Safety and Security Process Measurement

Paul Caseley - DSTL Information Management, UK
Graham Clark, John Murdoch, Tony Powell -
Department of Management Studies, University of York, UK

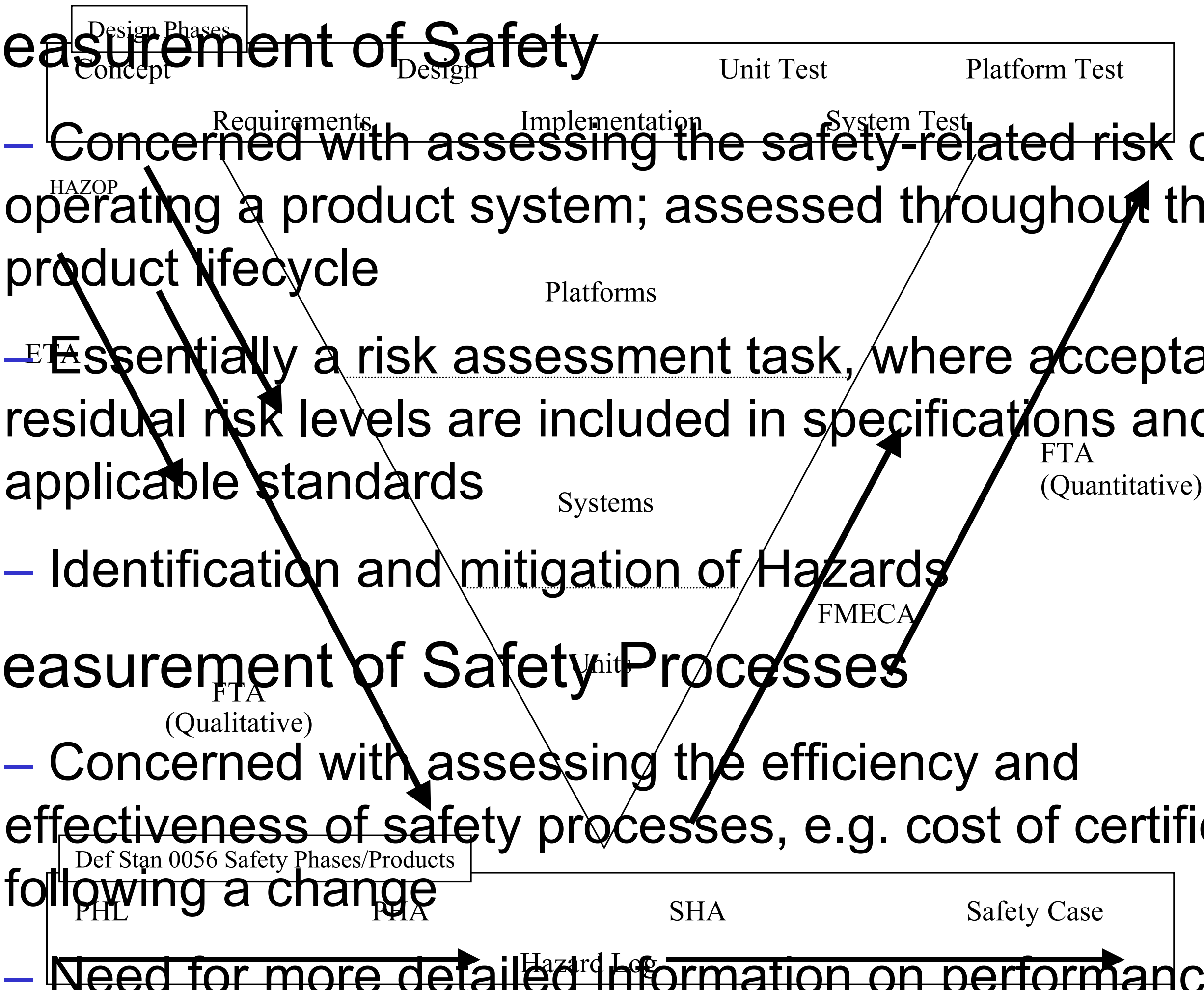
PSM Conference, Denver, 15-17 July 2003

Overview

- Safety and security processes, what are they?
- Why bother measuring these processes?
- Who benefits from safety and security process measures?
- Examples of Safety Measurement
    - A *language-based* measurement instrument
    - Comparing analysis
    - Potential Indicators
- CMMI and PSM - what's the future?

Safety and Safety Processes

- Measurement of Safety
  - Concerned with assessing the safety-related risk of operating a product system; assessed throughout the product lifecycle
  - Essentially a risk assessment task, where acceptable residual risk levels are included in specifications and applicable standards
  - Identification and mitigation of Hazards
- Measurement of Safety Processes
  - Concerned with assessing the efficiency and effectiveness of safety processes, e.g. cost of certification following a change
  - Need for more detailed information on performance of safety assessment work



Security and Security Processes

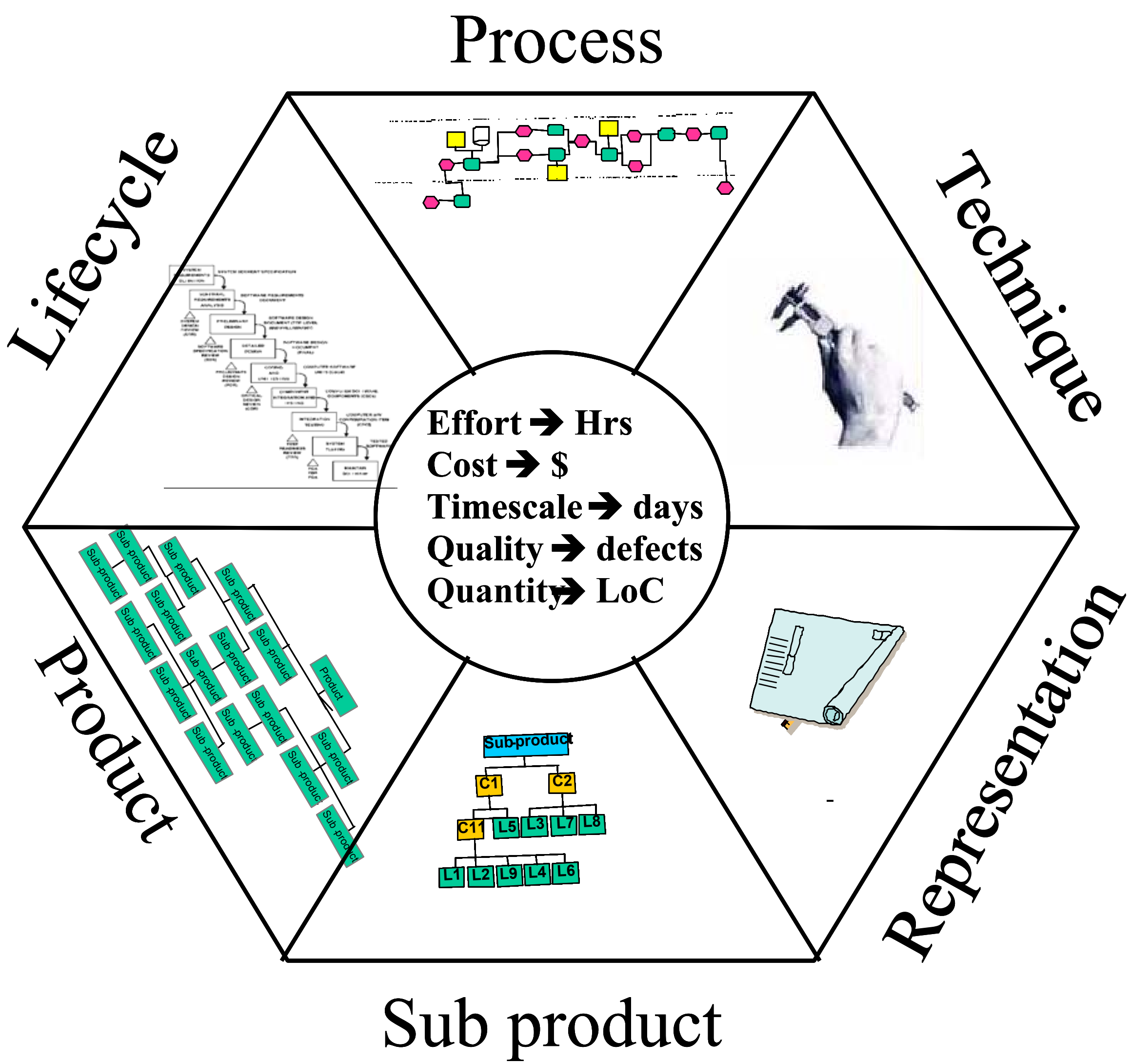
- Measurement of Security
  - Similar to safety, assessing the security-related risk of operating a product system; assessed throughout the product lifecycle
  - Just like safety it is a risk assessment task, where acceptable residual risk levels are included in specifications and applicable standards
  - Identification and mitigation of Vulnerabilities
- Measurement of Security Processes
  - Concerned with assessing the efficiency and effectiveness of security processes
  - Need for more detailed information on performance of security analysis

Who uses safety process measures?

- Business/ organisation senior managers: (Business viewpoint)
  - investment, performance
  - integrated capabilities
  - inter-organisational collaboration,
- Projects: (System development viewpoint)
  - planning, estimating, integration with other processes
  - progress monitoring and management
- Safety Engineers: (Capability viewpoint)
  - efficiency and effectiveness of safety techniques
  - appropriateness of techniques across lifecycle
  - safety process improvement

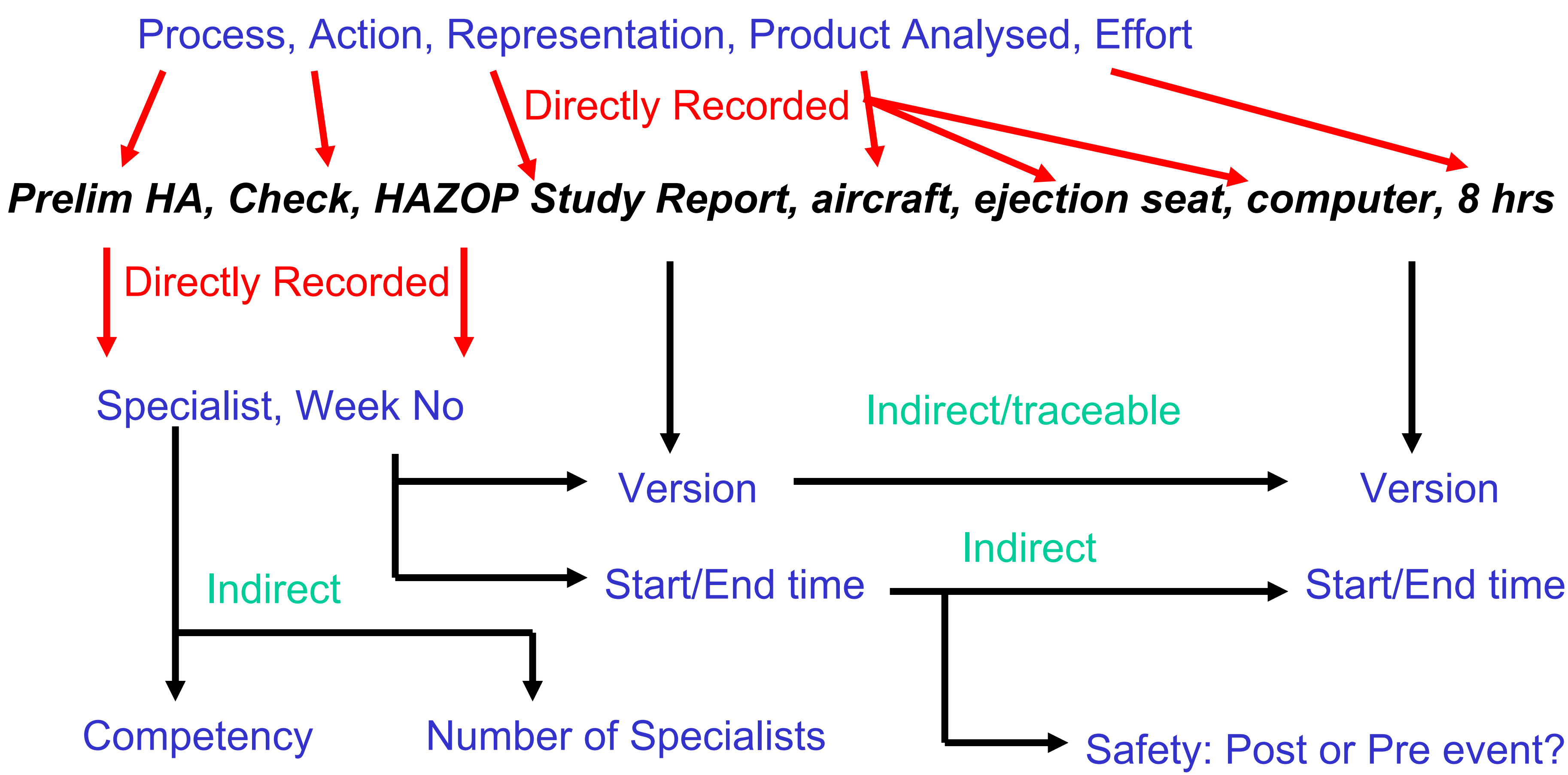
Equally applicable to Security

An organic approach to measuring



Language based measurement

"Today I checked the prelim HAZOP report for the EF ejection seat, computer"



<u>From a simple language statement up to 18 base measures with context!</u>

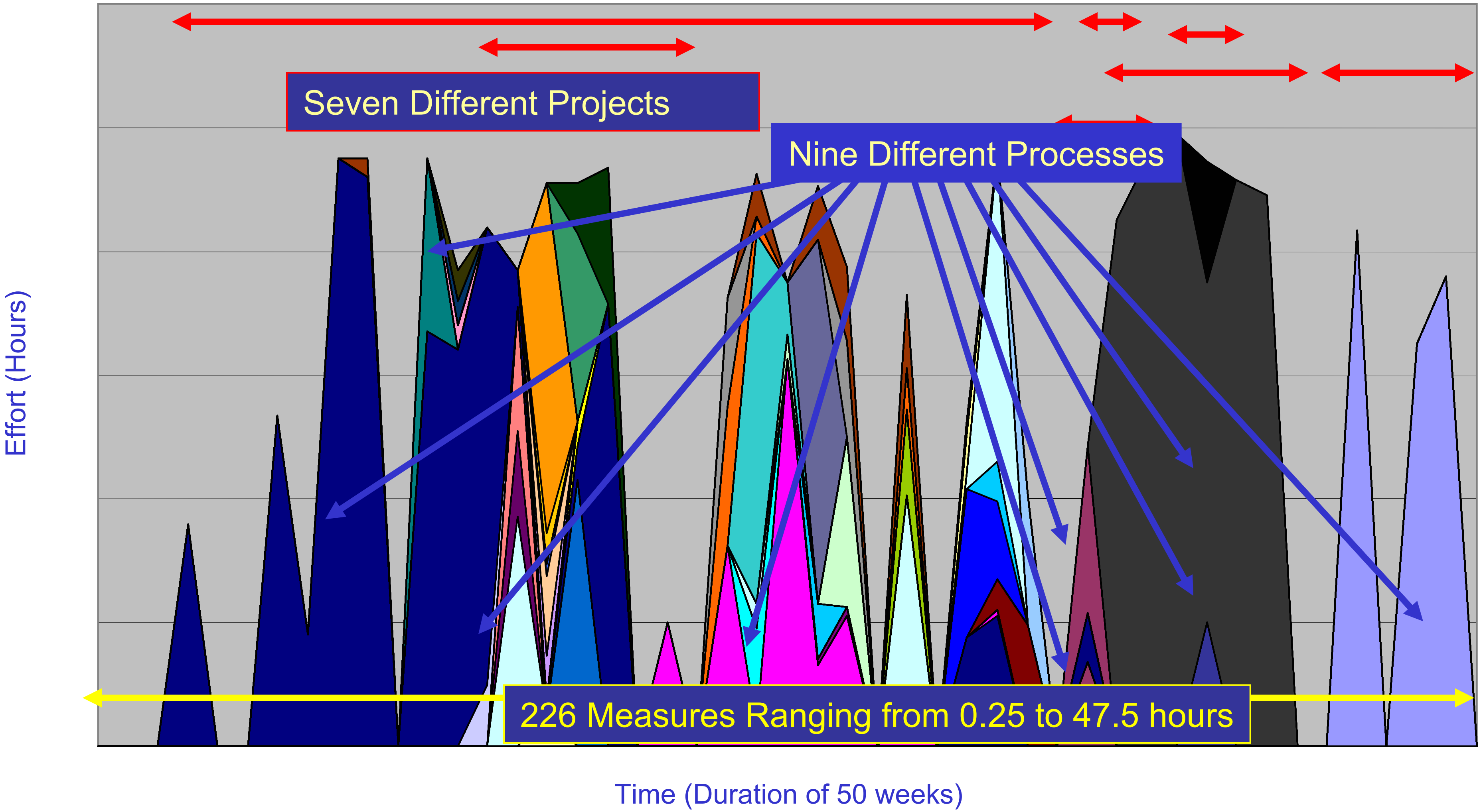
Statement construction

Process	Action	Representation	LRI/Unit	Sub-Element
Compliance	Contract Support	CLAWZ files	Software-Builds, e.g.	CSCIs, e.g.
	Develop	Compliance Process	X1	Y1
	Identify	Compliance Script	X2	Y2
	Management	Milestone Report	X3	Y3
	Produce	Modified Ada Files	:	:
	Re-Witness	Process Input Ada Files,	:	:
	Run	Staff	:	:
	Witness	tools		
		Tutoring		
		Z procedure Specifications,		
		:		
		:		

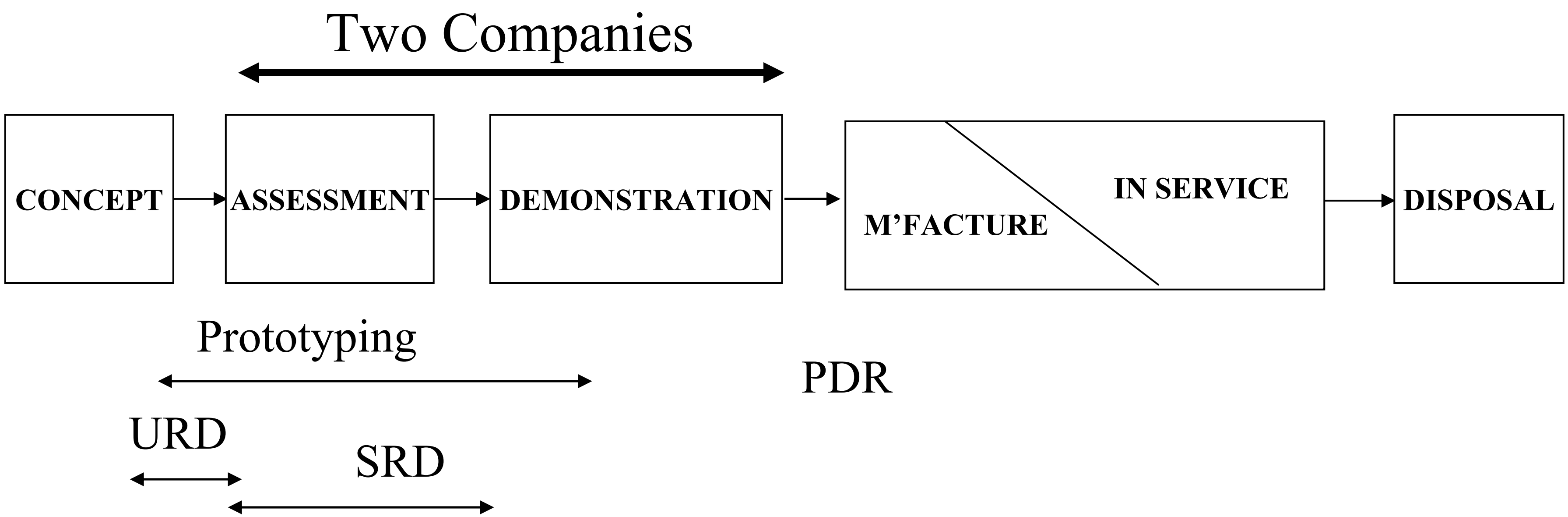
"In the *Compliance* Process, *Witness* the *Modified Ada files* for *X2, Y3* "

A record of what actually happened from the person who did it!

An individual engineer's distribution of activity



CADMID Procurement Cycle



- Two or more companies develop the user and system requirement and initial designs.
- After demonstration 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 (Security/Safety)

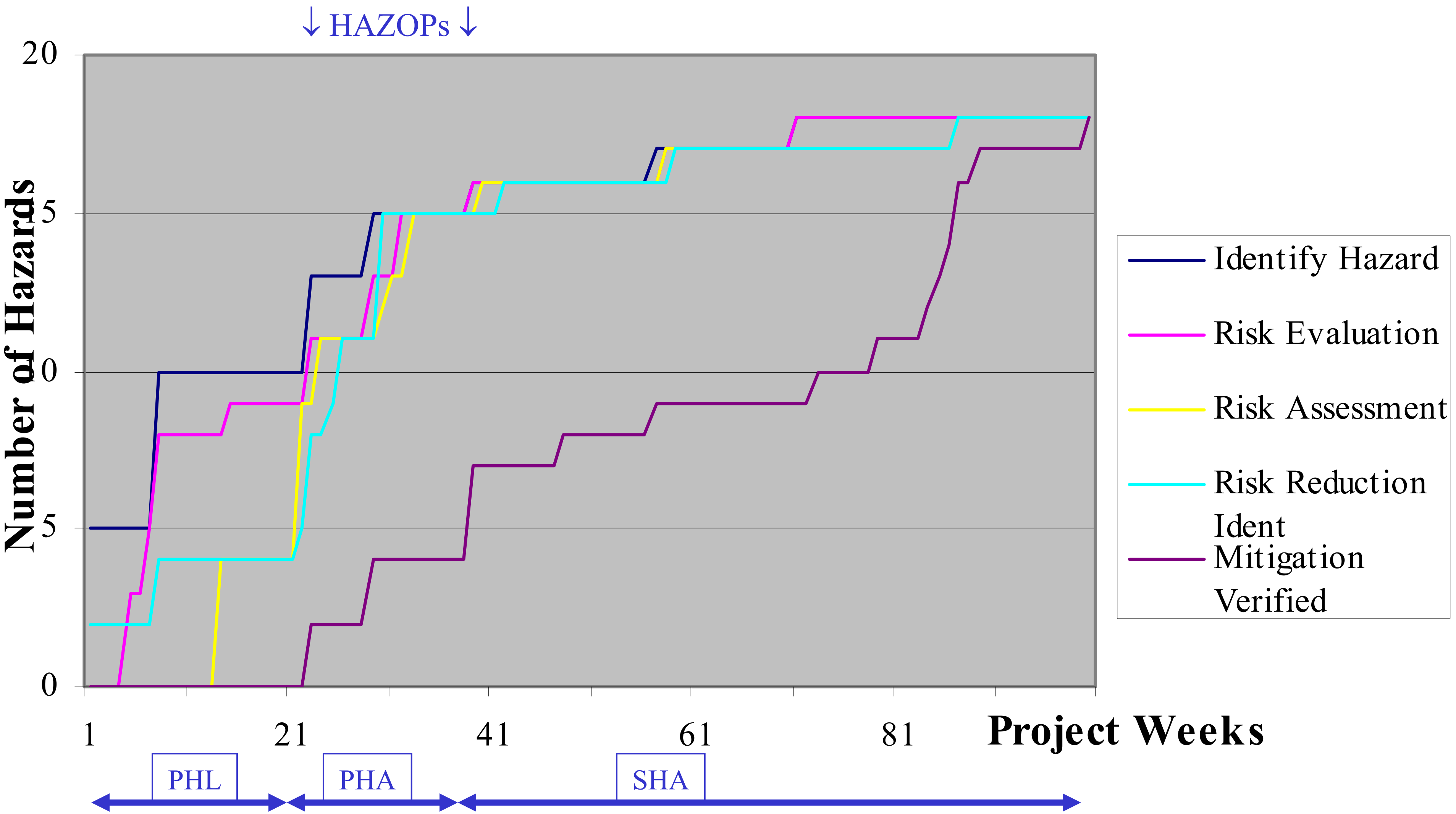
Assessment

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

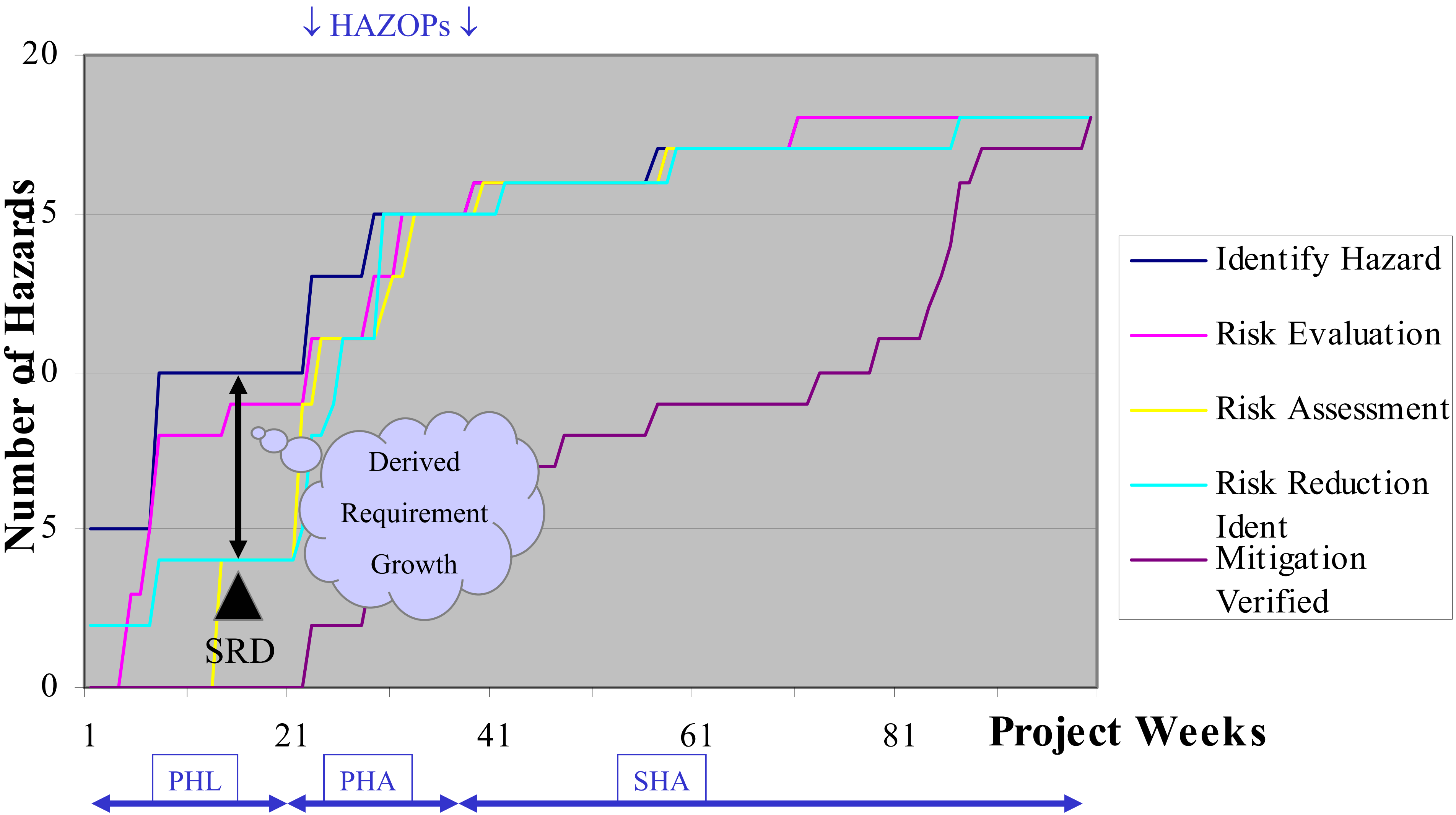
Comparing the Hazard Identification Processes

- The hazards from both teams were compared and equivalents identified
  - Using “data sleuthing” comparison method, e.g.
    - 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
  - Note: not the actual data! Results yet to be released.
  - Simple analysis gives some confidence in the quality of the identification process
  - Assumes processes are truly independent

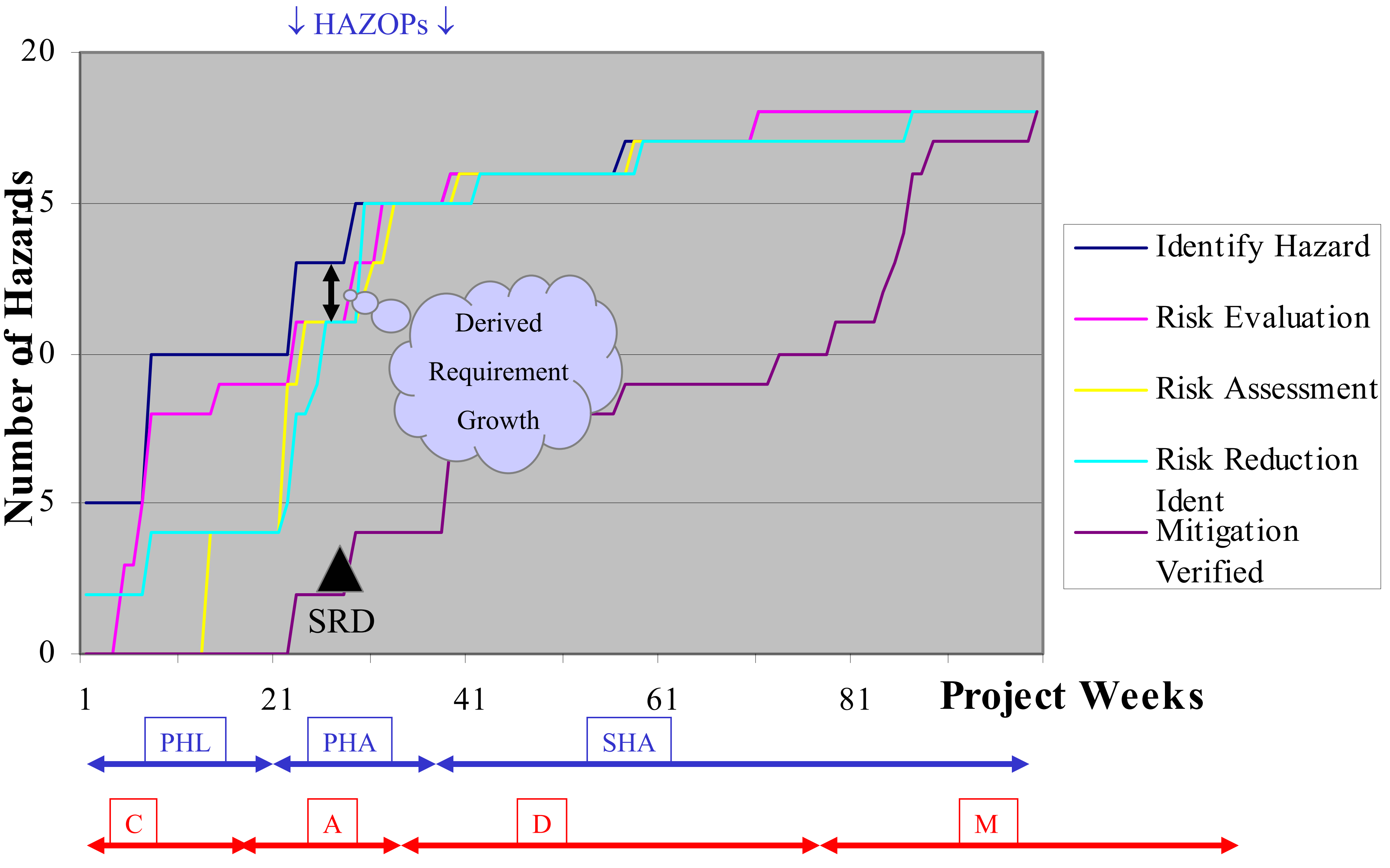
Typical Indicators - Safety Program



Typical Indicators - requirement effects

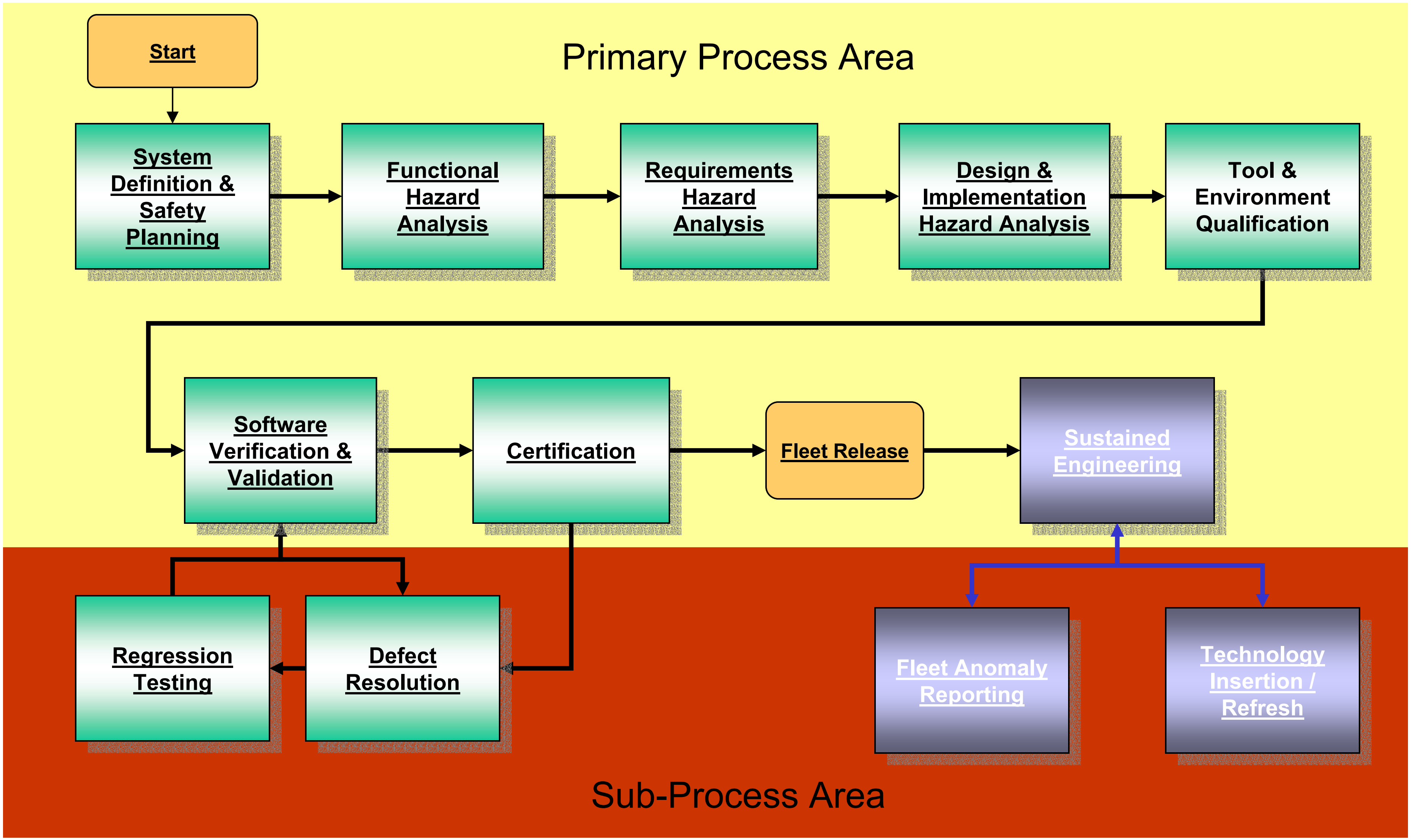


Typical Indicators - Procurement Lifecycle



Standardized software safety certification methodology for use within the US Navy for all weapon systems,

Navy's Weapon System Explosives and Safety Review Board



ICM Table: Augmentations v2

Issue - Category - Measure Mapping		
Common Issue Area	**Measurement Category**	**Measures**
Schedule and Progress	Milestone Performance	Milestone Dates
		Critical Path Performance
	Work Unit Progress	Requirements Status
		Problem Report Status
		Review Status
		Change Request Status
		Component Status
		Test Status
		Action Item Status
	Incremental Capability	Increment Content - Components
		Increment Content - Functions
Resources and Cost	Personnel	Effort
		Staff Experience
		Staff Turnover
	Financial Performance	Earned Value
		Cost
	Environment and Support Resources	Resource Availability
		Resource Utilization

Minor modifications to the existing ICM descriptions

ICM Table: Augmentations v2

Product Quality	Functional Correctness	Defects
		Technical Performance
	Supportability	Time to Restore
	Maintainability	Cyclomatic Complexity
		Maintenance Actions
	Efficiency	Utilization
		Throughput
		Timing
	Portability	Standards Compliance
	Usability	Operator Errors
	Dependability - Reliability	Failures
		Fault Tolerance
	Dependability - Safety	Hazards
		Hazard Scenarios
		Failure Modes
		Safety Assessments & Assumptions
		Mitigations
		Safety Incidents & Accidents
	Assurance - Safety	Safety Argument

Conclusion

- Discussed the measurement of *safety/security processes*
- Identified who would benefit
- Looked at a language/organic based method of measurement
- Discussed the value of comparing processes
- Looked at potential indicators and how they would benefit a project
- A sketched future development for PSM

Contact points:

Dr. John Murdoch
Department of Management Studies, University of York, UK
+44 1904 434893
jm48@york.ac.uk

Paul Caseley
DSTL Information Management, UK
+44 1684 77 1476
prcaseley@dstl.gov.uk