Applying safety process measures

Paul Caseley

prcaseley@dstl.gov.uk

01684 771476

Jun 2004

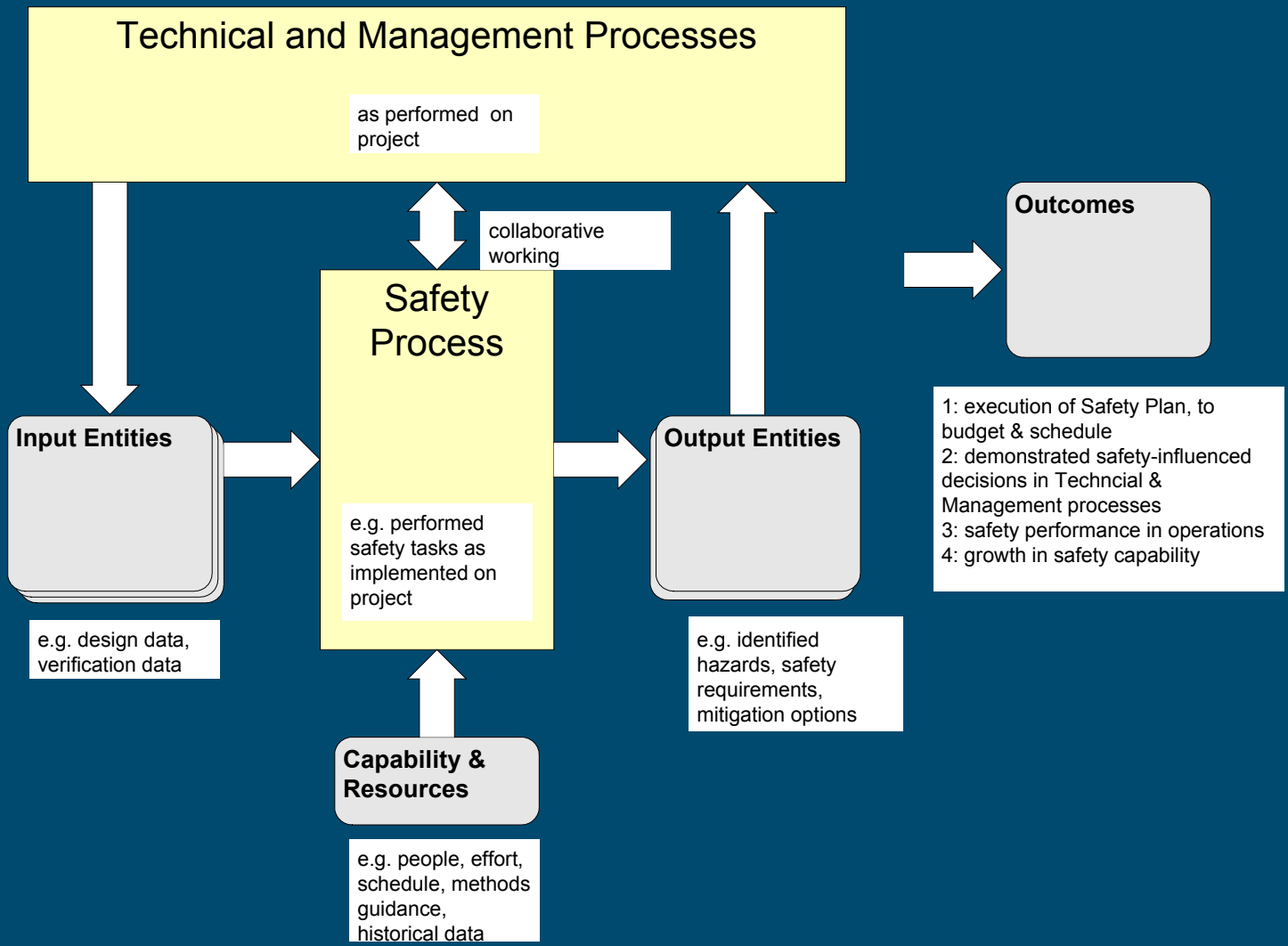
Applying Safety Processes Measures

- Overview of the presentation
  - The Practical System and Software Measurement white paper
    - Practical Safety Process and Project Measurements
  - A view on the safety lifecycle (from Draft Def Stan 00-56)
  - Some examples of existing SMS and safety process measures
  - A MOD study with example measures
    - Background CADMID and project
    - Study highlights
  - The future - level 3 Def Stan 00-56 proposal

Safety and Security Measurement - white paper

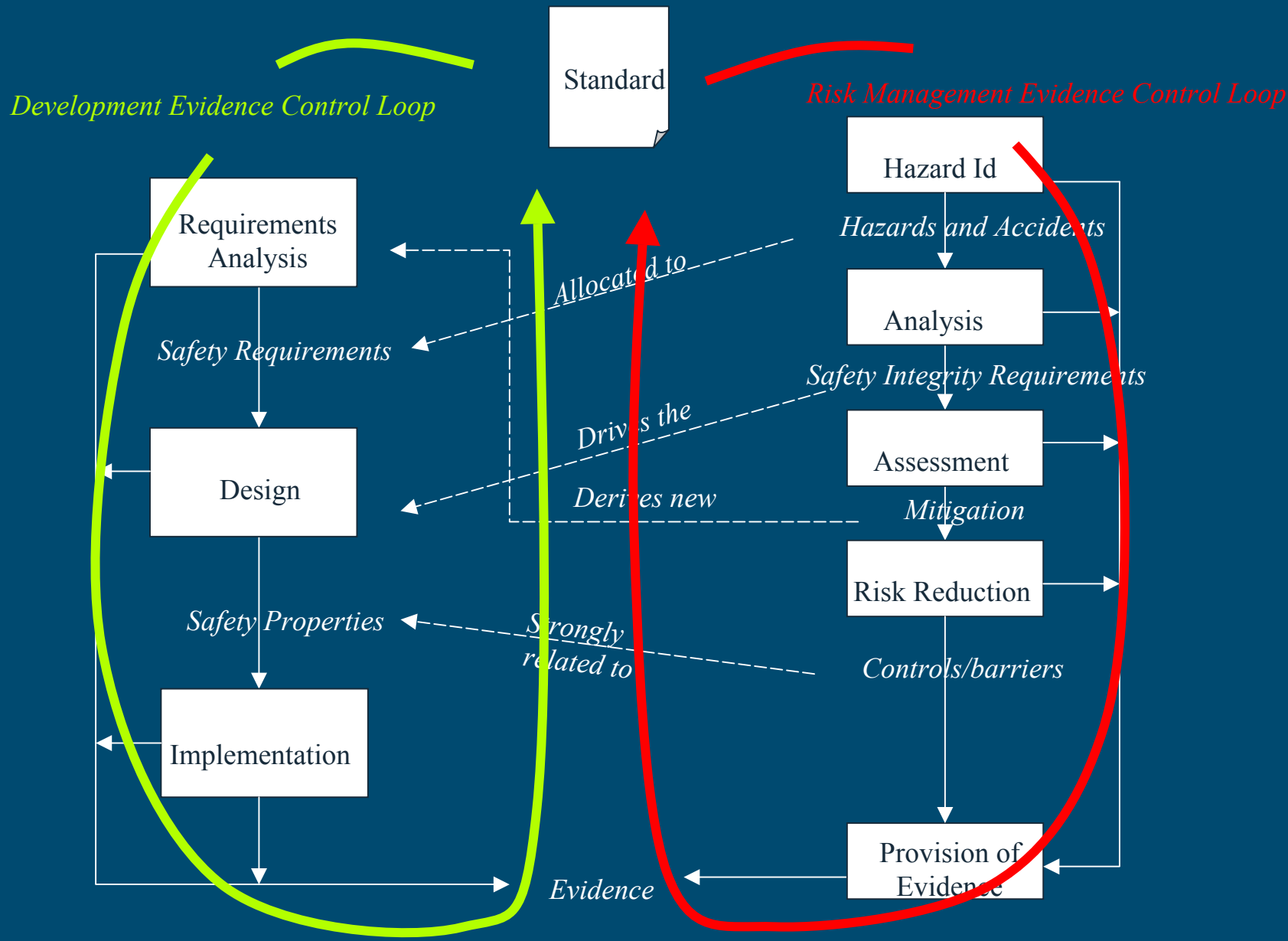
- Safety and Security Measurement white paper is a Practical System and Software Measurement (PSM) working group product
- Aimed at:
  - Enhancing PSM
  - Supporting processes improvement initiatives such as CMMI safety and security and +SAFE
  - Aid companies that need to apply safety standards
- Covers the safety aspects but security still to be fully addressed

Safety Process interaction - white paper

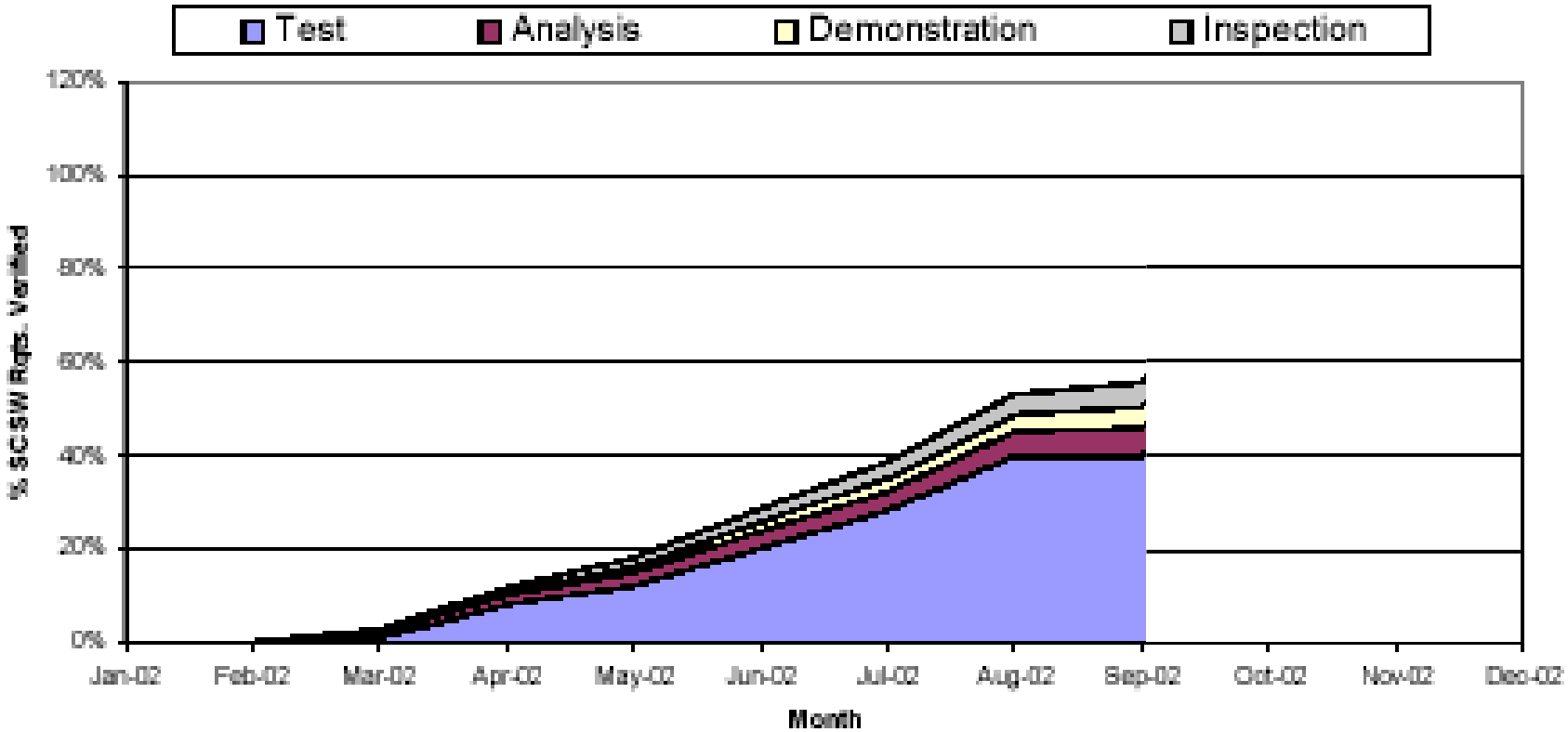


Important issues - white paper

- Easy issues to measure
  - Progress of safety work against a plan
- Difficult but important issues to measure
  - Showing safety influences the design
    - requirement
    - design risks
    - effects on cost
  - Showing safety influences from technical levels to enterprise levels
    - “safety culture”
    - Assessment of safety risk to the business
    - assist in ALARP decisions

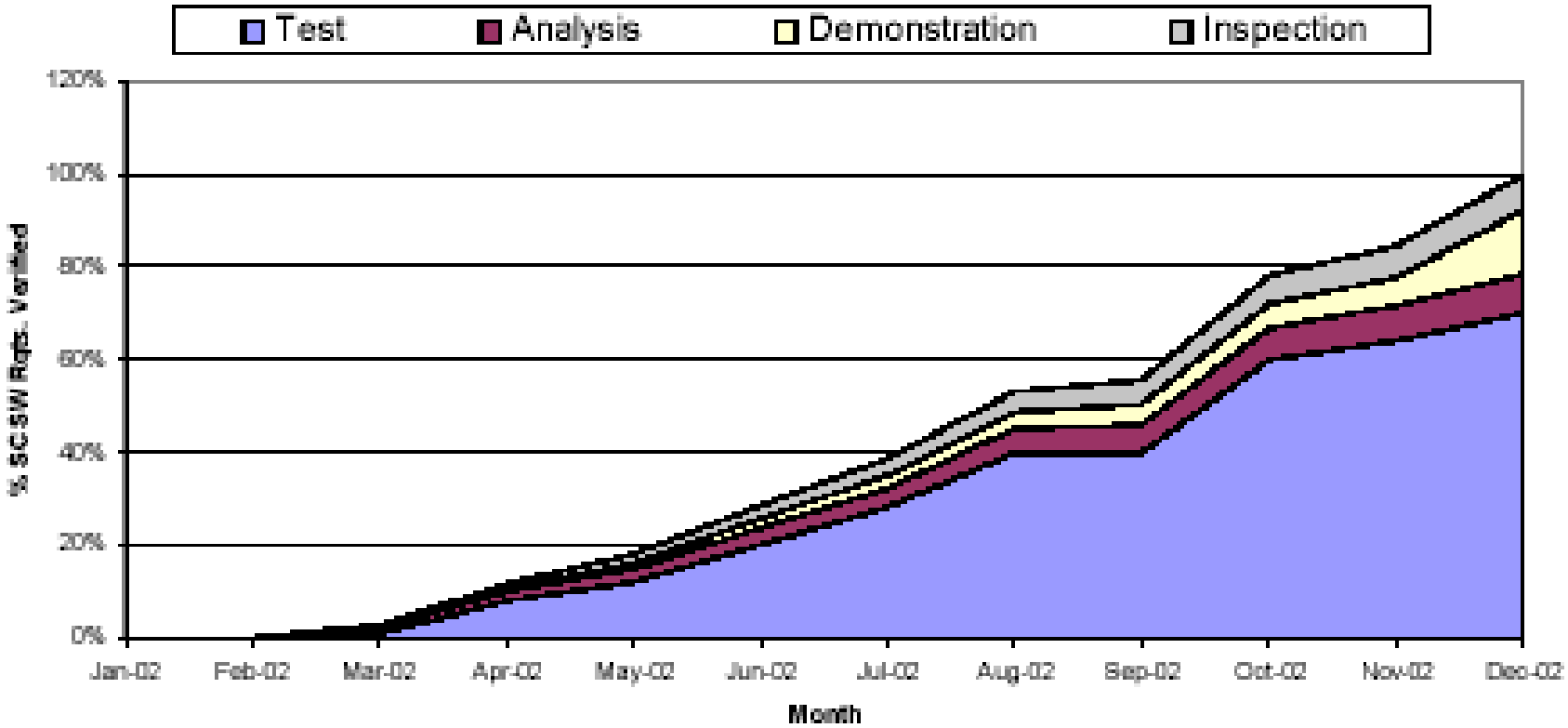

Standard
Development Evidence Control Loop
Risk Management Evidence Control Loop
Requirements Analysis
Design
Implementation
Safety Requirements
Safety Properties
Evidence
Allocated to
Drives the
Derives new
Strongly related to
Hazard Id
Analysis
Assessment
Risk Reduction
Provision of Evidence
Hazards and Accidents
Safety Integrity Requirements
Mitigation
Controls/barriers

Examples 1a - Howard/Emery



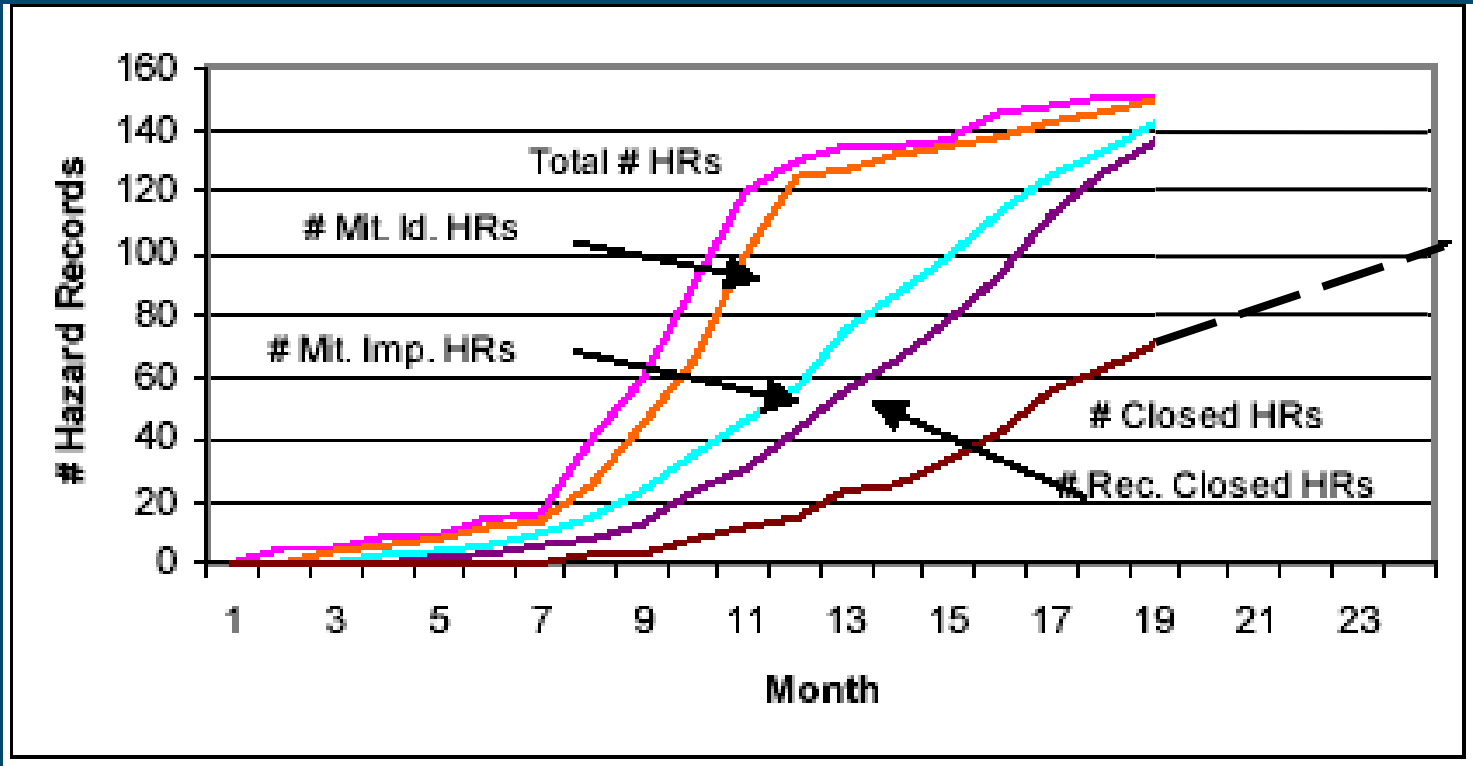
- Only 55% safety critical requirements verified?
- Management action required?

Examples 1b - Howard/Emery



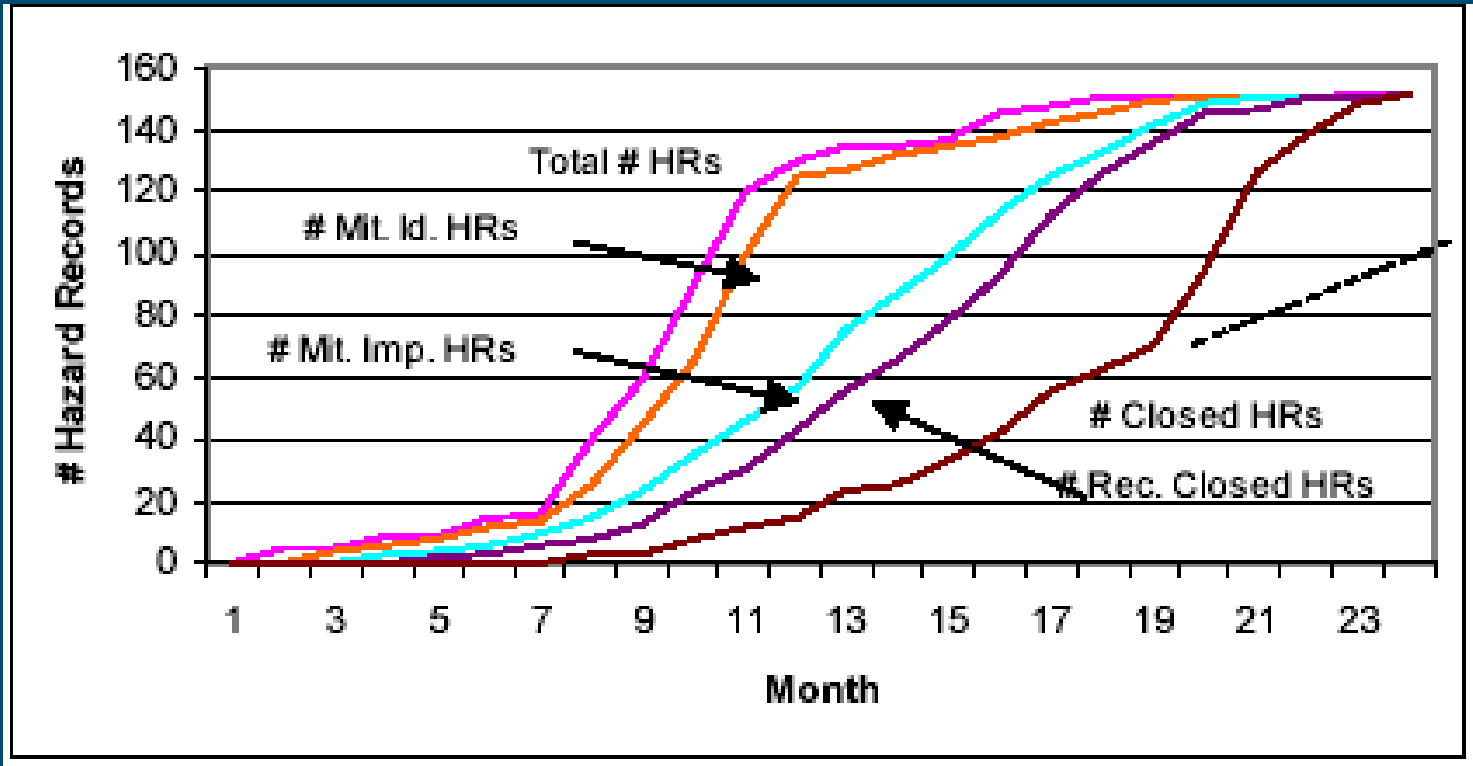
- 10% verified by inspection and analysis?
- Indicates system engineering is effected by safety?

Examples 2a - Watt



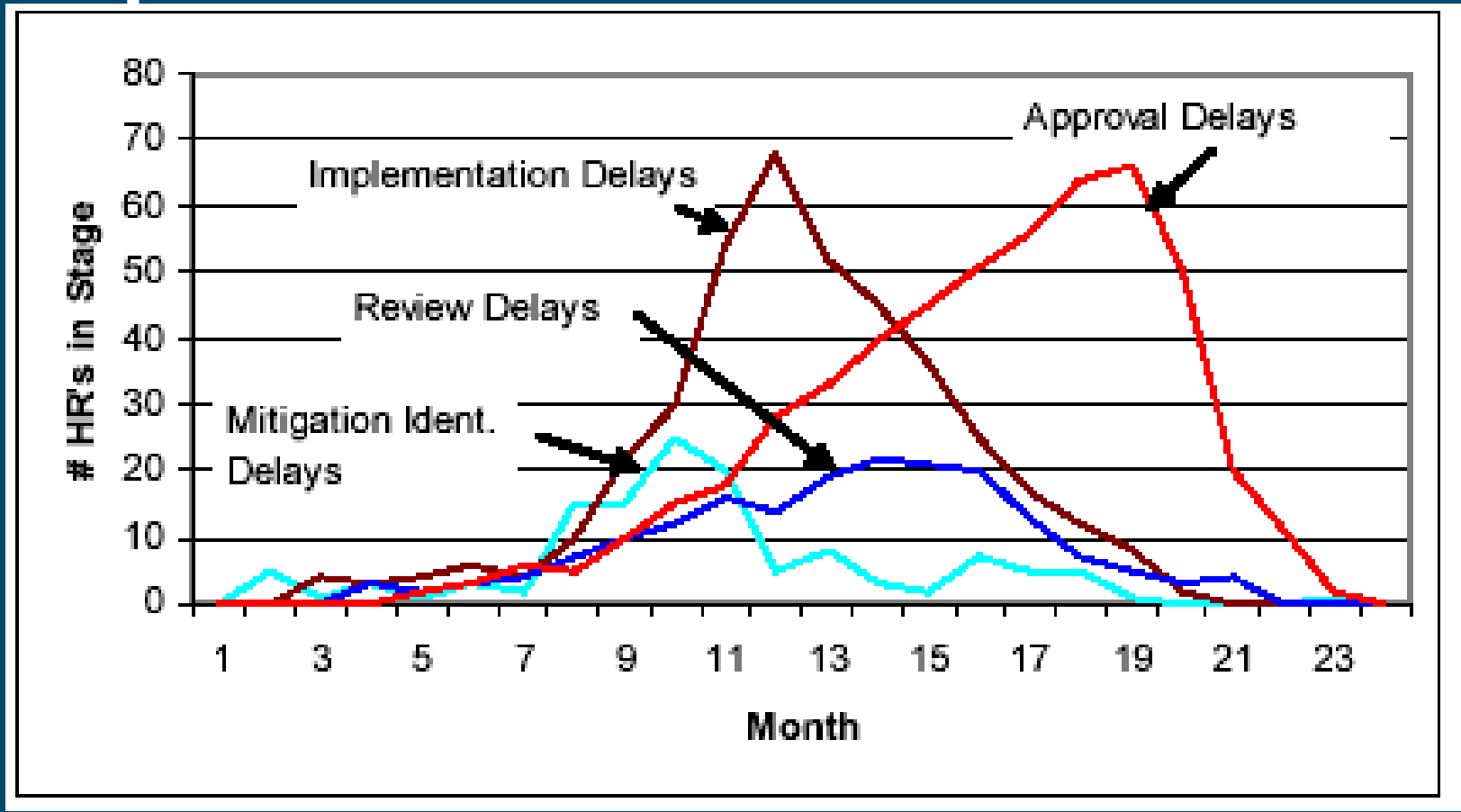
Hazard closing trends? Shows management of Hazards?
20 Hazards without mitigation at month 10 - requirement growth?
Delivery in month 24, will hazards be closed?

Examples 2b - Watt



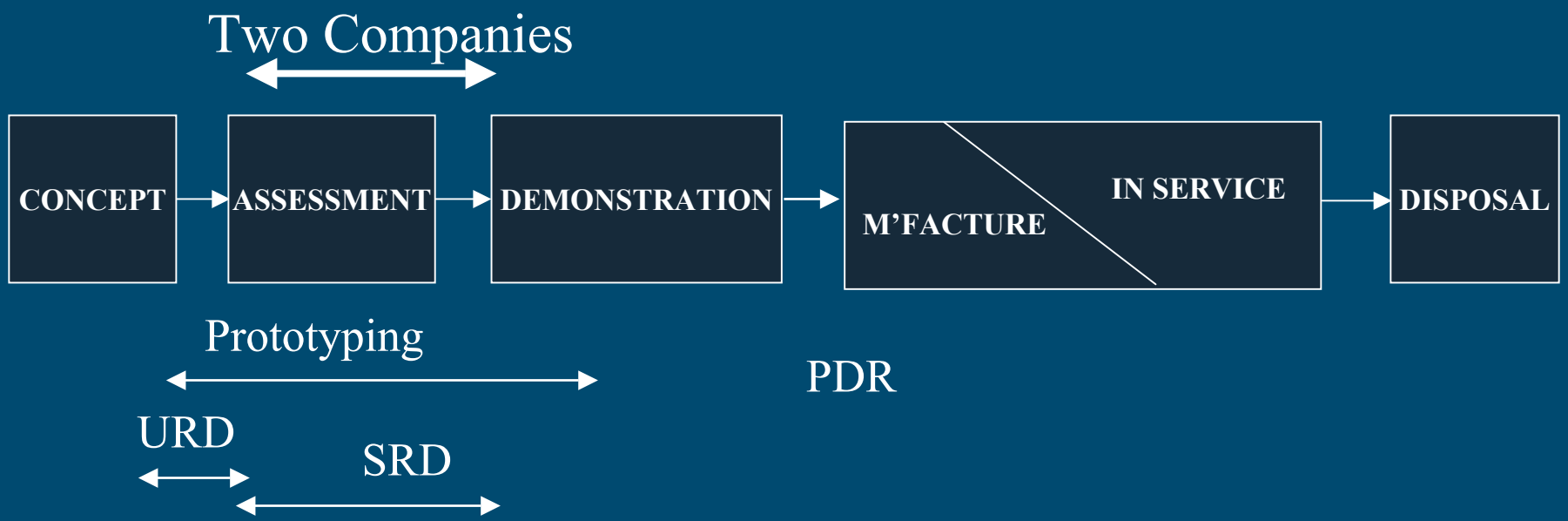
Corrective action worked?

Examples 4 - Watt



Safety bottlenecks and risks: Implementation delays?
Mitigation identification delays (potential requirement delay)?

CADMID Procurement Cycle - MOD



- Two or more companies develop the user and system requirement and initial designs.
- After the assessment phase a company is selected to further develop and manufacture the product

Measuring the processes

- Both teams used the same safety standard

Process is risk management (Safety)

- Hazard Identification
- Risk Analysis (Severity),
- Risk Assessment (Likelihood*Severity = Risk)
- Risk Reduction
  - Identify safety requirements
  - Mitigation identification
  - Implement and verify

Measurement can help safety - study example

- This study was looking at how efficient and effective the hazard identification process was for a particular project
- It is an example of applying safety measures
- The PSM Safety and Security Measurement white paper suggests this is an applicable area of measurement

General Project Information

- Small to Medium size project
- Judged to be a low safety risk at outset
- Two leading suppliers
- Both had strong safety teams
- Both were judged compliant with the applicable safety standard at the end of the assessment

Comparing the Hazard Identification Processes

- The hazards from both teams were compared and equivalents identified (comparison carried out by ISAs)
  - Using “Capture-Recapture” analysis method, for example.
    - Group 1 have 20 hazards, Group 2 have 30 hazards
    - Common hazards = 15
    - proportion of hazards captured 15/30 = 0.5
    - Possible total hazards 20/0.5 = 40
  - Simple analysis gives some confidence in the quality of the identification process (efficiency and effectiveness)
  - Assumes processes are truly independent

An Example of the comparison

- Process relies on accurate matching of hazards
- Team A
  - H01: “Inadvertent xxx operation”, Catastrophic
- Team B
  - H005: “XXX inadvertently activated”, Catastrophic
- Some comparisons showed one to many relationships
  - e.g. Team A’s H06 mapped to Team B’s H01, H03 and H04

Note: XXX and xxx were synonyms

Comparison before end of assessment phase

- During PHA:

	No of haz (options)	No of haz (no options)
Team A	46	45
Team B	40	33
Common	22	22
Estimated Total	*83.6*	*67.5*
Efficiency	(48%-55.4%)	(48.9%-66.6%)

Comparison before end of assessment phase

- At the end of Assessment (using a different judge):

	No of haz (options)
Team A	40
Team B	41
Common	35
Estimated Total	*46.86*
Efficiency	85% - 87.5%

Comparing effort

- Both teams measured their effort during the assessment phase
- The comparison of overall effort shows that they both used similar amounts of resources
- The figures for the assessment phase are:
  - Team A = 1326.9 hours
  - Team B = 1350 hours
  - Safety case + PHL + criteria (Team A = 344.5; Team B = 350)
- Assessment estimated effort compared to contract award ~1.3%
  - Ignores the impact of safety on the design

Other Issues - based on 2nd Judge's comparison

- Team A identified five Hazards (four catastrophic and one marginal) that Team B did not
  - Two of the cat hazards may not be hazards
  - Two of the cat hazards may be implied by some of Team B's hazards
  - One hazard may be valid, i.e. Team B missed it
- Team B identified six Hazards (five catastrophic and one marginal) that Team A did not
  - All except one of the cat hazards could be related to features not considered in the Team A design (extra options)

Comparing Severity - Risk Assessment

- Looking at the matched hazards:
  - Using Team A as the base for the 35 matches:
    - 23 hazards could be traced to matching severity
    - 7 were off by 1 degree e.g. catastrophic = critical
    - 3 were off by 2 degrees e.g. negligible = critical
    - 2 were off by 3 degrees negligible = catastrophic
- Care must be taken here e.g.
  - Team A H11:"Exposure of environment to toxic waste", Neg
  - Team B H40: "Ozone depleting/greenhouse …", Crit
  - Team A may not have any serious toxic waste in their design

Study Observations

- The data gave a good indication effectiveness/efficiency of safety processes for the assessment phase
- The comparison of hazards is sometimes very subjective
  - Although the two judges found similar comparisons the second judge showed more latitude in the comparison process
- Both teams impacted the requirement process and measuring the effect of safety on requirements is a useful safety process effectiveness measure, especially for prediction.
- The teams use very similar processes so are not truly independent
  - Used similar hazard identification techniques
  - Used same standard

Def Stan 00-56 level 3 guidance

- Draft proposal for measurement requirements and guidance
- Based on the Draft DS 00-56 part 1 (mandatory) policy
  - The SMS uses effective processes and is managed
  - The System Engineering and Safety Engineering are integrated
  - ALARP decisions are justified
- Suggests that ISAs be part of the process

Summary

- Measuring the safety process using PSM principles is practical, useful and necessary for some organisations
- Basic safety process indicators do aid decision makers (managers and designers) in controlling safety risk both at project and organisational levels
- Applying similar principles to security should be possible and would increase confidence in overall security

Useful papers and references

- Gibbons, J., In Search of the Elusive System Safety Metric, International System Safety Conference, 2002.
- Walker, S. A., Ward D. C., Talso, W. W., System Safety In Support Of Construction Project Management, International System Safety Conference, 2003.
- Watt, G. T., Metrics for Assessing Safety Program Effectiveness in Hazard Identification and Resolution, International System Safety Conference, 2003.
- Elliot, B.J., Creating an Environment for Making Better Decisions about System Safety, International System Safety Conference, 2003.
- Howard K. D. Jr., Emery, M. E., Practical Application of Software Safety Metrics, International System Safety Conference, 2003.
- V2.0 Safety and Security White Paper (Update to v3.0 of Safety & Security White Paper, due for PSM User's Conference, Keystone, July 2004) available from psm website