Applying safety process measures

Paul Caseley

prcaseley@dstl.gov.uk

01684 771476

February 2004

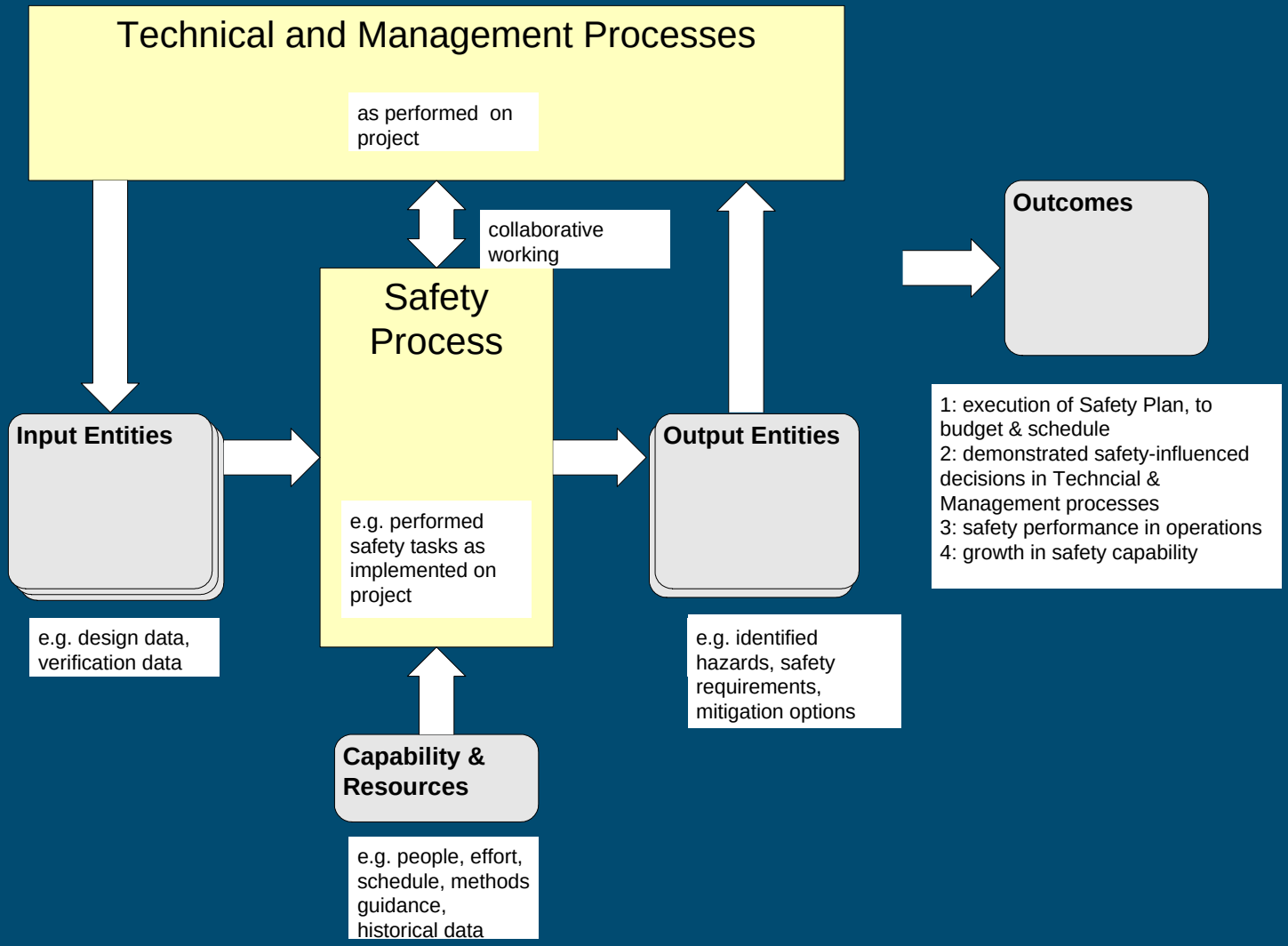
Applying Safety Processes Measures

- Overview of the presentation
  - The white paper
  - A view on the safety lifecycle
  - A MOD study with example measures
    - Background CADMID and project
    - Study highlights
  - The future - security measures

Safety and Security Measurement - white paper

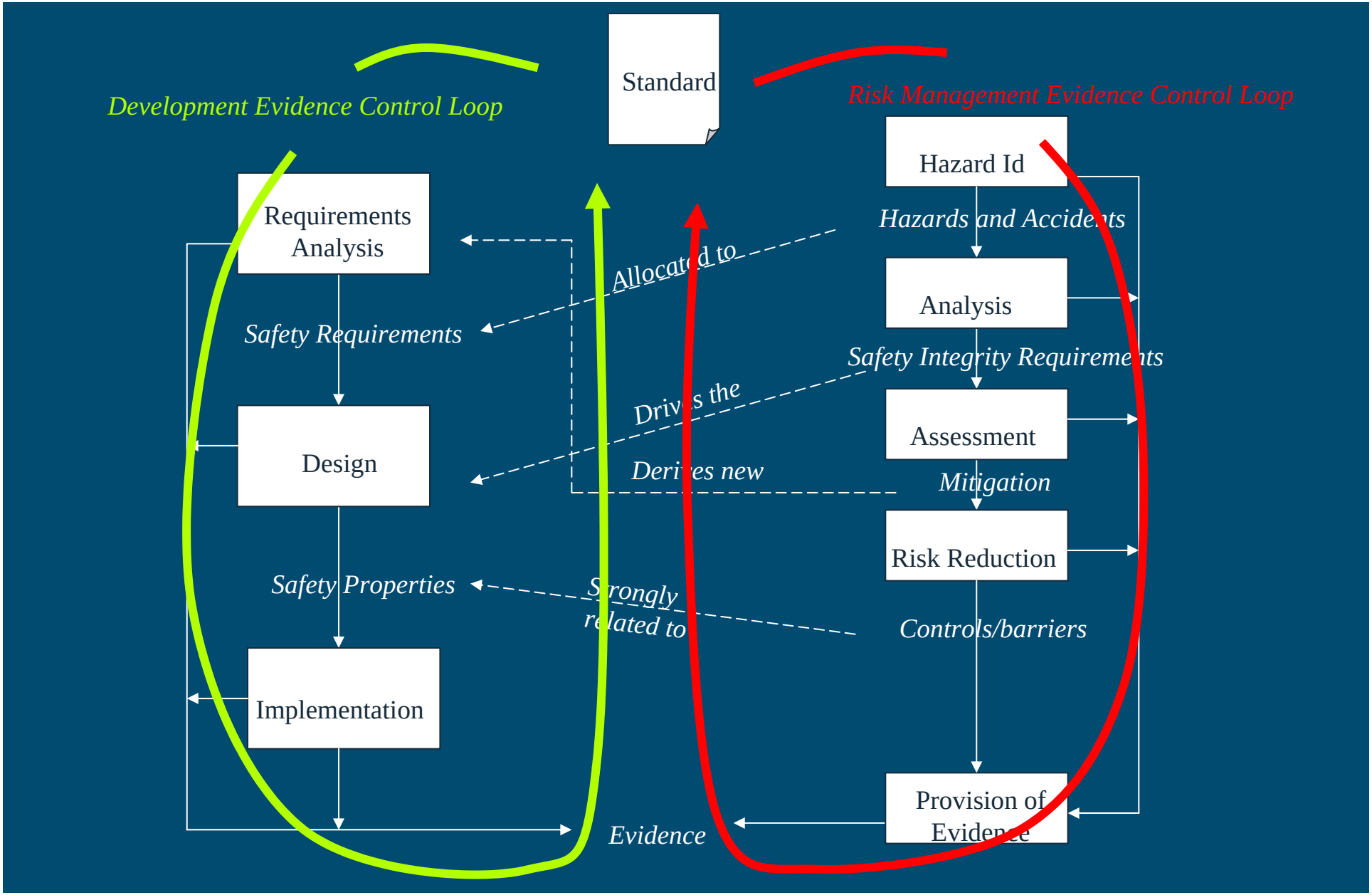
- Safety and Security Measurement white paper is a PSM working group product
- Aimed at:
  - Enhancing PSM
  - Supporting processes improvement initiatives such as CMMI safety and security and +SAFE
  - Aid companies that need to apply safety standards
- Covers the safety aspects but security still to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

Safety Process interaction - white paper

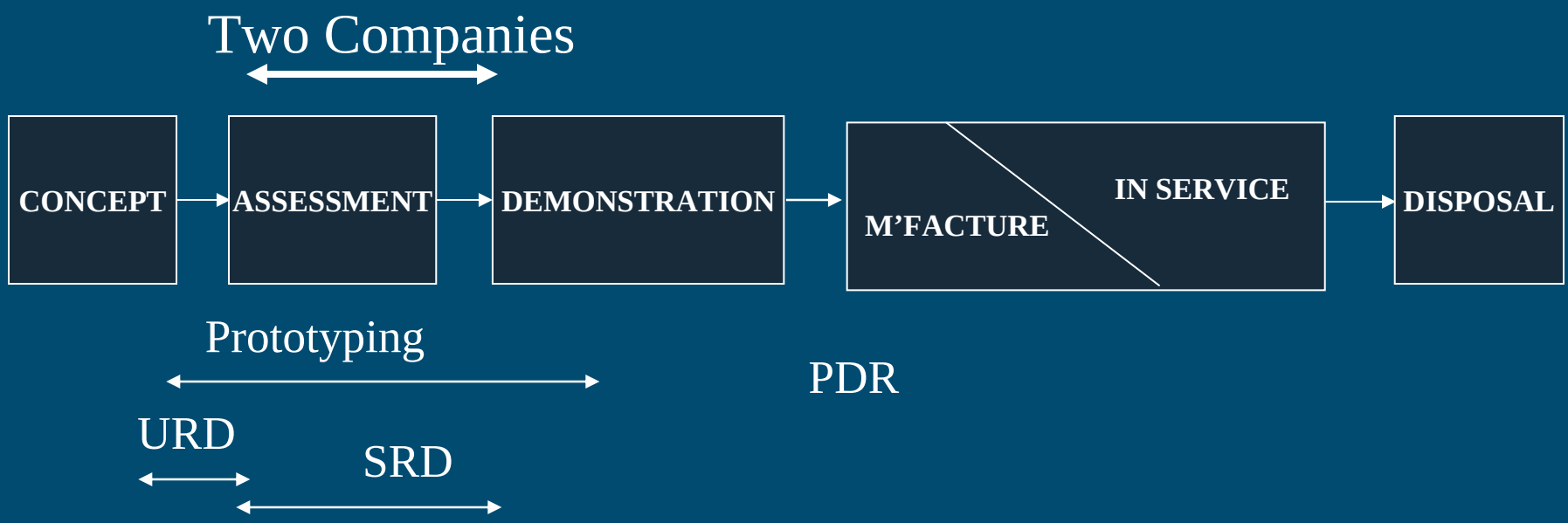


Important issues - white paper

- 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


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

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
  - Using “data sleuthing” comparison 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
  - 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

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

Future: Workshop Objectives

- Briefly review Safety & Security White Paper v 2.0; status of work; define the task of applying PSM to security measurement
- Develop an initial scan of typical information needs, measurable concepts and base measures for security
- Propose draft augmentations to the PSM tables, to serve as a starting point for further work
- Propose a plan for the work to be continued and completed, along the lines demonstrated

Future: Workshop Outputs

- Workshop Report, 5th March 2004
- Update to v3.0 of Safety & Security White Paper, due for PSM User's Conference, Keystone, July 2004. To include security measurement proposals and iCMM/CMMI AA harmonization

Questions?