

CEMSIS

FIKS-CT-2000-00109

Cost-Effective Modernisation of
Systems Important to Safety

Robin E Bloomfield
Adelard

Professor of System and Software Dependability
Director, Centre for Software Reliability
Founder Adelard LLP
reb@adelard.com

Drysdale Building, City University, London EC1V 0HB
Tel: +44 20 7490 9450 (sec Adelard)
Tel: +44 20 7040 8420 (sec CSR)

CEMSIS

Overview of talk

- a quick tour through Cemsis
- the Public Domain Example
- cost modelling and lessons learnt

A quick tour



CEMSIS Objectives

- Programmable Instrumentation and Control (I&C)
 - safety systems (e.g. protection)
 - safety-related systems (e.g. control, data presentation)
- Common approach to development and safety justification
 - maximise safety
 - minimise cost
- Modernisation/Refurbishment
 - analogue/discrete logic replacement with computer-based systems

Participants in CEMSYS

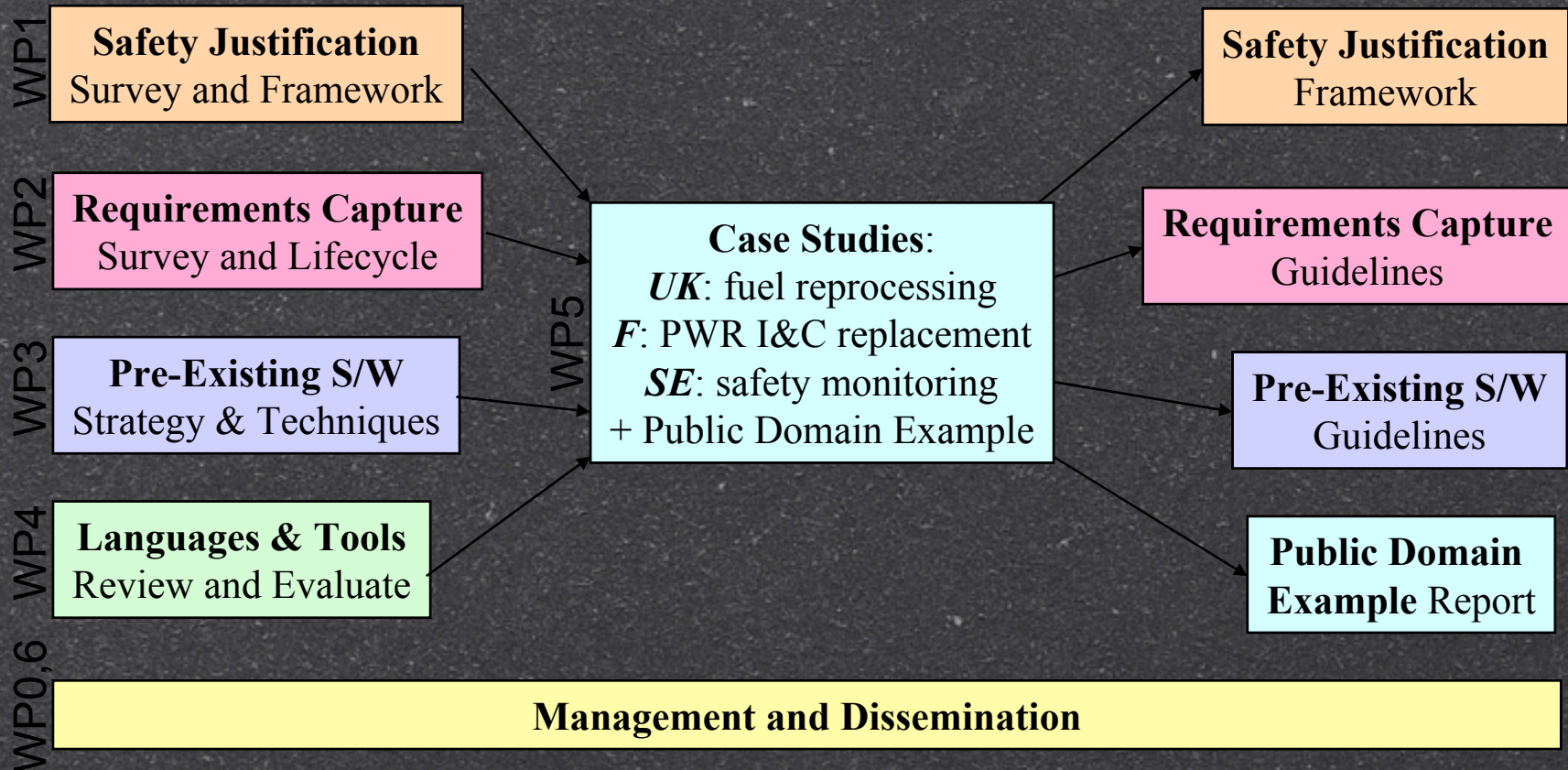


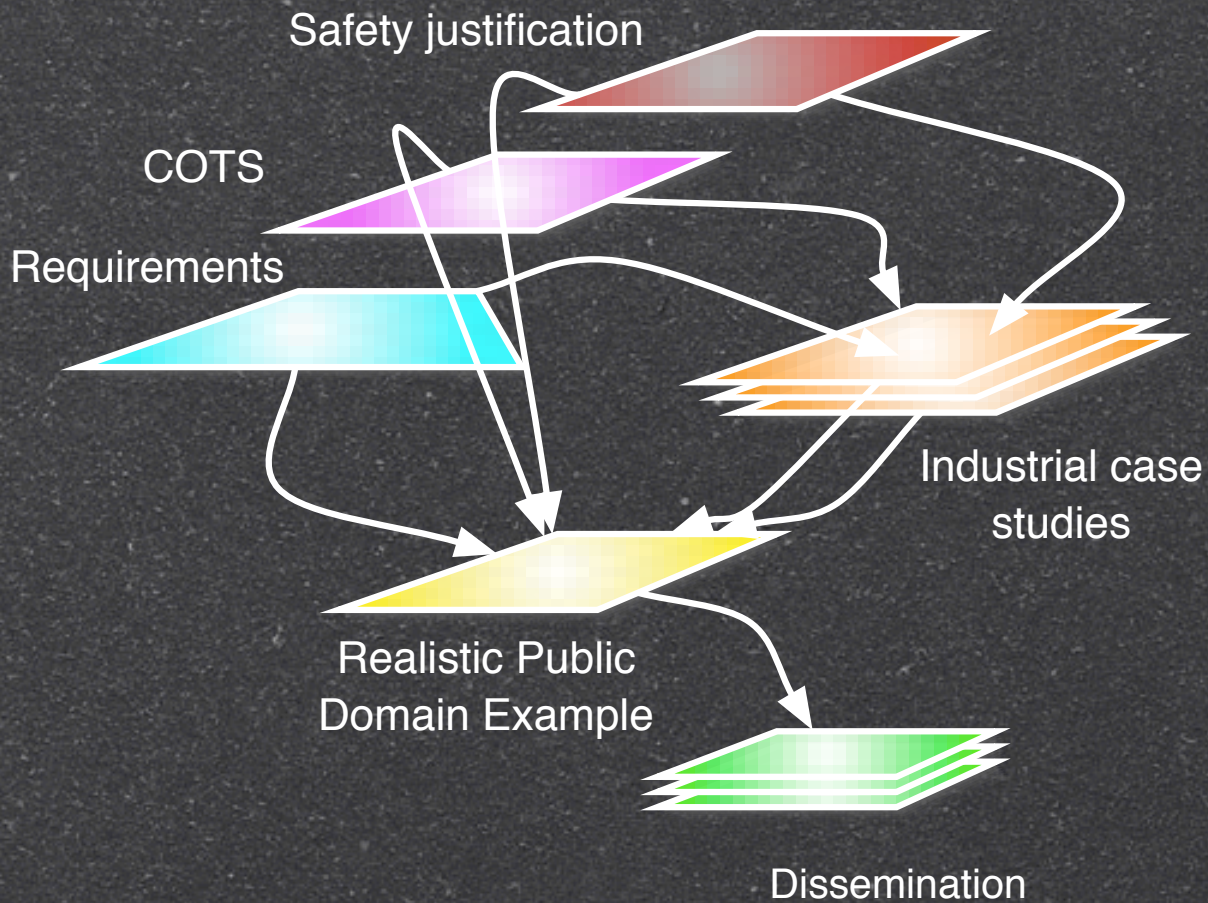
Key Issues

- Harmonisation & Structuring of Safety Justification approaches
- Definition of Requirements for Systems Important to Safety
- Use of Pre-Existing Software in Systems Important to Safety
 - potentially including class A systems
- Use of Languages & Tools in Systems Important to Safety

Reflected in Work Package Structure

Work Packages and Deliverables





Application and Evaluation

■ Case Studies:

- UK Nuclear fuel reprocessing plant control BNFL
- I&C replacement on a French PWR EDF
- Safety monitoring system on a Swedish NPP CarlBro
- Public domain nuclear material transport example Adelard

■ Identify safety and cost-relevant aspects

- safety requirements
- implementation options
- example arguments for safety justification

■ Evaluate and refine guidance documents

Three key work packages

Safety Justification Framework

- Take account of current EU experience
 - EC NRWG Task Force on Safety Critical Software (ARMONIA)
 - Survey shows no systematic method used in Member States
- Pragmatic framework for cost-effective safety justification
 - Elicit and organise disparate claims and evidence
 - Allow modularity and reuse of elements of previous cases
 - Deal with system models at different levels:
 - plant: hazards/threats identified in a valid manner
 - architecture and design: SIS correctly implements safety function
 - operation: SIS behaviour remains valid

claims

0: initial claim

1: plant-SIS interface

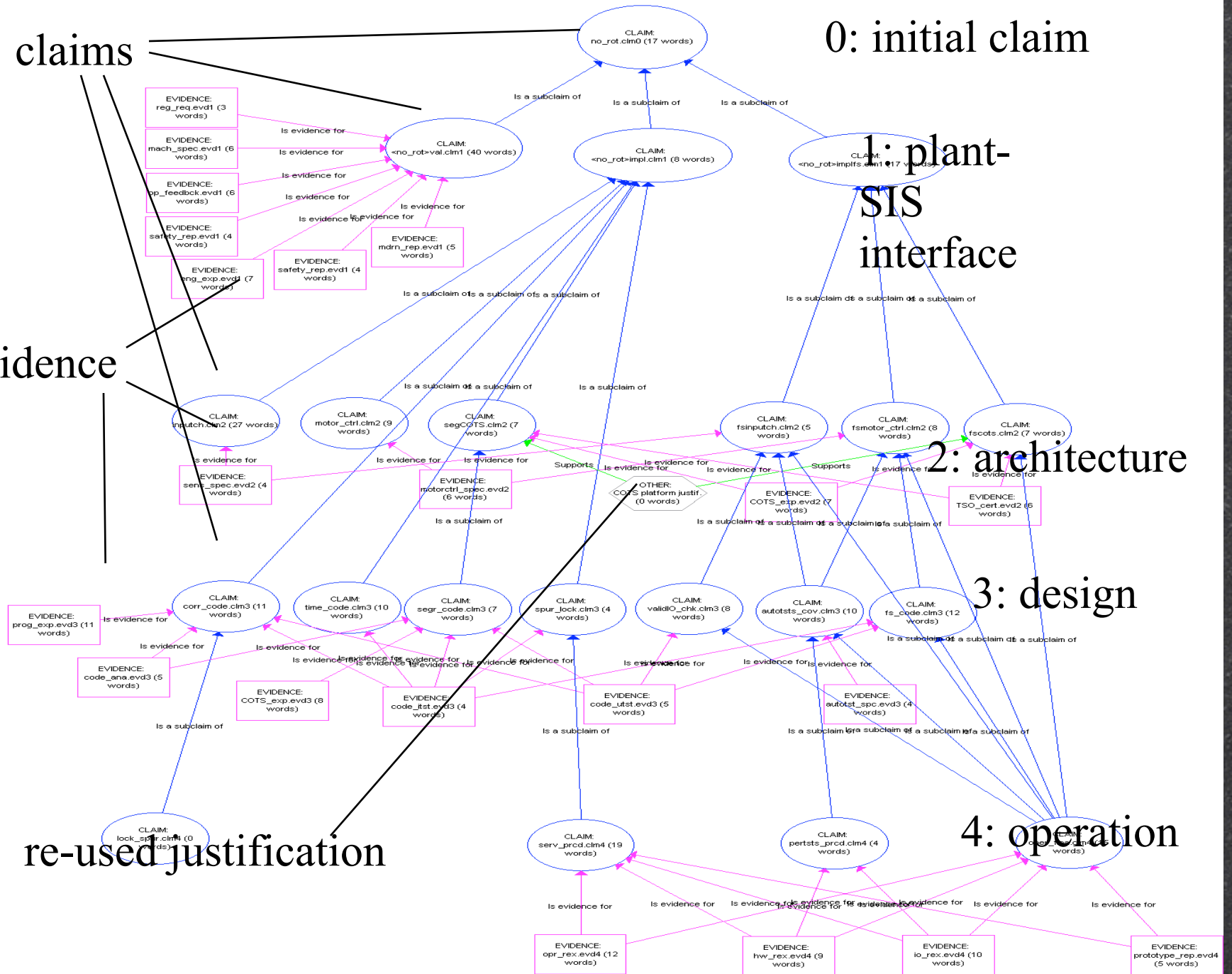
2: architecture

3: design

4: operation

evidence

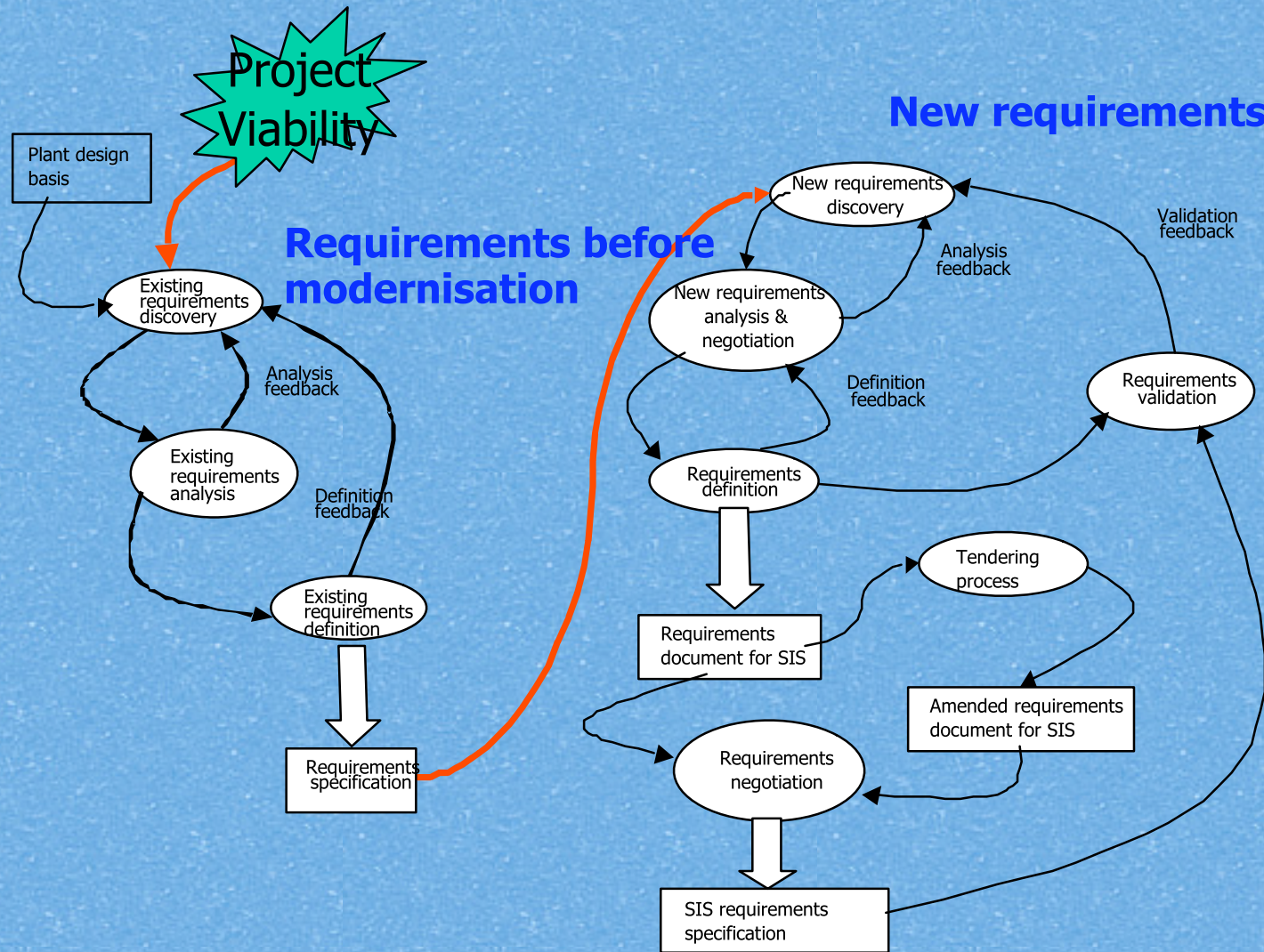
re-used justification

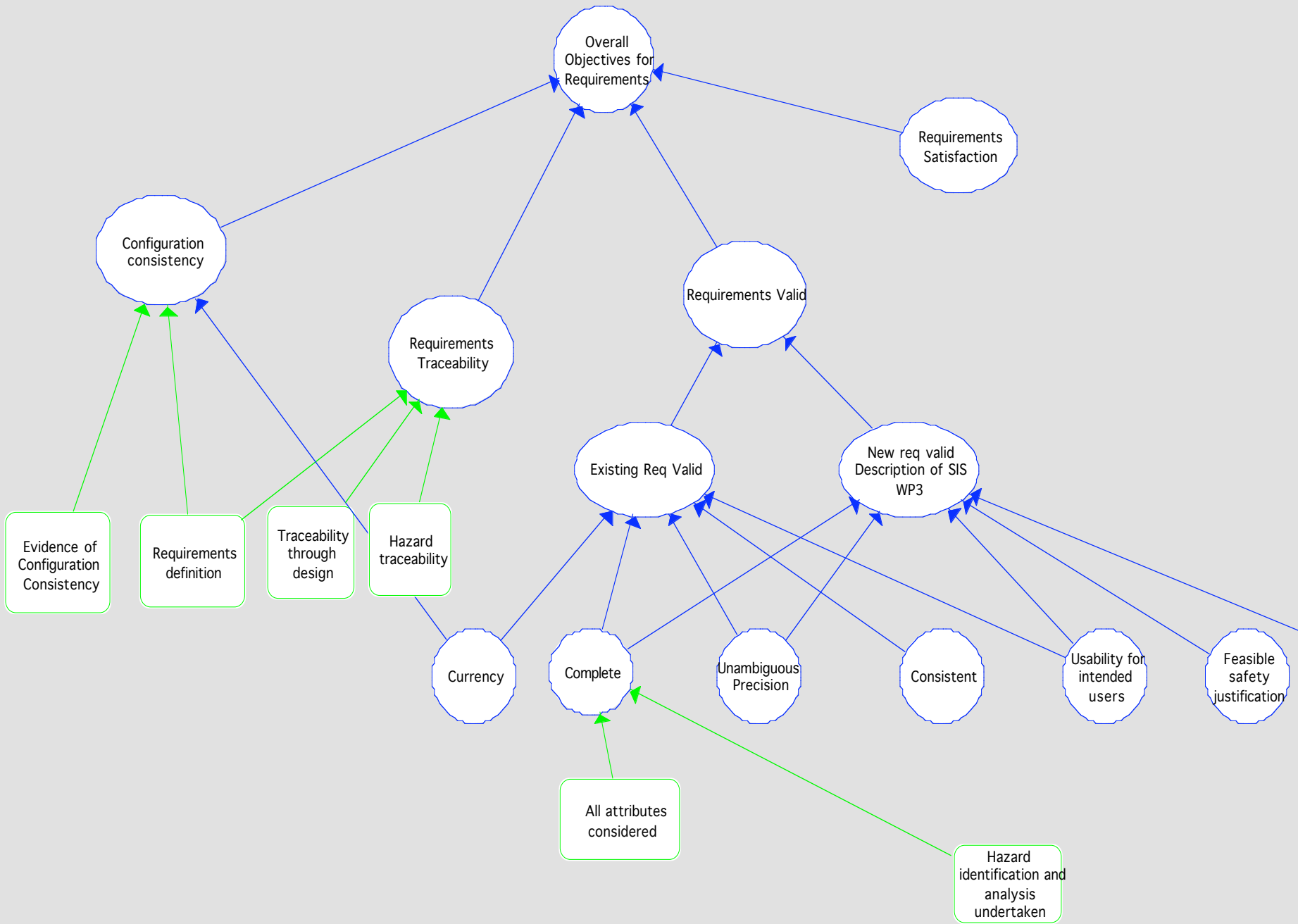


Requirements Capture

- Survey of requirements techniques, research and experience.
 - 84 available techniques identified & classified
 - in current use: interviews, documents, reviews, checklists
- Requirements process for refurbishment guide
 - requirements engineering process - 'modernisation oriented'
 - claim-based view - link to safety justification framework
 - set of stakeholders or viewpoints - completeness

Requirements Process





Pre-existing Software

- Including “COTS” (Commercial Off The Shelf)
- Strategy: Two phases
 - “Pre-qualification” - reduce uncertainty and delay
 - provide evidence in advance for all applications
 - Application Qualification - some always needed
 - provide evidence specific to one application
- Types of assessment
 - Functional - ensure features of product are adequate for safe use
 - Dependability - evidence that the product is sufficiently reliable
 - taking account of its safety class

		white-box	grey-box	black-box		
		experience in operation				
criticality complexity		no	yes	no	yes	no
Class A	high	A-WB				
	med	A-WB	A-BB			
Class B	high	B-GB				
	med	B-GB		B-BB		
	low	B-GB		B-BB		

◆ Properties essential to safety:

- characterisation
- functional adequacy
- correctness
- robustness
- maintenance

**Partially
addressed during
pre-qualification**



The Public Domain Example

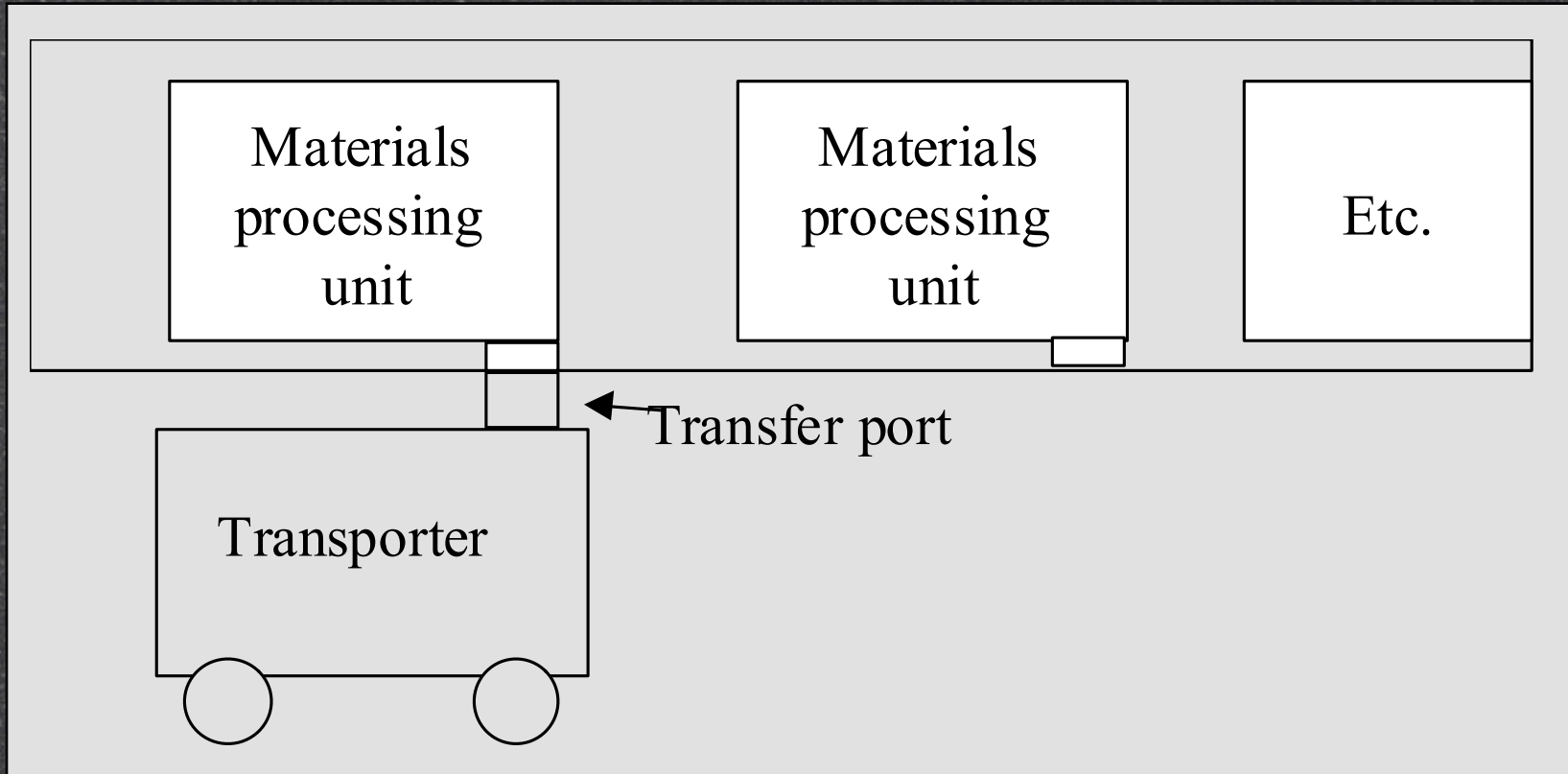
Public Domain Example

Has been produced to:

- Illustrate the application of the CEMISIS approach
 - use of CEMISIS guidance throughout modernisation process
 - focus on safety and cost effectiveness issue
- Incorporate the lessons learned (but maintaining confidentiality)

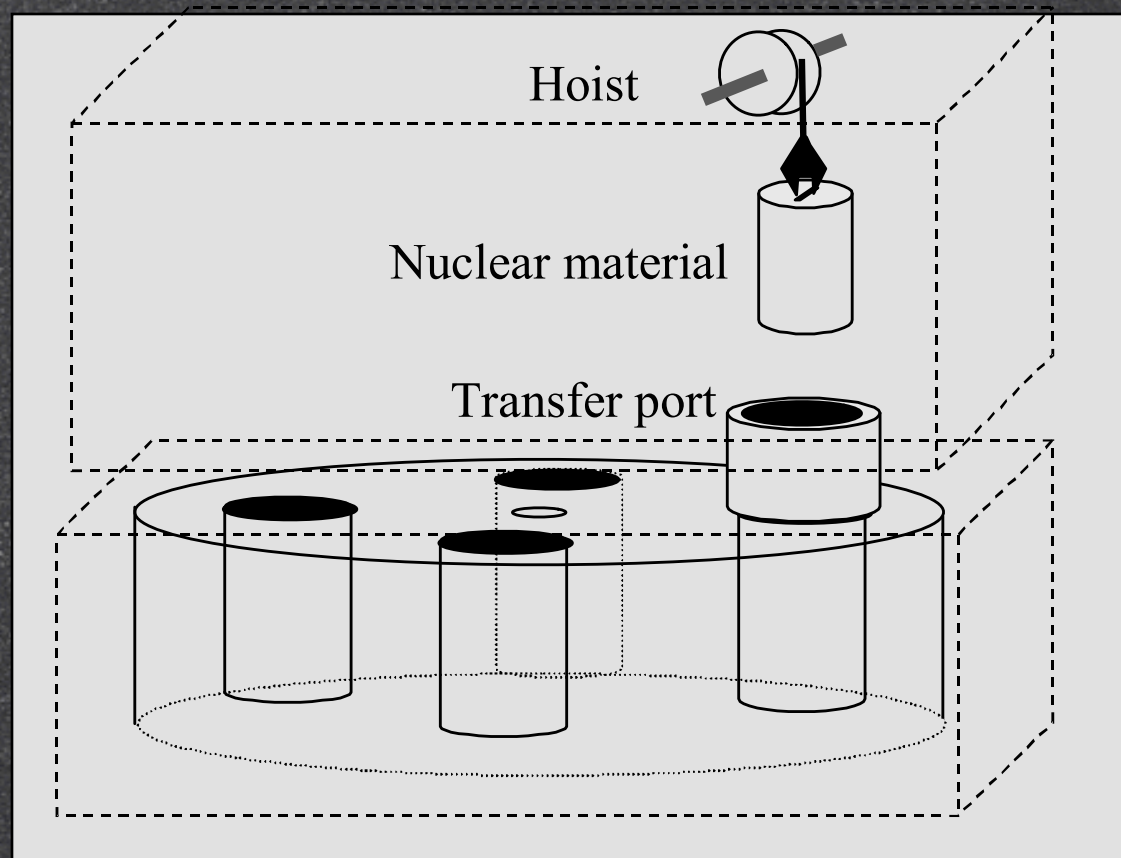


Materials handling system



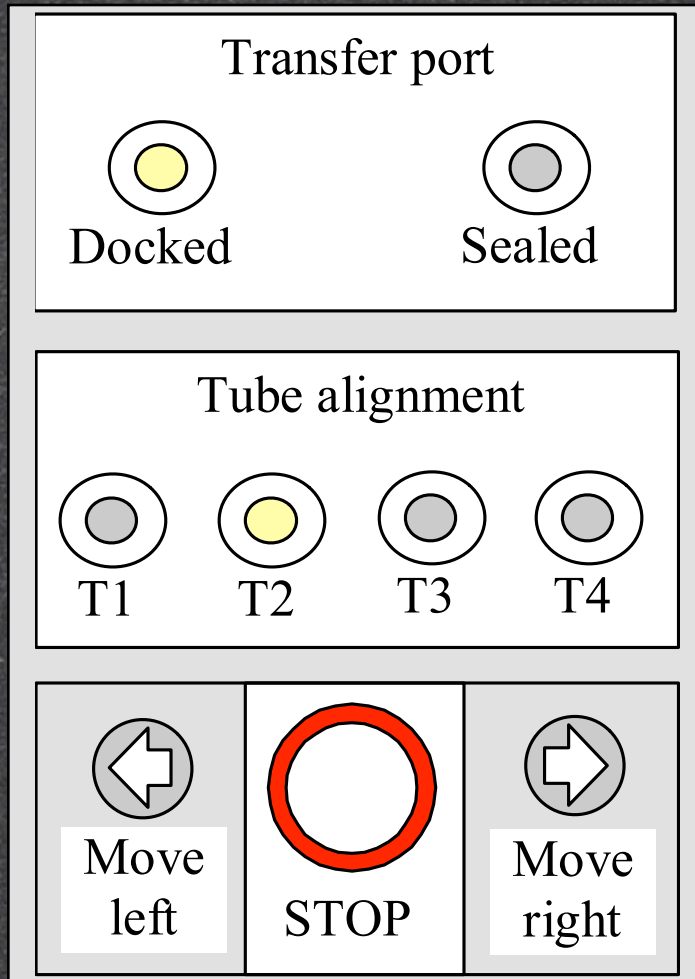
- MHS moves nuclear material between different processing units

MHS



- Carousel holds material (can rotate, but not 360 degrees)
- Material loaded/extracted via transfer port using hoist

MHS controls



- Existing control logic implemented with discrete components
- Movement control has separate relay-based safety interlocks
- Control panel composed of pushbuttons and indicator lamps

Example MHS hazards


Hazard

- Rotation of carousel while hoist active
- Rotation of carousel past end-stops
- Carousel chamber not aligned with transfer port and hoist operation allowed

Consequence

- Rotation of carousel while hoist active
- Rupture of container
- Radioactive contamination
- Motor burn-out, operational delay
- Rupture/jamming of container during transfer
- Radioactive contamination within cell

Modernisation process

- Prequalification (of suitable COTS)
 - Project viability
 - Requirements for MHS replacement
 - Safety Justification plan
 - SIS Tender, assessment, negotiation
 - Implementation
 - Installation and commissioning
 - Operation
- 
- Safety justification claims and production of evidence
- Focus on project viability, requirements and safety justification plan (COTS and safety case structure covered later)

Project viability

- Do we need to replace?, e.g.:
 - Unreliable equipment (production losses)
 - High maintenance cost, obsolete
 - Regulatory changes
 - New operational requirements
- Replacement costs and project risks
- Safety / licensing implications
- Replacement decision

MHS replacement decision

■ Reasons for replacement

Obsolete components,
5 years spares stock remaining
Maintenance cost (24 hour): £120 000/year
Cost of production delays:

£500/day

■ Cost of replacement

System procurement:

£237,000

Safety Case:

£120,000

Maintenance (12 hour):

£50,000/year

Excess outage cost:

CEMSIS

MHS replacement decision (2)

■ Assessment

Need to replace in 5 years

Yearly savings could be £180, 000 (reduced production loss, and maintenance cost)

Could recover cost in 2 years

Main risk is licensing delay (£10 000 /day)

■ Decision

(Now), replace control logic with computer-based system

(Later), replace interlocks with modern discrete logic equivalents

MHS requirements

- Establish plant design basis for current system
 - plant context
 - safety claims made on the MHS
 - MHS design, operation and maintenance documents
 - operating experience
 - physical constraints (space, weight, power ...)
 - .. etc
- Establish requirements for replacement system
 - New regulations (e.g. IEC 60880)
 - Experience with existing system (safety/operational issues)
 - Support for test and diagnosis
 - Changes in maintenance strategy

MHS functional safety requirements

Safe operating states

■ Hoist move

Transporter	Stationary AND Locked
Transfer port	Docked with cell AND Open
Carousel	Stationary AND Aligned with port

■ Carousel rotate

Transporter	Stationary AND Locked
Transfer port	Docked with cell AND Open
Hoist	Retracted
Carousel	Within rotation limits

■ Dock/Undock etc

Functional safety requirements unchanged

Integrity requirements

- Single failure criterion
- 10^{-2} Control action failure
- 10^{-4} Safety interlock failure

Additional requirement for computer control system to be compliant with IEC 61508 SIL 2

MHS Control logic

- Plant interface signals specified
- MHS logic diagram uses unusual logic components
- Time response not specified

Check of drawings against actual logic reveal inconsistency
Logic updated, and respecified in AND / OR logic form
Maximum time response defined (100 msec)

Working with legacy documentation and drawings a key part of case study realism

New requirements

- Could be derived from known safety/operation/maintenance problems that were not feasible to fix in the old technology.
 - e.g. from safety, operating problem reports, or discussions with stakeholders (controllers, maintainers, engineering)
- Also may need to support new operational requirements (like automated tracking of nuclear material)
- Take into account contemporary standards
- Example new requirements:

Built-in support for MHS interlock function testing (to reduce outage time)

Improved user interface (to indicate the carousel movement direction)

Barcode reader to identify what container is loaded /unloaded

Safety Justification Plan

Plan needs to:

- Define the structure and evolution of the safety justification
- Decide on regulator interface
- Define who does what (regulator, supplier, utility)

In the MHS example:

- Regulator involved from an early stage
- Safety justification developed incrementally
- Safety justification evidence identified as project deliverables (by SIS supplier and/or utility)

Safety justification approach

(explained in more detail in later talk)

- Identify top level claims
- Break down into sub-claims
- Identify the evidence supporting the claim
- Evidence can include claims about COTS component
(evidence re-usable in different safety justifications that use the component - hence saving effort)

Lesson learnt

- Explicit identification of arguments

MHS top-level claims

- MHS functionality is sufficient to maintain safety in all plant states (when there are no failures)
- MHS behaviour is adequately safe when failures occur
- MHS can be safely maintained, operated and updated throughout its planned lifetime

Types of claim

- Level 0 - Top-level
 - Level 1 - Interface (behaviour at the system interface)
 - Level 2 - Architecture (components of the system)
 - Level 3 - Design (about a component of the system)
 - Level 4 - Operational (operation/system interaction)
-
- The top-level claim is expanded into sub-claims at different levels
 - Illustrated in next slide (**supporting evidence shown in green**)

Expansion of first claim

- Level 0. MHS functionality is sufficient to maintain safety in all plant states (when there are no failures)
 - Level 1. MHS requirements are complete (cover plant hazards)
MHS interlock - hazard coverage analysis
 - Level 1. MHS requirements are complete (actions prevent hazard)
MHS logic simulation, review
 - Level 2. MHS requirements are correctly implemented
 - Level 3. MHS interface conversions correct
COTS interface specs, interface tests, installation testing
 - Level 3. MHS application logic program correct
Review, tests against logic simulation, commissioning tests
 - Level 3. MHS COTS platform correctly executes logic
COTS pre-qualification evidence
 - Level 3. MHS time response within specification (100 msec)
COTS platform evidence (predictable timing behaviour)
Compliance to COTS platform timing constraints
Timing analysis of logic applications

COTS safety justification

- ◆ Pre-qualification of the COTS (if already accepted) can reduce the licensing delay risk.

Provides a separate set of level 0 claims about the COTS

- ◆ For a specific application using the COTS need to show:
COTS is suitable for the intended application

The application meets the constraints imposed on the COTS

- ◆ Pre-qualified Level 0 timing claim for the MHS COTS is:

Maximum logic response time < 3 schedule cycles

provided total application logic time $< 90\%$ of one cycle

- ◆ Level 3 application claim: “time response < 100 ms”

— COTS level 0 claim (< 3 cycles + 90% cycle constraint)

— schedule cycle time is 20 msec so max delay is 60 msec

— application logic takes 10 msec (only 50% of cycle time)

Evolution of safety justification

- Some of the sub-claims will evolve during development,
 - e.g. additional claims may be needed about the operational environment
- In addition the status of evidence supporting claims may change over time.
 - e.g. planned -> interim -> final
- This will be illustrated for specific sub-claims of the MHS
 - development evidence: timing analysis of logic diagrams
 - post-development evidence: systems tests for response time

Summary

- The public domain example is used to illustrate CEMISIS guidance
 - identified a specific example MHS
 - covered some of the stages of modernisation (project viability, requirements, safety justification planning)
-
- Reflects experience of case studies and experience of partner
-
- Indicates how project risks (like licensing delay and inadequate requirement) can be reduced by:
 - considering the scope of replacement at the project viability stage
 - addressing both existing and new requirements prior to tender
 - providing a clear structure of claims and evidence at an early stage in the project

The full Monty

■ (on release in March 2004)

Public domain example contents

1. Introduction
2. The materials handling system (MHS)
 - 2.1 Plant context
 - 2.1 Legacy system and interfaces
 - 2.3 Operation and maintenance
3. Project viability phase
 - 3.1 Need for modernisation
 - 3.2 Cost of modernisation
 - 3.3 Replacement decision
 - 3.4 Project viability of MHS SIS replacement

Chapter 4

4. MHS requirements

4.1 Establishing the plant design basis

- plant context, safety claims for the logic
- SIS safety integrity requirement,
- Plant interfaces, Plant logic
- ...
- Design basis validation

4.2 Requirements for the replacement system

- New regulations, experience with the existing system
- Maintenance changes, Operational changes
- Installation and commissioning constraints
- Safety justification requirements
- Consolidation

Chapters 5 and 6

5. Safety Justification Approach

- 5.1 Evolution of the safety justification
- 5.2 Regulator interface
- 5.3 Planning
- 5.4 Structure of the safety justification
- 5.5 Use of COTS

6. Safety justification evolution for the MHS

- 6.1 Pre-tender safety claims (utility)
- 6.2 Post-tender safety sub-claims claims and evidence (supplier)
- 6.3 Post-development safety sub-claims claims and evidence (supplier)
- 6.3 Preoperation safety sub-claims claims and evidence (utility)

Appendices

Appendix 1 CEMSYS safety case guidance

Appendix 2 CEMSYS requirements guidance

Appendix 3 Guidance on the use of COTS

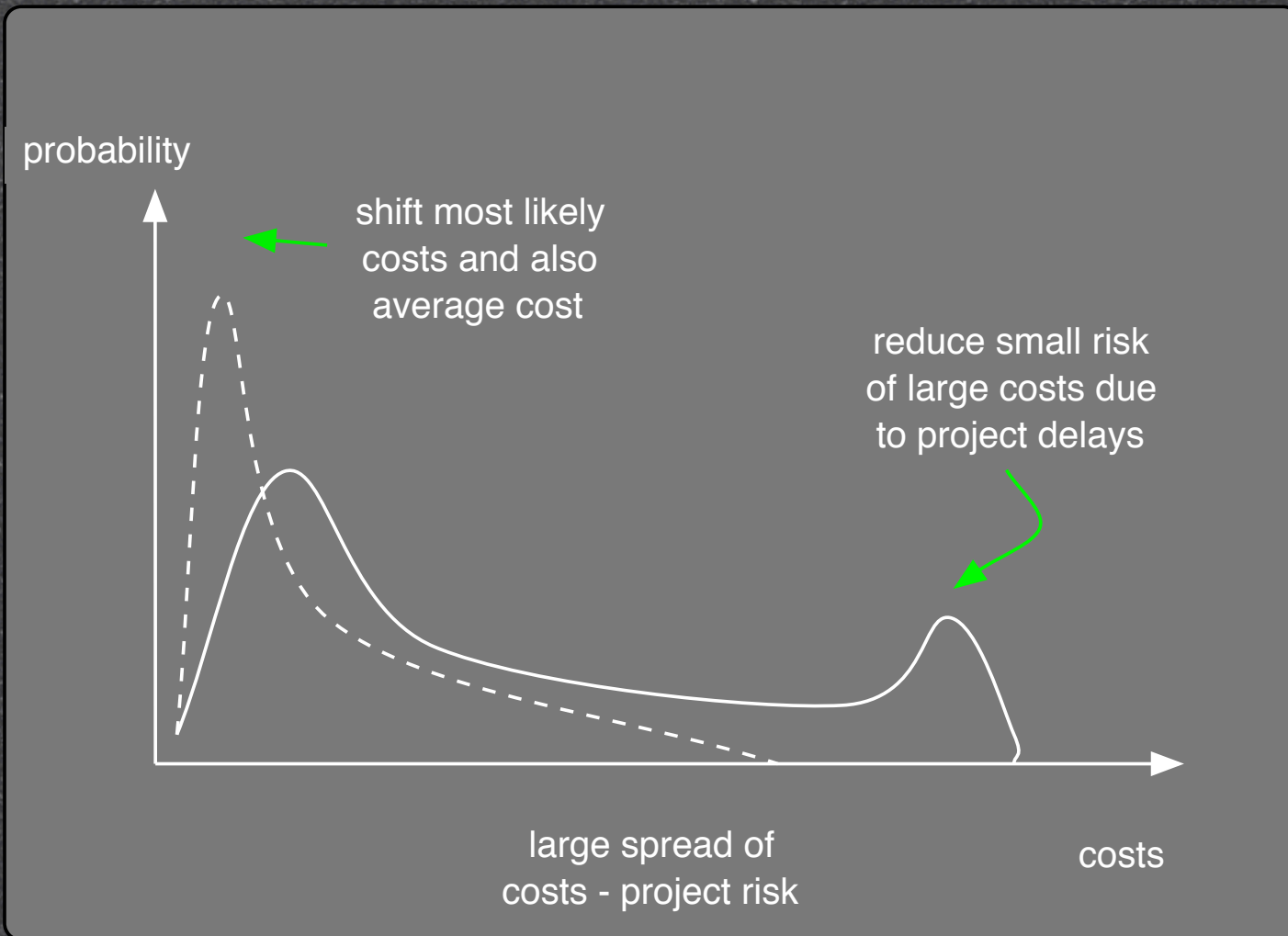
Appendix 4 Cost modelling

Cost Issues

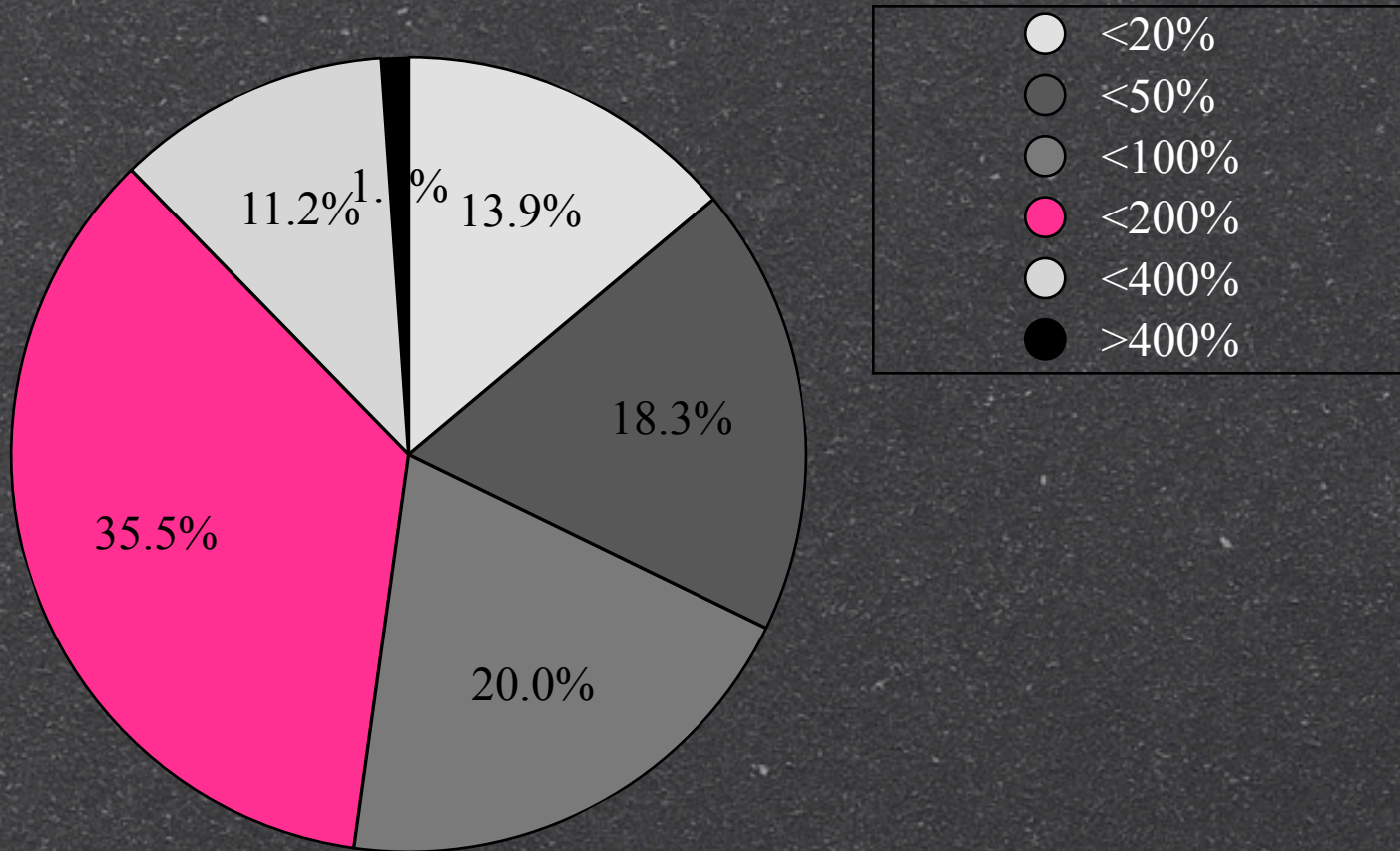
Cost effectiveness claims

- reduced costs. Historically the costs for assurance can be 100% of the development cost not accounting for any delays to plant commissioning and subsequent lost generation.
- reduced uncertainty in costs. The extra costs of a safety related system has varied between 6-100% of the cost of a system of normal industrial quality. Uncertainty arises from direct costs and time
- reduced time to develop and assure systems important to safety.
- increased commonality in nuclear I&C between different countries/utilities and with other industrial sectors

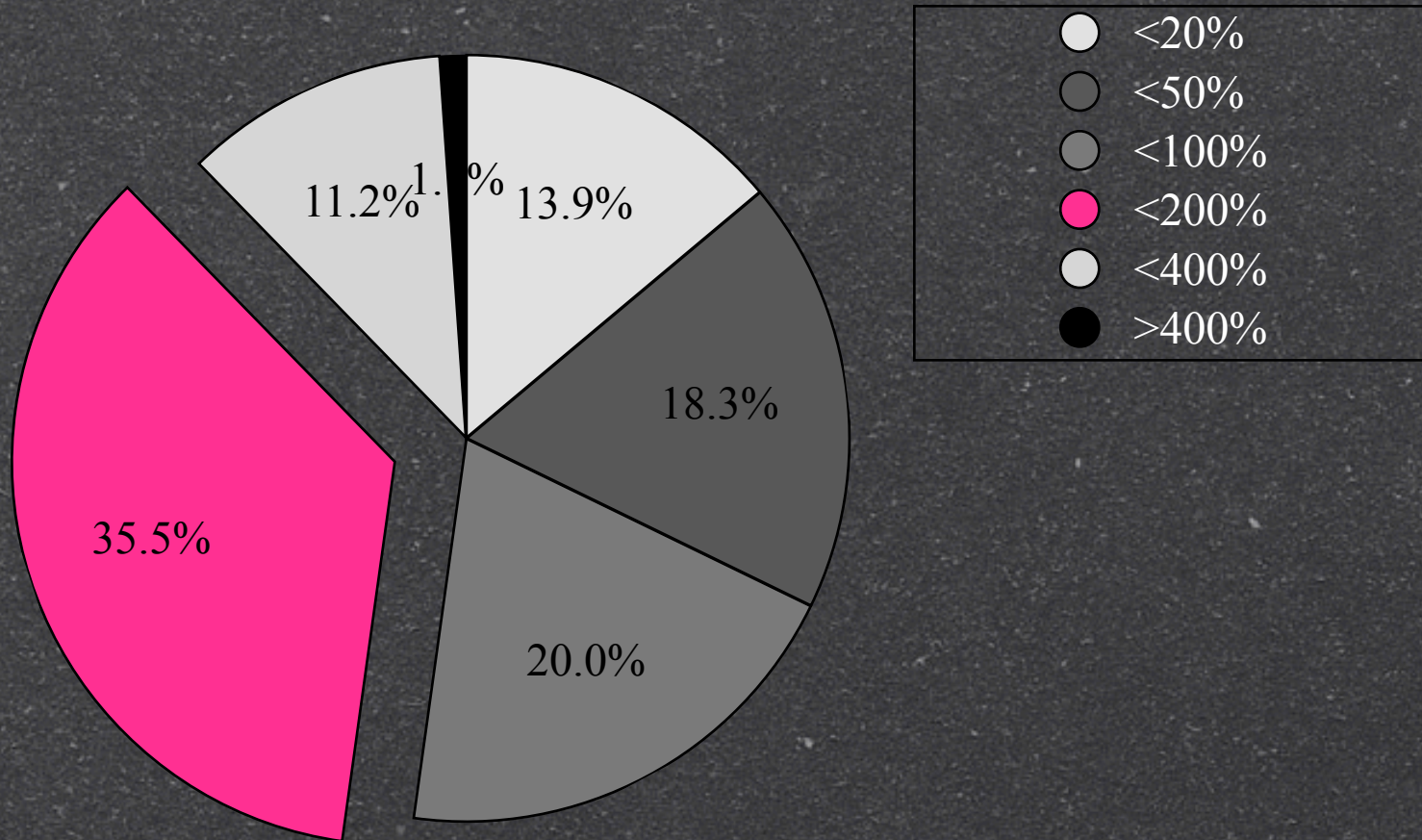
Cost distribution



Delayed software projects

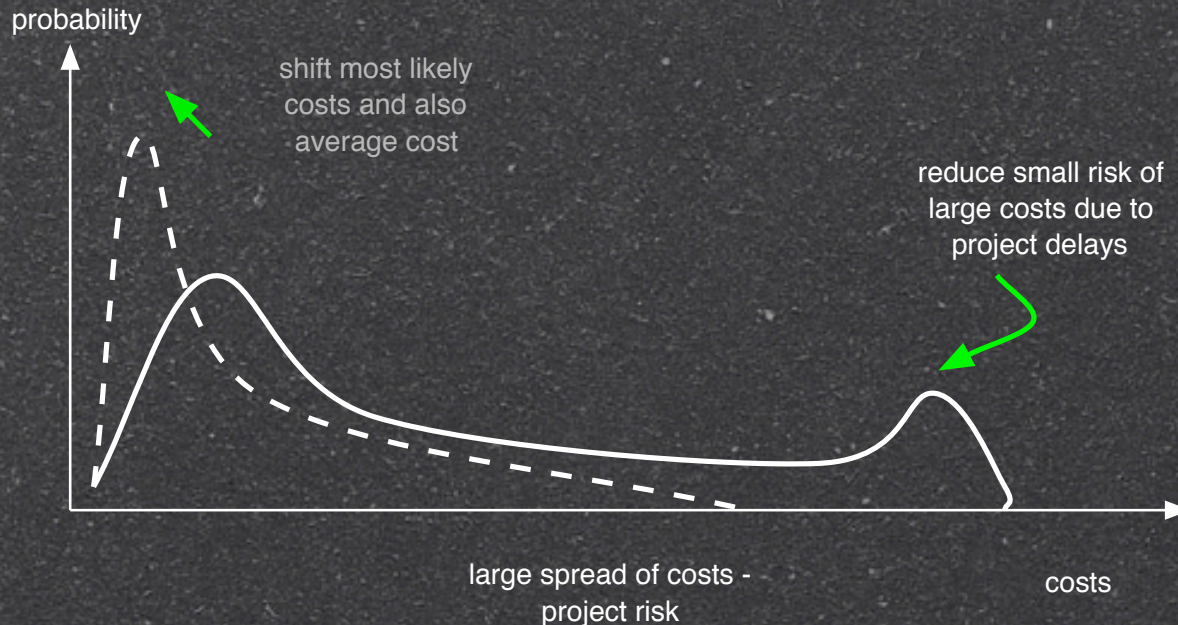


Delayed software projects

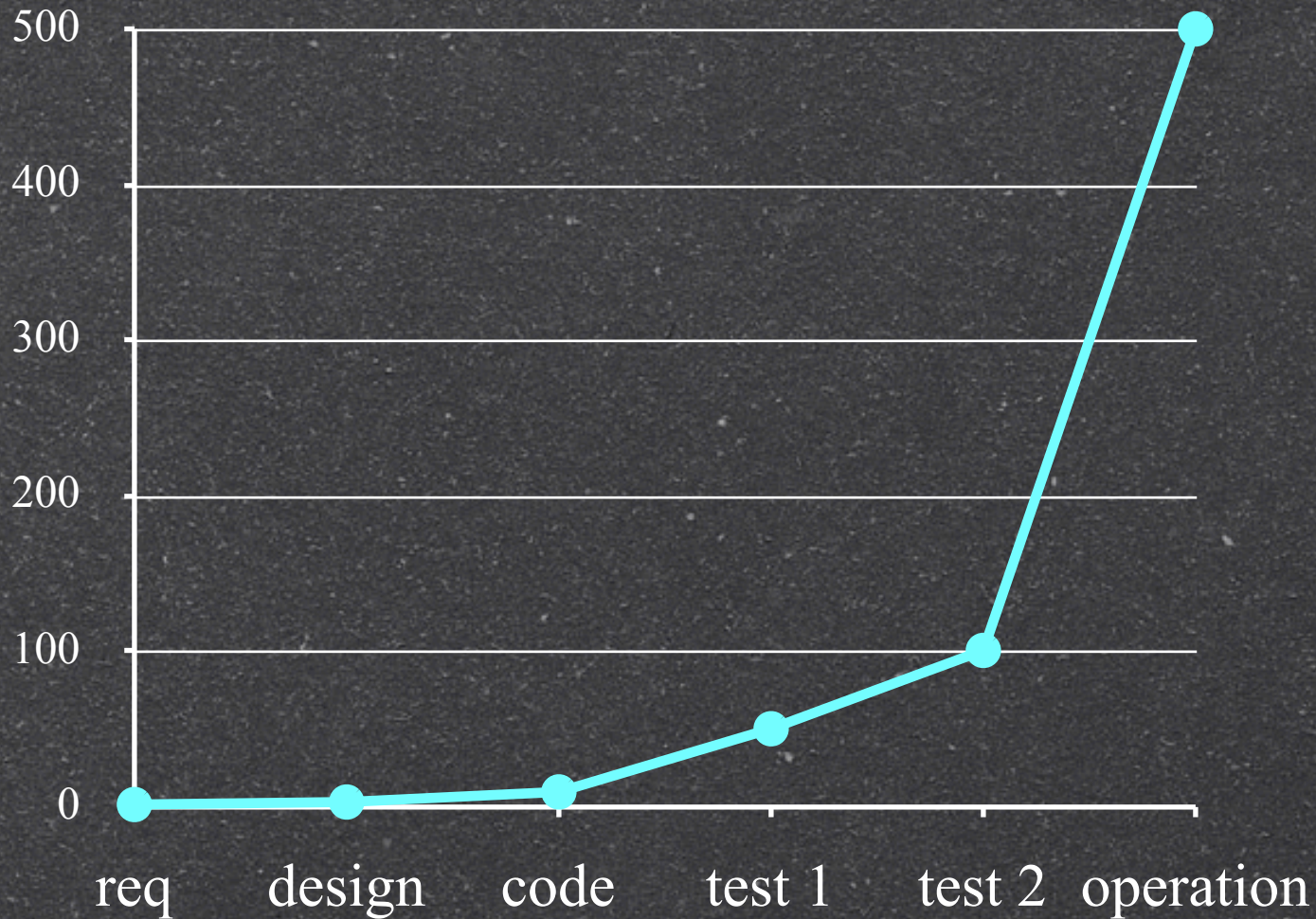


Requirements

- identifying requirements errors early in the lifecycle.
- allowing changes to the existing system to be minimised, but integrating new requirements if desired.
- using an incremental requirements process
- correctly and completely documenting requirements



Benefits of early fault detection



Data adapted from Boehm

CEMSIS

COTS/PDS

- assessment of pre-developed products allows product assessment costs to be shared by projects.
- User-Supplier communicating ahead of projects can lead to medium or long-term policy that addresses nuclear industry needs.
- use of pre-developed products can be more cost effective than the development of bespoke items

Apart from direct cost reduction pre-qualification of products reduces project uncertainty as last minute questions can be costly in effort and delay. it also provides a transparent approach that allows for more open competition.

Licensing

- By allowing the stakeholders to restrict their attention on those claims only that are dictated by the replacement/upgrade and/or by the use of a new technology
- By allowing the stakeholders of the safety case to focus attention on the critical safety issues specifically raised by the SIS to be replaced/upgraded,
(thereby avoiding endless debates on the applicability of - and compliance with - rules or standards that are not necessarily adapted to a given project, environment or system)
- By allowing safety claims to be prioritised so that the required evidence is limited to what is arguably necessary and sufficient
- By allowing claims and subclaims to be re-used in other safety justifications, with their supporting arguments and evidence

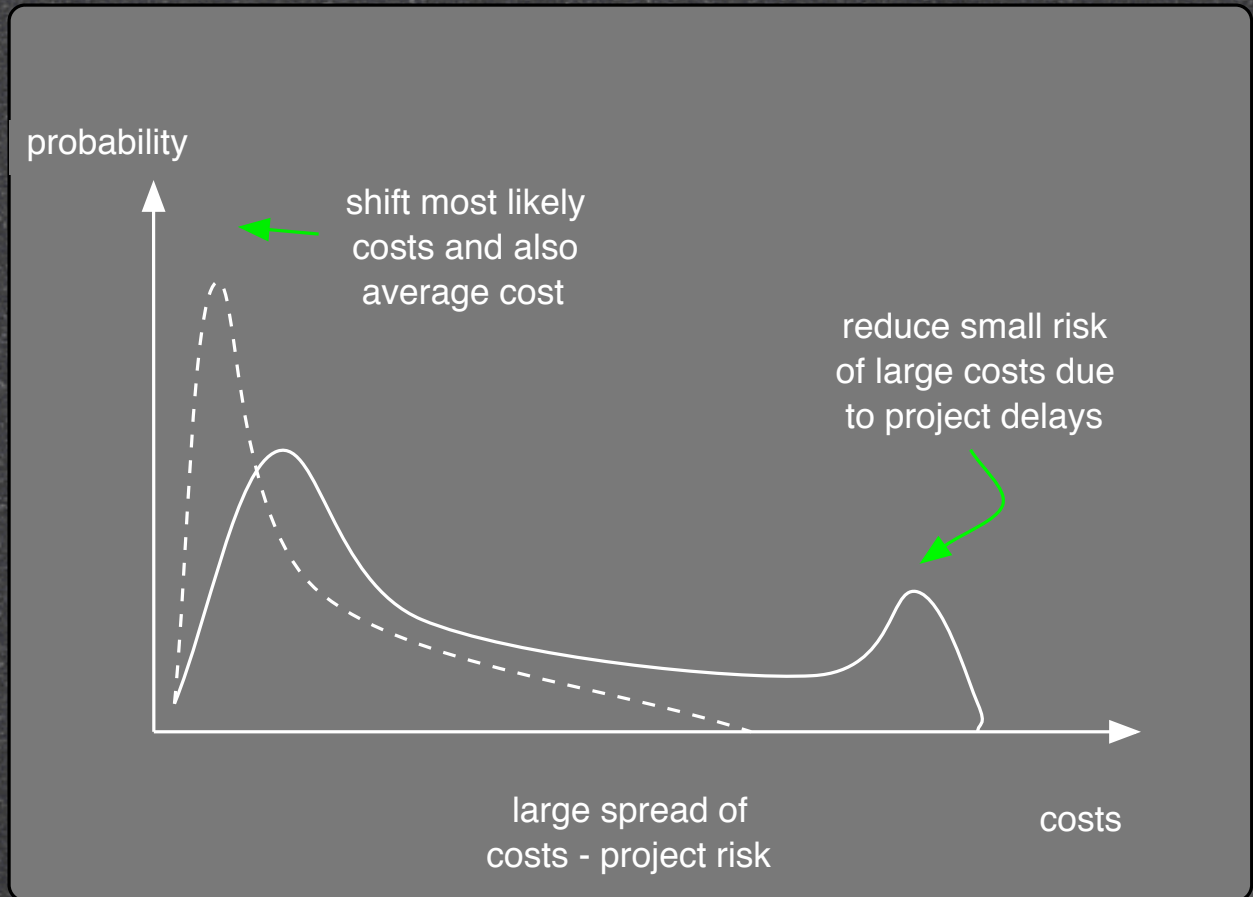
Licensing

- Focus on relevant claims
-
- Focus attention on the critical safety properties
-
- Prioritise safety claims so that evidence is limited to what is arguably necessary and sufficient
-
- Allow re-use of safety justification

Cost savings and project risks

due to

- Claims
- Arguments
- Evidence
- Reuse



Cost model

■ Work in progress - scenarios

Cost of ownership =

$C_{tech} + C_{IO} * IO + C_{support}$

$+ (C_{logic} + C_{req} + J_{tech} + J_{io} + J_{logic} + J_{req} + J_{support} + J_{maint}) / N$

$+ C_{site_specific}$

$+ L * T$

$+ P * T$

$+ (M_{io} * IO + M_{tech} + M_{test} + M_{repair}) * T$

$+ (U_{tech} + U_{io} + U_{support} + J_{upgrade}) * S * T$

$+ U_{logic} * R * T$

Conclusion

- Provides practical guidance illustrated with realistic examples.
- Diffusion of expertise and experience within partners
- Key audience:
 - Senior I&C engineers and managers of refurbishment projects
 - Development engineers and managers in the supply industry
 - SMEs and service companies in the refurbishment market
 - Regulators and policy makers
- Impact on strategy:
 - Accelerate inter working in member states
 - between utilities, suppliers and regulators
 - Help to focus national R&D efforts

Continuing Influence

- Public and Limited Circulation Deliverables
 - Use within members organisations and member states
 - Dissemination by web-site <http://www.cemsis.org>
- Members participation in international activities
 - International standards, e.g. IEC 60880 and 61508 revision
 - European Nuclear Regulators Working Group
 - Electric Power Research Institute (EPRI)
- Continuing research, possibly under Framework VI

www.cemsis.org

The end

