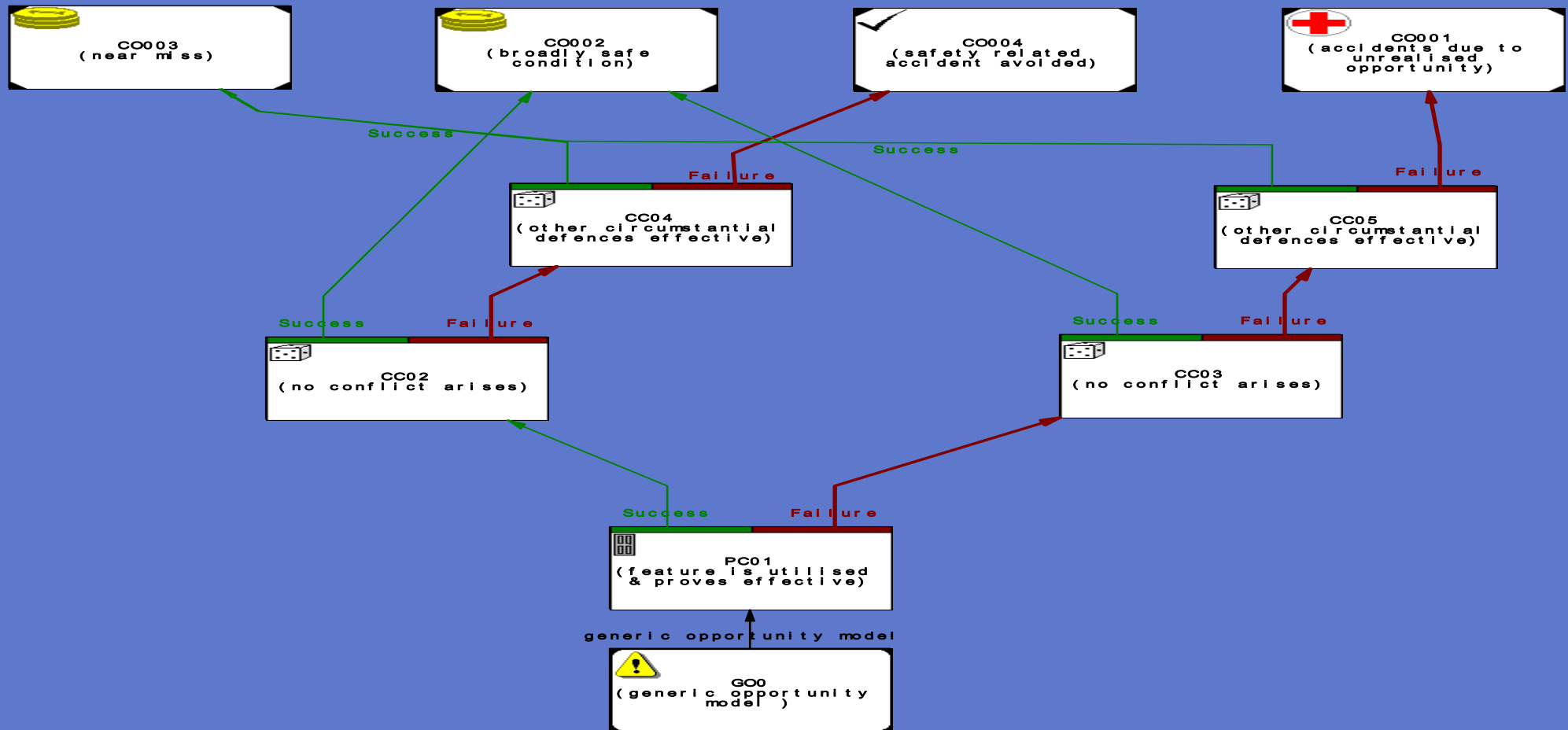
Generic Hazard Model



RaRA Constituents - 2

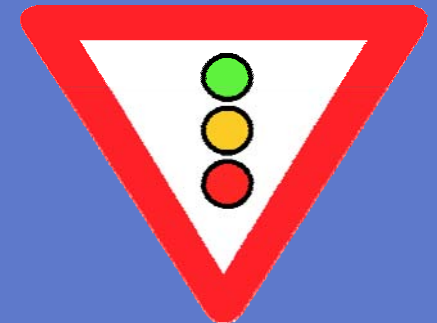
ISAE V07.07.003	Hazard: SDOG00 : Generic class of differential opportunities
Consequence Model	Project: MSCIP-SDO : Ansaldo SDO Signal Problem
Worksheet 1 C	Study
Created On: 27/10/2002	Author: THE ADMINISTRATOR
Last Accessed On: 15/05/2003	Last Accessed by: THE ADMINISTRATOR
Issue/Draft: 1.0	Panel:

Generic Opportunity Model



Applied to two Difficult Problems

- ◆ Safety Acceptance of a new Signal Head
- ◆ Safety Argumentation of Axle Counters



Axle Counters vs Track-Circuits – Options

- ◆ Full scale and independent study of Track-circuit and Axle Counter safety performance to contrast the risk profiles
- ◆ *Differential and full safety study of the Axle Counters risks and rewards baselined against Track-circuits*
- ◆ Detailed scrutiny of the loss of broken rail detection issue in the project



The plan for the study comprises three key stages;

- ◆ Identification/review of the Problems and associated hazards
- ◆ Identification of the Beneficial aspects and associated Opportunities
- ◆ Qualitative yet numerical evaluation of the Hazards and Opportunities based on expert judgement



AXC classes of Problems Compared with Traditional TC

<i>Ref</i>	<i>Description</i>	<i>Observations</i>
P1	Discontinuous train detection	Track circuits are designed to continuously detect the presence of a train throughout its transition through the track section. In contrast Axle Counters merely detect the train entering and leaving the track section.
P2	Increase fixture of axle counter heads to the line	The additional need to drill the rail to affix the axle counter heads to it. This is countered to an extent by the removal of the need to make track circuit connections to the rail. See benefit B14
P...	Possession spanning across TC and AXC sections	There may be additional risk associated with the management of possessions which span the interface between track circuited and axle counter sections of line.
P18	Losing potential detection of major arcing	There is a potential for gross traction arcing to be detected by track circuits by the rupturing of track circuit fuses etc. This feature is lost when axle counters are introduced.

Axle Counter Problems potentially causing Safety Hazards

<i>Item</i>	<i>Ranking</i>	<i>Ref.</i>	<i>Cause/Scenario</i>	<i>Hazard</i>
1	M	P1/H1	Train derailed and wreckage fouls the adjacent line, in a manner which would have caused a TC to operate WSF occurs (The differential hazard is that the WSF may be present for longer, as it does not have a tendency to self rectify as in the case of Track circuits)	Obstruction not detected
2	M	P1/H2		Section shown clear when occupied for longer due to WSF of AXC.
...	L	P17/H1	Different procedures for AXC and TC (Ranked “L” on the basis of likely familiarity of staff with locality)	Some one not realising correct procedure, more staff present at track side to correct the error. (exposed to possibility of failure of protection)

Axle Counter Beneficial Features

<i>Ref</i>	<i>Description</i>	<i>Observations</i>
B1	Increased reliability	There is an expectation that axle counters will prove to be significantly more reliable than track circuits
B2	Removed IBJ	The elimination of track circuits will enable the removal of insulated block joints, which are an inherent weakness in the structure of the rail.
...	Rail break will not cause WSF	With track circuits, rail breaks in combination with other failures can cause wrong side track circuit failures.

AXC Features Differentially Contributing to Safety

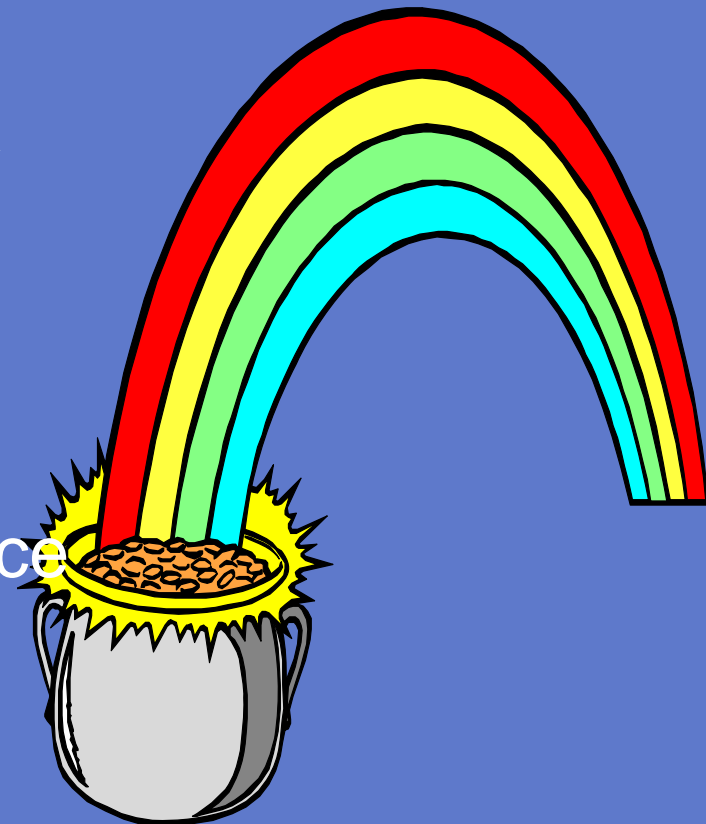
<i>Item</i>	<i>Ranking</i>	<i>Ref.</i>	<i>Cause</i>	<i>Opportunity</i>
1	H	B1/O 1	Fewer failures of AXC, resulting in less degraded mode of signalling	Less human error through hand-signalling etc., security of interlocking preserved at all times
2	H	B1/O 2	Fewer failures of AXC	Fewer staff at track side fault finding, and hence less red zone working (exposed to possibility of failure of protection)
...	L	B20/ O1	Parallel bonding	Preserve the integrity of interlocking system
29	-	B21/ O1	Short physical length of a scheme	Greater design flexibility

- ◆ Assess Risks arising from Hazards
- ◆ Assess Rewards arising from Opportunities
- ◆ Determine the net Balance
- ◆ Present an Objective case for Decision Support



The Way Forward

- ◆ Adopt a Systemic Perspective
- ◆ Go beyond Cause and Consequence
- ◆ Ensure Whole Life-cycle is Addressed
- ◆ Exploit Creativity in Tackling Complexity
- ◆ Address Risks & Rewards
- ◆ Employ an Objective Framework
- ◆ Make Informed Decisions on Performance
- ◆ Deploy Opportunities for Enhancements



Questions ?

ATKINS



Contacts

ATKINS

Ali.Hessami@AtkinsGlobal.Com

A.G.Hessami@IEEE.Org

WWW.ESSS.ORG