Practical Software and Systems Measurement

A foundation for objective project management

Safety Workshop

PSM Technical Working Group

Paul Caseley, Tony Powell

Next Steps/Action Items

Task 1, Develop White Paper - by July 2003:

- ***Literature search***
  Draft, currently being reviewed
- ***Questionnaire supported by site visits.***
  Draft, but need to identify suitable distribution medium
- ***A workshop to identify safety information needs and potential measures, by end of January 2003.***
  This workshop
- ***Development of measurement specifications.***
- ***Final White Paper - Measurement and Safety***

Task 2, Conduct Field Trials - by July 2004. ***Field trials to validate the recommendations in the white paper.***

Task 3, Update White Paper - by Sep 2004. ***Update the white paper with lessons learned from the field trials.***

Presentation Overview

Safety Process Measurement

- What is it?
- Using PSM
- Research area
- Example applications
- Safety and Security CMMI

Safety Workshop

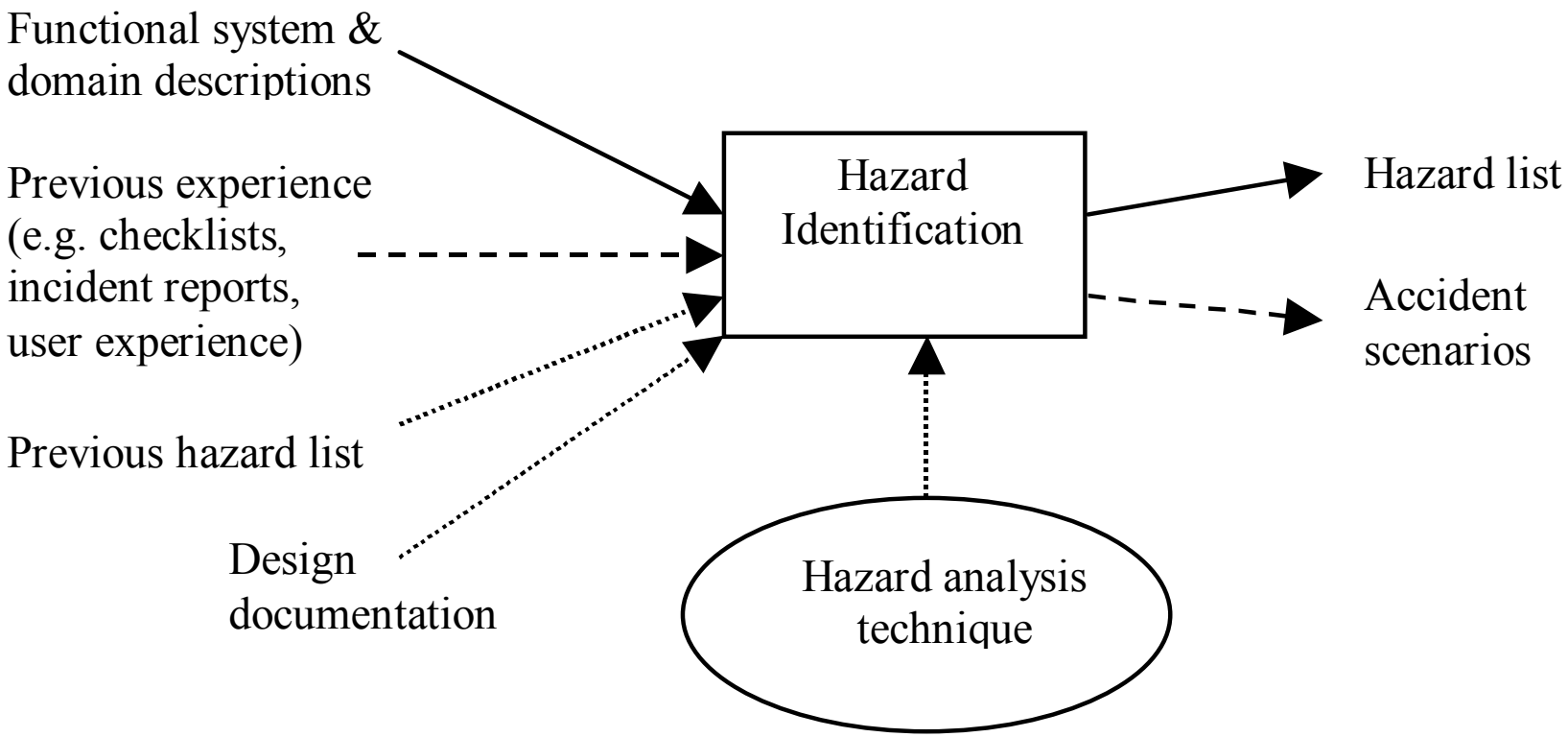
Safety Processes, what are they?

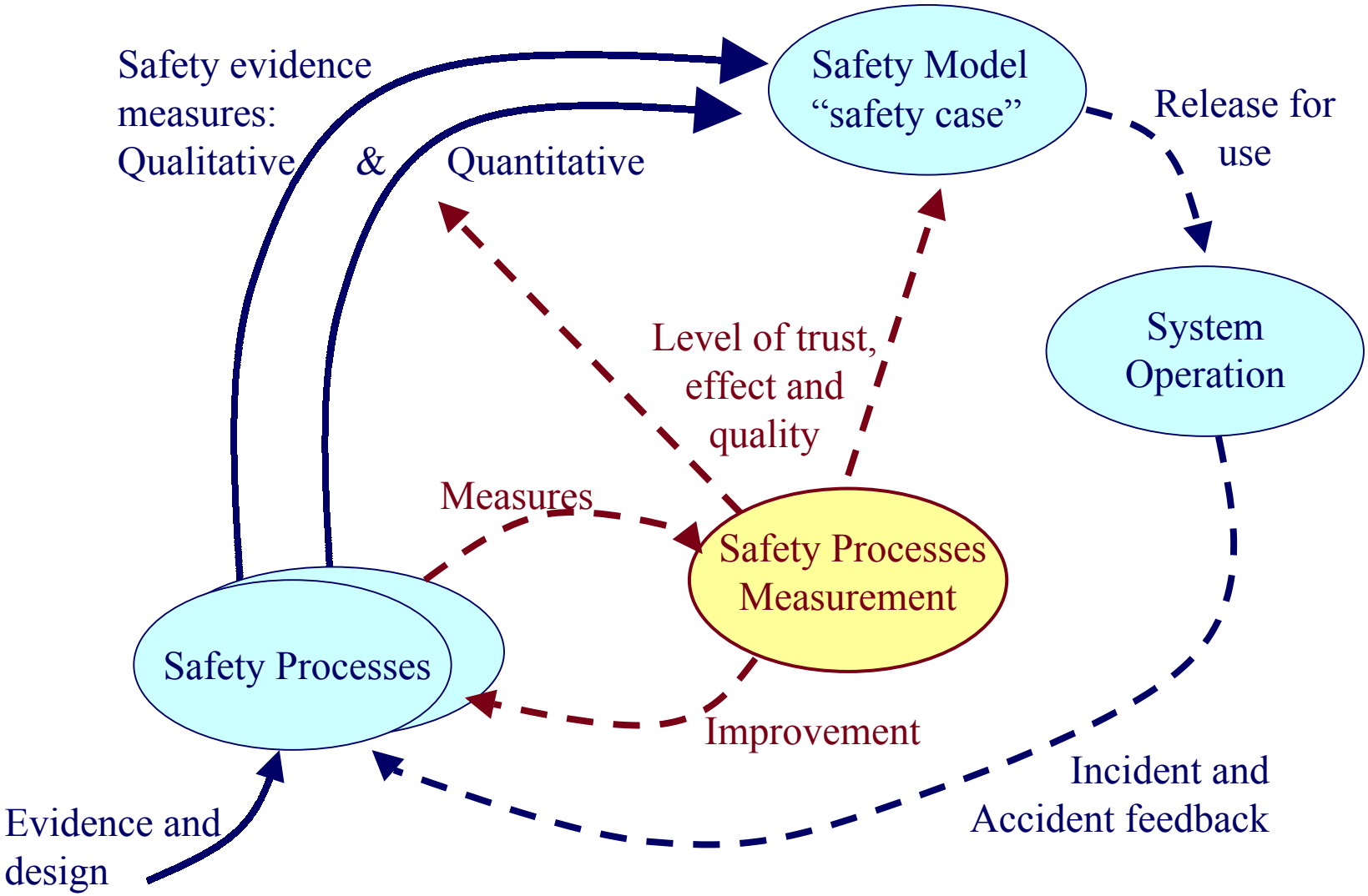
- All safety activities and techniques that produce products that in turn support the Safety of the System

Processes	Techniques
Hazard Identification	HAZOP, What if..
Preliminary Hazard Analysis	ETA, FTA ..
System Hazard Analysis	FMECA, FTA ..
Failure Integrity	FMET, Proof, Modelling ..
Accident/Incident Investigation	ETA, CCA ..
Safety Management	Hazard Logs, Plans..

- Over 200 documented techniques
- Safety is Estimated of between 1% and 15% of the system cost (possibly more for some super critical systems such as Nuclear)

Typical Input and Output Products





Safety Process Measurement

Common Issue Area	Measurement Category	Measures	Data Items; Attributes
Product Quality	Efficiency	Utilisation	Maximum capacity of resource, Maximum amount of resource established as design limit, maximum amount of resource established as performance limit, Date/time of measurement, Amount of resources used Resource type, Increment, State or Mode Operational Profile, Function , task or operation measured, Test sequence
	Usability	Operator Errors	Time period over which task was performed, Number of operators errors; Task identifier, Increment, User interface device, Priority, Test sequence, Category of operator errors, Operations document identifier
	Dependability – Reliability	Fault Tolerance	Number of single point failures, Number of identified failure modes, Number of identified failure modes with fault-tolerant design protection; Failure mode, Failure effect, Redundancy level, Type of Fault

I-C-Ms where safety is implicated or quoted

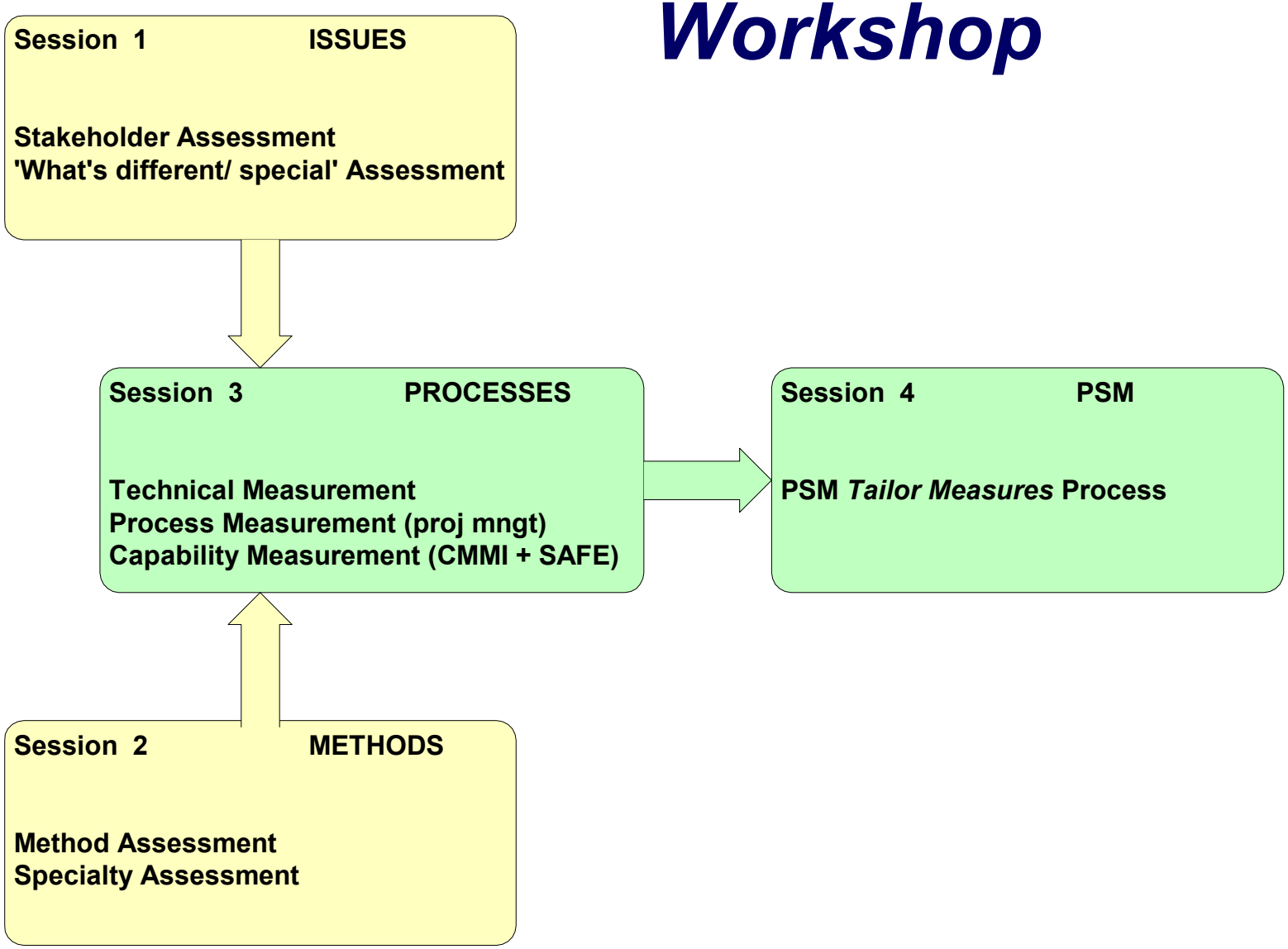
Common Issue Area	Measurement Category	Measures	Data Items; Attributes
Customer Satisfaction	Customer Support	Request for Support	Number of requests, Number of reported defects; Increment, Priority (safety hazard, critical impact, minor), Type of support requested, Request mechanism, Non support resolution (request beyond support agreement), Status code (open, closed) Customer or originator of request, Activity when problem was discovered.
		Support Time	Number of requests received, Average response time, Maximum response time, Average time to resolve, Maximum time to resolve Type of maintenance required, Increment, Priority (safety hazard, critical impact, minor), Non support resolution (request beyond support agreement), Customer or originator of request, Request mechanism.

I-C-Ms where safety is implicated or quoted

Using PSM to Manage Security/Safety

- Schedule and Progress
  - Ensuring safety processes correctly influence the program
  - Estimating safety impact
- Resources and Cost
  - Competency of personnel
- Product size and capability
  - New threats/hazards always add new requirements
  - Unique safety products (FTA, ETA, FMECA, safety cases)
- Technology Effectiveness
  - Novel designs new safety issues

Workshop


Session 1 ISSUES
Stakeholder Assessment
'What's different/ special' Assessment
Session 3 PROCESSES
Technical Measurement
Process Measurement (proj mngt)
Capability Measurement (CMMI + SAFE)
Session 4 PSM
PSM *Tailor Measures* Process
Session 2 METHODS
Method Assessment
Specialty Assessment

Final Session to add to PSM

Schedule and Progress	*Work Unit Progress*	*Safety Requirements Status*
		Safety Action Item Status
Product Size and Stability	*Physical Size and Stability of safety-critical systems, at different risk levels*	*Subsystems*
		Components
		Interfaces
		Operations
		Physical Dimensions (zones)
	Functional Size and Stability of safety-critical systems, at different risk levels	*Requirements*
		Modes
		Functions
Product Quality	*Safety*	*Hazards*
		Hazard Scenarios
		Failure and Contributory Modes in Hazard Scenarios
		Coverage
		Single Point Failures
Process Performance	*Process Compliance*	*Compliance with regulatory & advisory models*
		Certification Data
	Process Effectiveness	*Operational safety-related 'events'*
Technology Effectiveness	*Technology Suitability*	*Safety Experience/ application*
Regulator Satisfaction	*Regulator Feedback*	*Survey Results*
		Performance Rating
	Regulator Support	*Support for certification process*

UK Law: Measurement for ALARP

- **As Low as Reasonably Practicable (ALARP)**
  - *'Low'* **refers to the effectiveness of safety processes, i.e. are they making systems and software safe.**
  - *'Practicable'* **refers to the efficiency of safety processes, i.e. how much is enough?**

- **Understanding ALARP Strategies**
  - **We need to understand the efficiency and effectiveness of existing safety processes in order to support ALARP arguments.**
  - **For example, does a HAZOP identify all the hazards? If not how many are identified and are they the important ones? Is it only suitable for some domains?**

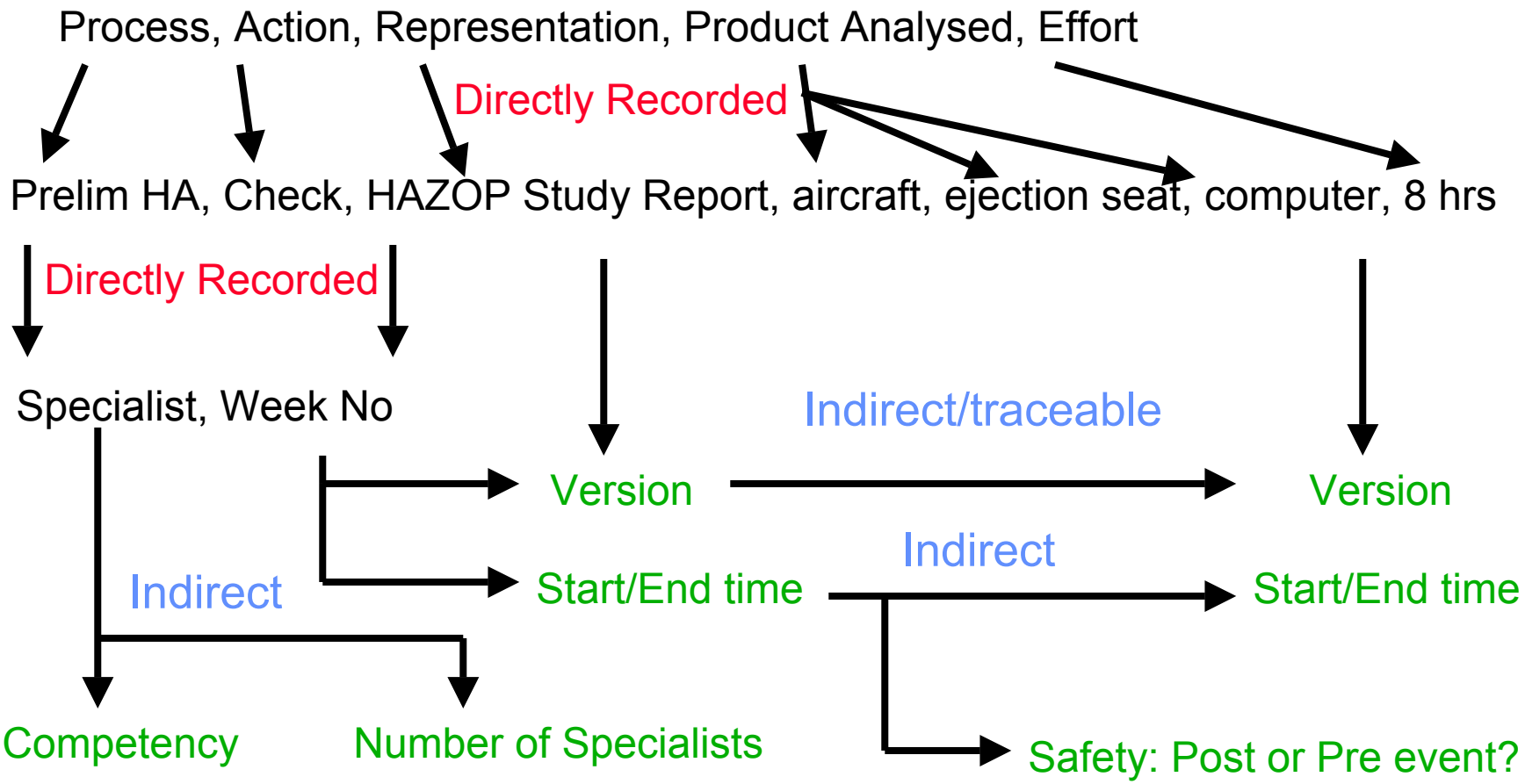
Research Directions

- Existing Research/Practice
  - Tribble (CBA from survey)
  - Soukas (empirical evaluation of hazard identification)
  - Rouhianinen (checklist)
  - Organisational Assessment: CASS, CMMI, TÜV, Nuclear
  - Practical System and Software Measurement (PSM)
  - Competency Assessment
  - Bayesian Belief Networks
- Directions
  - CMMI, Integration Assurance Practices, +SAFE
  - PSM (identification of safety attributes)
  - Organic Measurement (PEL)
- Measurement requirements
  - Industrial measuring processes?
  - Capable of fine-grained data
  - Had to successfully migrate across different organisations
  - Needed to carry a context of activities with the measure

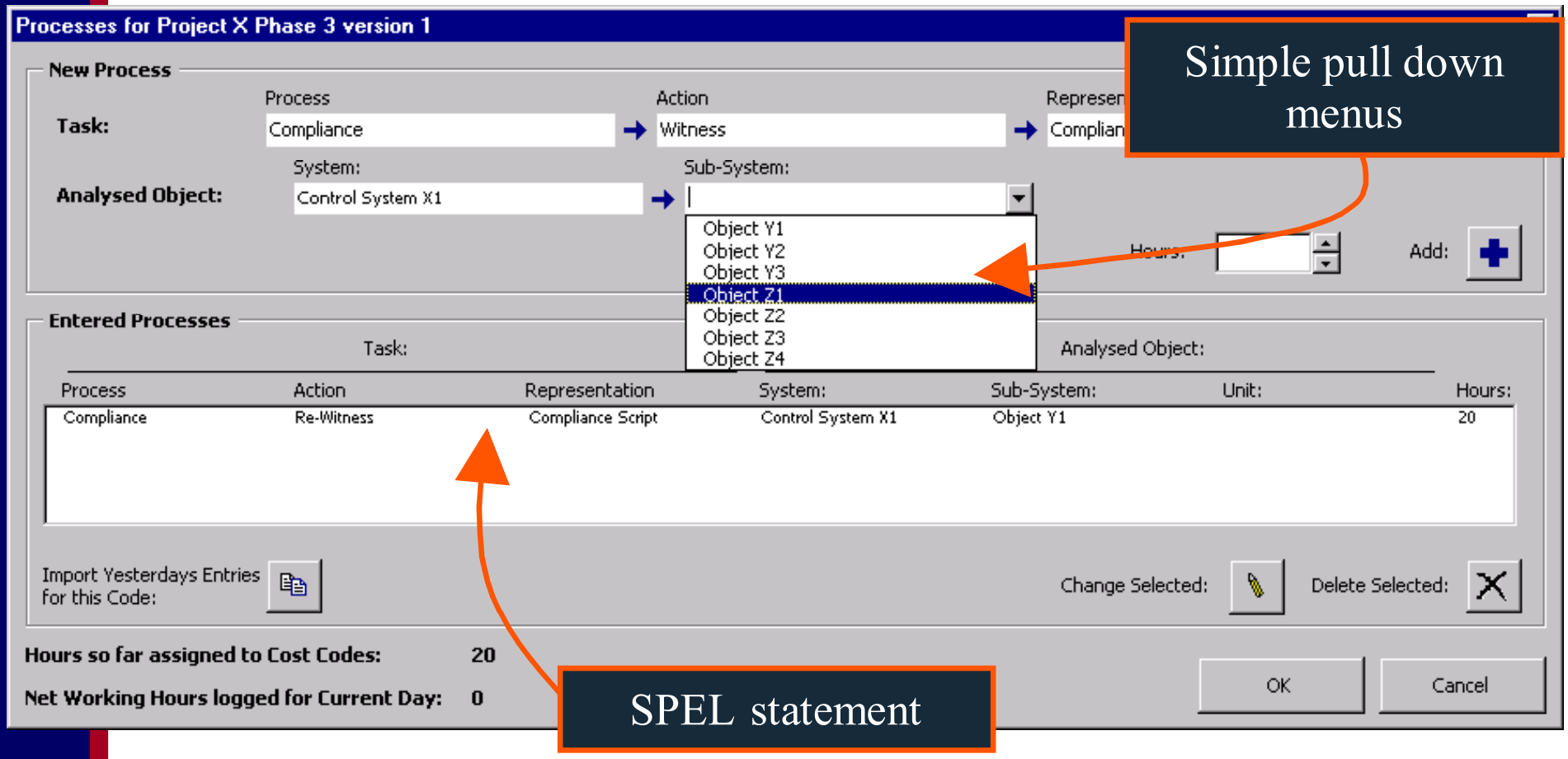
The SPEL Sub-Project

- Part of a MoD Corporate Research Programme
  - Supporting Safety Process Measurement for ALARP
  - 2/3-year project between DSTL/MoD, QinetiQ, BAE SYSTEMS and University of York
  - Overall aim is to provide a practical framework for measuring safety processes
- Methods and Research
  - Identify practical and useful safety process measurement attributes
  - Use of Safety Process Engineering Language (SPEL) technique to capture fine-grained process measurements.
  - Trials of SPEL on projects within QinetiQ, BAE SYSTEMS and trials within Rolls-Royce and Invensys to follow.

SPEL Measurement Technique example



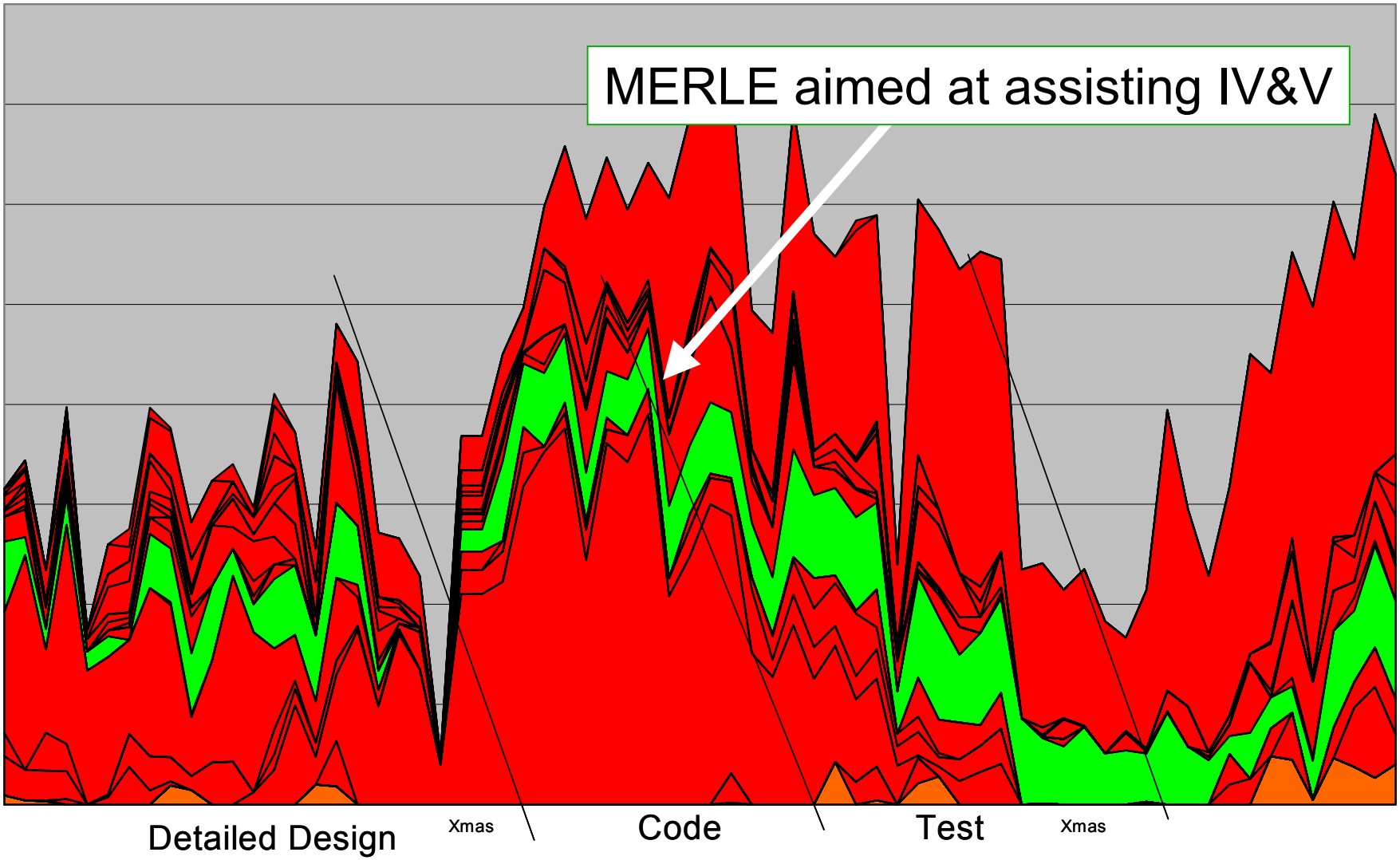
Example of SPEL collection



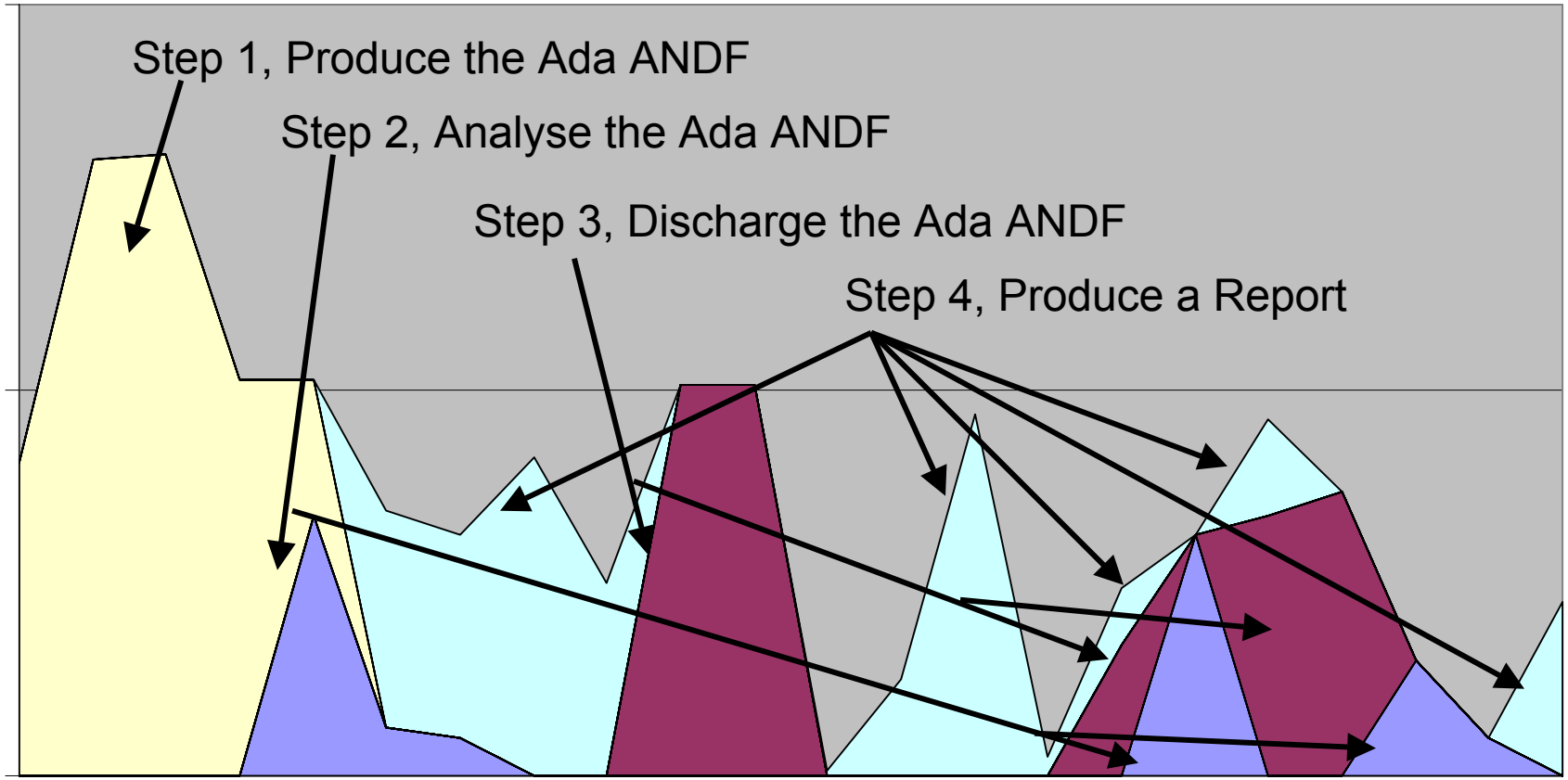
Case Studies

- **Case Study 1 – MERLE on a control system**
  - ***Aim:*** *Experiment to discover if new static verification process is efficient and effective and practicable.*
  - ***Context:***
    - *Additional assurance requested by customer*
    - *Developer willing and co-operative*
    - *MERLE claims to find potential runtime errors in source code*
    - *team size 2, project duration ~10 weeks, applied as a post development analysis*
  - ***Process:*** *definition of starting grammar for SPEL, refinement of grammar with the users of MERLE, data collection using spreadsheet tool, analysis and identification of potential improvement, presentation of results*

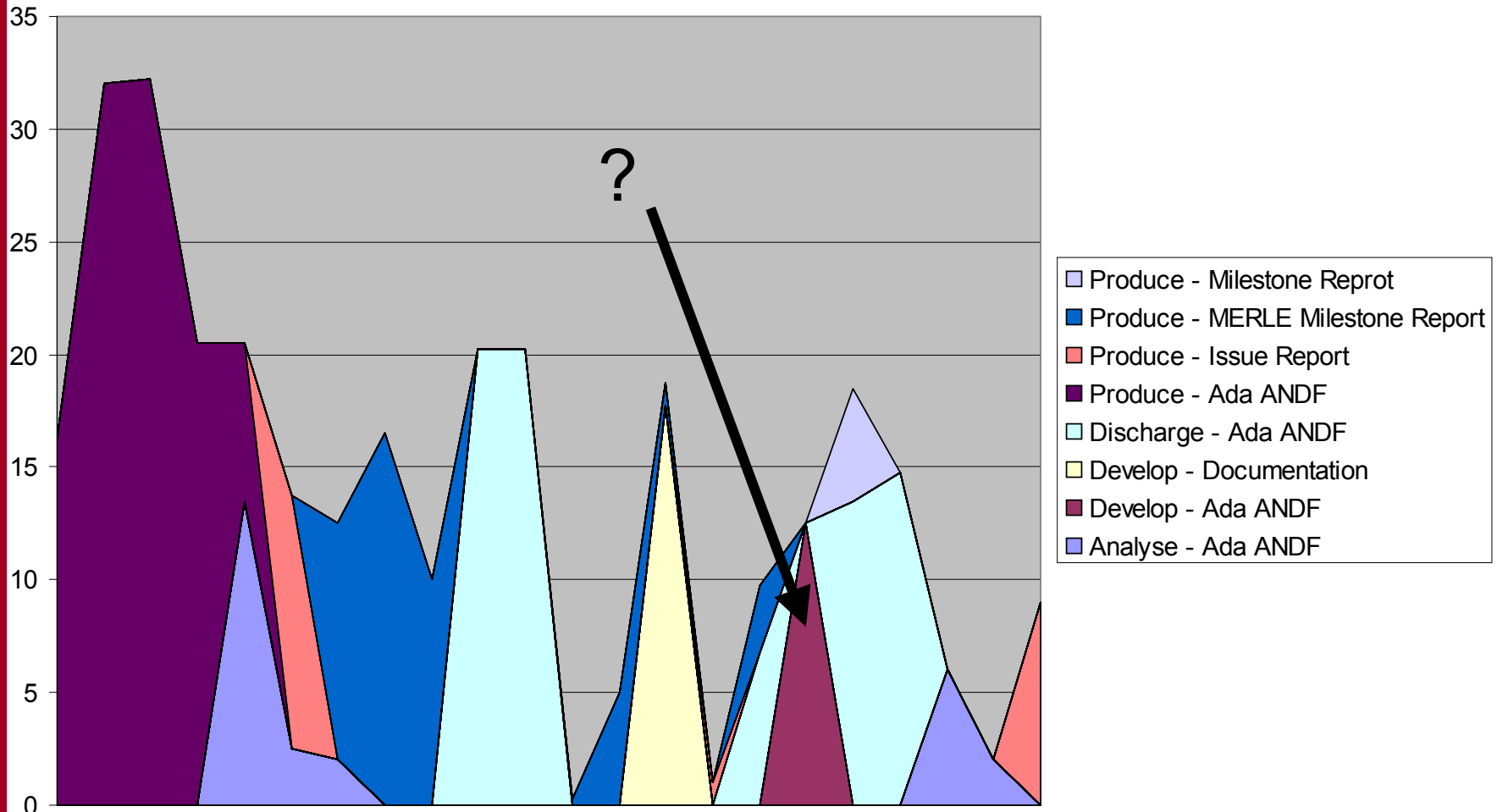
Large scale S/W development cycle



MERLE – Reconciled data on the Control System



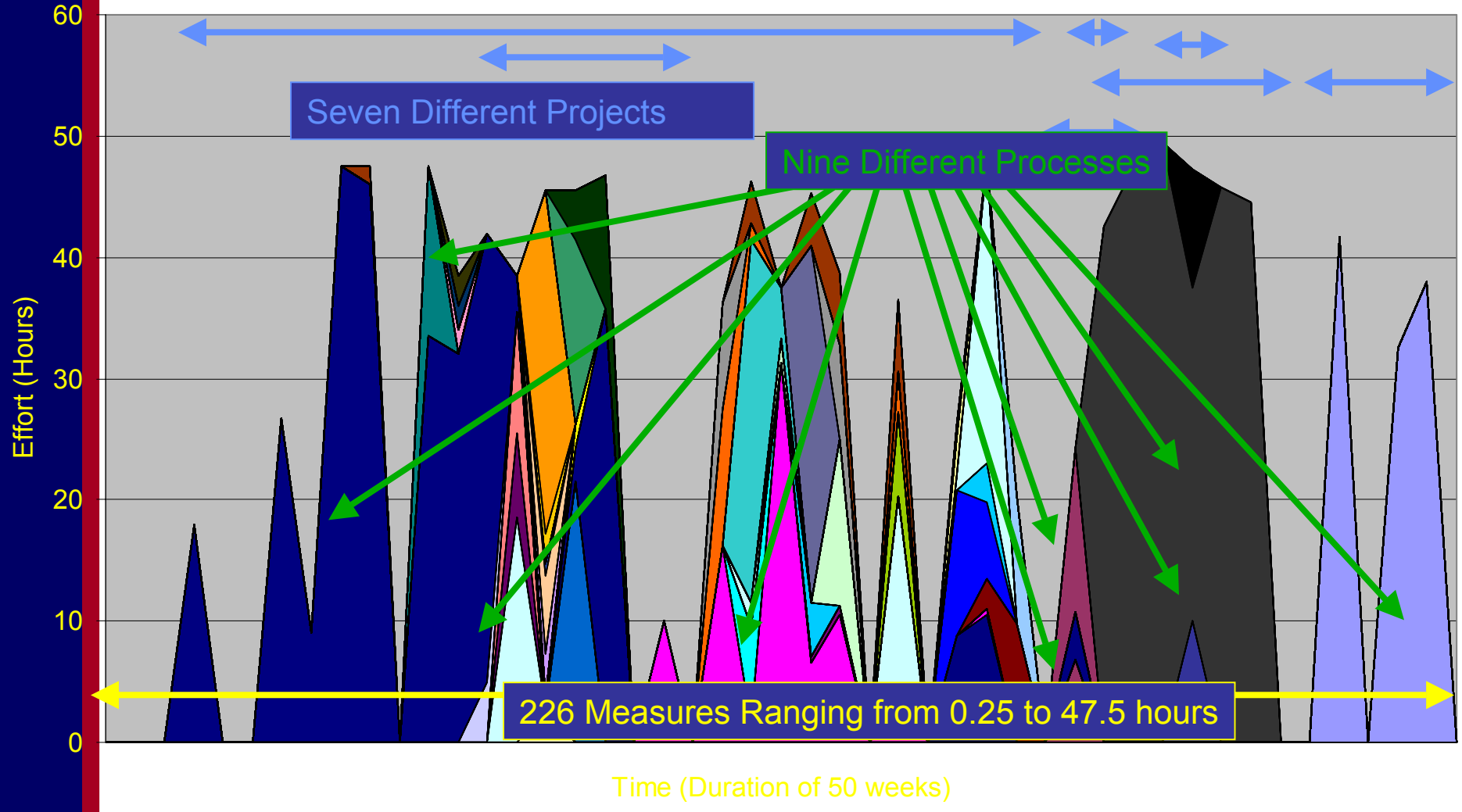
MERLE: Action, Representation



MERLE – Some provisional figures

- Case 1
  - Full process (per hour)
    - ~1066 LOC
    - ~377 SLOC
    - ~108 BELOC
    - per issue ~ 1.1
  - Producing Warnings only
    - ~2860 LOC
    - ~1010 SLOC
    - ~291 BELOC
  - Producing and Discharge
    - ~1400 LOC
- Case 2
  - Full process (per hour)
    - ~971 LOC
    - ~331 SLOC
    - ~110 – BELOC
    - per issue ~ 2.6
  - Producing Warnings only
    - ~2264 LOC
    - ~959 SLOC
    - ~320 – BELOC
  - Producing and Discharge
    - ~1366 LOC
    - ~466 SLOC

Example of an Individual



Insights

- **Results and Observations**
  - Identification of overheads, predictive measures, effectiveness
  - Improvements in novel processes for software verification
  - Confirmation of anecdotal perspectives on safety processes

- **Implications**
  - Further refinement of terminology and collection approach.
  - Ownership of measurement process passed back to team.
  - New questions being asked about safety process and ALARP.

Conclusions and Future Work

- Conclusions
  - SPEL presents a promising way forward for measurement of fine-grained aspects of safety processes.
  - Industrial trials are in their early stages but have already given examples of the value of fine-grained data in support of ALARP
- Future Work
  - Further trials are planned and participation of others is welcome.
  - Linking SPEL approach into PSM and CMMI.

Contact Information

- Paul Caseley
  - Information Management, DSTL Malvern, St Andrews Rd, Worc, WR14 4RY
- Graham Clark
  - BAE SYSTEMS Research Fellow, Department of Management Studies, University of York, Heslington York YO10 5DD
- Antony Powell
  - Lecturer, Department of Management Studies, University of York, Heslington York YO10 5DD

Workshop Participants

Participant	Area of Interest
Paul Caseley	Safety/Security Process measurement
John Murdoch	Safety Measurement