DARP
HIRTS

Computer Science Department
Department of Management Studies

THE UNIVERSITY of York

Document Number	Version	Status	Date
DARP/TN/3/02	6	Issued	06 June 2003

Title

Report of the Safety & Security TWG 27th March 2003

Summary

Input material and summary report for the PSM Safety and Security TWG, 27th March 2003, Washington.

Authors
Paul Caseley, John Murdoch

Approved

Distribution:	General	Strand 1	Strand 2	Strand 3
	PSM Office			Paul Caseley
				Graham Clark
				Tony Powell
				John Murdoch
				Claire Lee

Document History:	Version	Status	Date
	6	DRAFT	06 Jun. 03

Table of Contents

1. INTRODUCTION 3

2. WORKSHOP RESULTS 3

3. IDENTIFIED ACTIONS 4

4. INDICATOR FOR SAFETY AND SECURITY 5

5. WORKSHOP SCHEDULE 6

6. WORKSHOP INTRODUCTION 7

7. SESSION 1: ISSUES 10

8. SESSION 2: METHODS 15

9. SESSION 3: PROCESSES 17

10. SESSION 4: AUGMENTING PSM MATERIALS 19

1. Introduction

This report summarises the results of the PSM Safety and Security TWG meeting, held 27th March 2003, Washington.

Sections 2-4 present the results and recommended actions. For completeness, workng materials prepared in advance of the TWG meeting are included (Section 5 onwards).

2. Workshop Results

The workshop delegates attempted to follow the planned schedule of work (Sessions 1 to 4 as described in Section 5 following). However this proved to be impractical. The group discussed each Session's work and debated many of the questions highlighted. A core issue was the extension of the CMMI to include the measurement of safety and security. It was decided that, in order to satisfy the extention of CMMI, basic measures were required. It was also decided to create measures that could be used generically for both the safety and security domains.

The basic template of levels of measurement to meet the CMMI need was as follows:

Level 1-2 on the CMMI scale. A realisation that some CMMI organisations are at level 1-2 thus their measurements will need to be relatively simple, for example:

Allocation of staff and planning a schedule of work for a safety programme.	
Start up measure:	Safety Plan (draft, review and issue)
	Appointment of staff
	Allocation of budgets
	Are the tools for safety appropriate, e.g. certified
Basic recording measures	Detailing mishaps and hazards
	Hazard log/ repository

Level 3 on the CMMI scale. Organisations have to manage the safety programme, thus there should be indicators of progress of safety programme:

Monitoring the maturation of hazards
Monitoring the maturation of safety models/ safety case
Monitoring safety requirements growth
Estimating and monitoring proportion of the project that is safety related
Measuring safety process to determine if they are behaving as predicted

Level 4-5 on the CMMI scale. Genuine use of measurement to show improvement in the safety/security of processes:

Effect of process on other factors e.g. requirements
Process improvement, effectiveness best for project

This led to a debate on the proposed 'strawman' solutions (Section 10 below). Individual measures were brainstormed and it was concluded that many of the strawman proposals were

valid but could be incorporated by expanding the existing text in PSM to specifically include safety and security. Thus the group decided that we must build on the existing strengths of PSM wherever possible, limiting complexity of PSM. The strawman table was then modified to that below:

Schedule and Progress	Work Unit Progress	Safety Requirements Status Already covered but the current PSM guidance needs to be expanded to include safety and security requirements. Review current requirements status specification table (part 3). Review part 5 to ensure the description 4.0b (note terminology needs to be in line with ISO standard).
		Safety Action Item Status (as above; need to review current text in PSM)
Product Size and Stability	Physical Size and Stability of safety and security critical systems, at different risk levels	Subsystems (proportion of system)
		Components (number and proportion of system)
		Interfaces (number and proportion of system)
		Operations (proportion of system)
		Physical Dimensions (zones)
	Functional Size and Stability of safety and security critical systems, at different risk levels	Requirements (for comparison)
		Modes (impact on operations)
		Functions (for comparison)
Product Quality	Integrity Assurance (Safety and Security)	Threats (Hazards and Vulnerabilities) Characterization using probability, consequence, risk levels and mitigation
		Threats Scenarios (Hazards and Vulnerabilities)
		Failure and Contributory Modes in Threat Scenarios
		Coverage
		Single Point Failures: is this relevant to security? Is this a back door?
Process Performance	Process Compliance	Compliance with regulatory & advisory models What is a realistic base measure? This is not a black and white issue. How many units are subject to 100% MC/DC testing?
		Certification Data. Is this a safety case? How complete is the certification data?
	Process Effectiveness	Operational safety-related 'events' Defects and escapes; where were they found? When were the hazards found? Effectiveness and timeliness of the process?
Technology Effectiveness	Technology Suitability	Safety Experience/ application Certification of tools and processes Appropriateness of the processes for technology

3. Identified Actions

It was judged that product quality measures seemed to be the most essential and are already defined for many projects, e.g. a Hazard or Vulnerability is usually defined by the appropriate project standard. Given this observation, the following actions were identified:

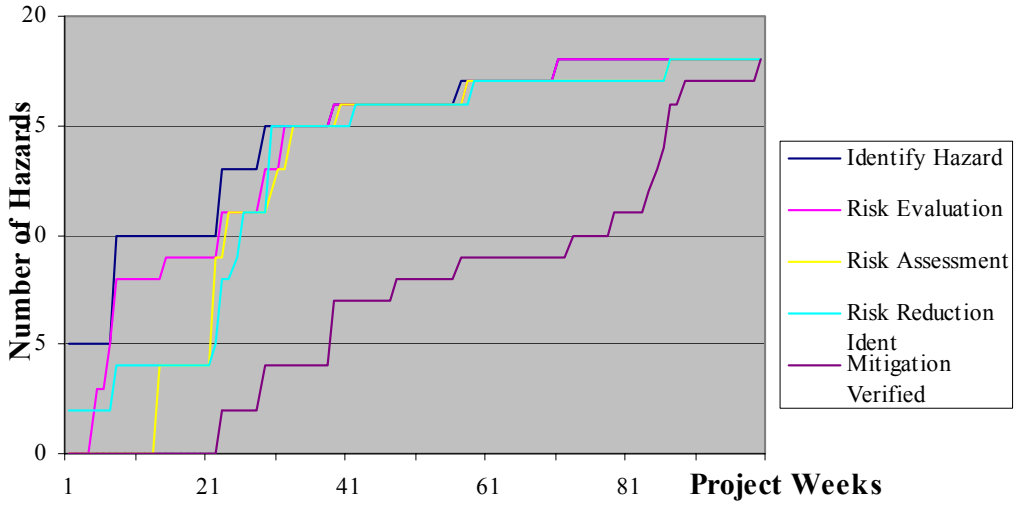
	Action
1	Write up measurement constructs for the product quality measures and consider the requirements of CMMI Integrity Assurance
2	Modify the existing PSM tables (including those that are already written in the new format) to include safety and security
3	Formalise results for presentation at PSM conference
4	Identify a project to use the measures

4. An Indicator Concept for Safety and Security

The design of a measurement construct that indicates progress in safety/ security work was considered. An indicator could be developed that uses threats (hazards/vunerabilities) to monitor the progress of the safety/security programme and derived requirements growth due to identification of Hazards. It is based on the concept of a risk management process, as shown below:

An Overview of the Risk Management Process

The risk management process maps to the proposed CMMI security and safety extensions. Project managers and safety specialists could monitor each of the process stages of risk management, i.e. Identification, Analysis, Assessment and Reduction. Thus, a safety programme could lead to results like those sketched below (this graph is purely speculative):



The step changes in the graphs may be traced to particular safety process events such as conducting a HAZOP assessment. The difference between hazard identification and mitigation identification would be indicative of progress in the safety process. It is also an indication of potential requirements growth.

Progress of safety work is also dependent on the confidence established that all hazards (at different risk levels) have been found and that all failure modes and scenarios leading to known hazards have been identified. These 'completeness' issues are indicated by the achieved product coverage of safety assessment work. Historical data seems to be involved also.

Other candidate indicators include safety incident/ accident measures and assumption log measures.

The following sections record the original workshop plans and inputs.

5. Workshop Schedule

The following schedule was originally proposed for the TWG meeeting. Further details are in the pre-read material and the vugraphs.

INTRODUCTION	Agree Orientation, planning, assumptions. Agree Objectives for the day
SESSION 1: ISSUES	Identify typical issues and information needs associated with safety and security specialties. Identify things which are different or special about safety and security work, compared with software and systems development processes
SESSION 2: METHODS	Identify measurement opportunities, derived from method-level assessment. Identify measurement opportunities, derived from a consideration of safety and security specialties.
SESSION 3: PROCESSES	Identify measures derived from process-level assessment, emphasising the performance of integrated work processes. Identify mappings between issues of concern, information needs and measures in the safety and security specialties.

SESSION 4: PSM	Augment PSM materials with advisory material appropriate for safety and security process measurement. Integrate results of previous sessions and apply to the PSM framework. Select key measures.
REVIEW, PLAN	Assess Workshop efforts. Develop outline plan for further work. Agree reporting of results.

6. Workshop Introduction

Some pre-read material was developed for the meeting, including the following questions:

1	What is the status of safety/ security work re PSM?
2	How much has been done to date?
3	How is it being taken forward? Just the workshops or a SIG, for example?
4	Should the Workshop itself plan an ongoing arrangement?
5	What is the progress of the PSM extension to cover SE? How is the PSM 4.0b version 'viewed'? Are subsequent versions being planned?
6	What is the relationship between PSM and CMMI? Is the Workshop looking exclusively at supporting CMMI application to safety/ security?
7	In terms of the CMMI safety/security extension work, how is 'security' defined?
8	What are the perceived challenges presented by safety and security, as far as PSM extension is concerned?
9	What are the objectives of PSM in these specialties?
10	Is there an established PSM development method, as distinct from a PSM *application* methodology?
11	Are there disagreements or conflicts that traditionally arise in PSM development work? Different camps or views? Are there important views which can get swamped by powerful interests? Are there thorny questions that are best avoided?
12	Looking at our proposed plan, are the objectives and overall approach OK?
13	Are there additional techniques we can use to explore the Issues, Measurement opportunities and 'processes'?
14	Subject product systems are assumed to be *computer-based systems*. Is this correct? Not just SW?
15	What are the expected types of attendee? Safety/ security specialists as well as measurement people?

Questions and notes regarding Introduction

1	Are the Workshop objectives agreed?
2	Are the proposed plan and method of working (four break-out sessions) agreed?
3	Are there additional or better techniques we could use to explore the work of the four sessions? Which techniques do attendees wish to apply?
4	Are the planned outputs of the Workshop agreed?
5	Prepare Attendee List
6	If we find problems that cannot be resolved, or unknowns, we should record these and then move on.
7	Are there any concerns or solution approaches that attendees wish to bring forward?
8	Summarise background of any work done to date or related work (research projects that are in process).
9	

General Objectives of applying PSM to Safety/ Security

The PSM Workshop is contributing to an effort to extend the PSM framework to the safety and security disciplines and their management. The effort has the following objectives:

1	To develop measures appropriate to the safety and security disciplines, in the spirit of the performance measurement approach of PSM
2	To draw up augmentations to the PSM materials, in particular the Issue-Category-Measure, Measurement Category and Measure Description Tables, with the objective of guiding users in developing measurement systems in these disciplines
3	To provide measurement support to the CMMI and +SAFE integration work

We have to be realistic about what we can achieve in one day. It is proposed to think of the Workshop as a first iteration through the measurement development process. This may then serve as a model for a subsequent, more detailed iteration. We hope to frame the whole problem, develop an approach to it and record examples of results.

Workshop Objectives

The following objectives are proposed for the Workshop:

1	Place the PSM extension initiative on a sound platform, which specialists are comfortable with
2	Develop a 'reasonably complete' scan of typical issues and measures
3	Propose some augmentations to the PSM tables, with some detailed examples
4	Propose a plan for the work to be continued and completed, along the lines demonstrated

One way to think of this is as an application of the PSM *Tailor Measures* process to a notional aerospace/ defence project, where we expect to have to augment the PSM tables. We are ready to uncover new kinds of *Measures*, *Measurement Categories* and *Common Issue Areas*, called for by the particular specialty domain. We also expect to re-use existing PSM measures.

In terms of CMMI, we are seeking to provide guidance on the implementation of parts of the *Measurement and Analysis* (MA) process area, as applied to the safety and security disciplines. This also involves current work on two new process areas, developed originally in the +SAFE work, on extending the capability maturity model approach to the safety domain.

Background issues

1	In the spirit of technical performance management, we need measurement to improve estimation, monitoring and control of specialty areas. But how should we measure safety and security work on projects? We can measure the costs of having these specialties, but how do we measure the benefits? How can we obtain indicators of technical progress? How can we support, through measurement, improvements in the effectiveness and productivity of these specialty areas? Will measurement systems help us with the high cost of re-working assessments following change?
2	Best practice process models provide useful guidance and can help in raising awareness

	of technical and management processes; but should measurement systems be designed exclusively based on such models? Are there other things that should be managed and measured?
3	How should we develop extensions/ augmentations to PSM to cover these specialty areas? PSM was developed in the software engineering domain and is being extended to systems engineering. Is this a valid approach? What would happen if we started from somewhere else, for example, hardware engineering?
4	PSM emphasises the development of measures based on experience, and cautions against unproven theoretical approaches; but has industrial practice provided us with the measurement experience we need in these specialties?

Assumptions

1	The PSM framework *is* appropriate for the safety and security specialties and can be adapted suitably; it is feasible to bring the safety and security specialties into a framework developed originally for software, and recently adapted for systems
2	The basic principles of technical performance management are accepted, i.e. management and technical work is improved by using 'fact-based' measurement approaches
3	Measurement does not require compliance with any external model of best practice (CMMI +SAFE) or process standard; however, organisations implementing maturity model-based approaches will wish to base their measurement systems on such models. Measurement can be deployed to meet the requirements of higher maturity levels and to support maturity assessment
4	We are considering software-intensive systems, avionics, control systems, C4I etc. These are computer-based systems, including related sensor, actuator and platform systems
5	The security and safety specialties have similarities, for example they are both types of *risk management*; there are also have differences

General Questions

1	To what extent can PSM and technical performance management be applied to safety and security? Are these specialties different and, if so, how?
2	We can never be assured that all hazards/ failure modes / vulnerabilities have been found in a system. How can we measure against an end state that cannot be defined?
3	Safety is an intrinsically multi-disciplinary subject, crossing interfaces, levels, specialties and project 'time zones'; a range of specialty engineering fields is involved. To manage and measure safety, do we have to engage with all these specialties?
4	Issues (e.g. potential failure modes or hazards) are uncovered *within* the technical processes and required subsequent work can vary greatly depending on the issues uncovered (e.g. development of specific risk analysis models). PSM assumes a separate risk management process.
5	Safety and security emerge as the outcome of many activities, throughout the lifecycle. Is it feasible to integrate many measures to provide indicators of safety and security? Can this be done predictively so as to inform decision-making? Can we develop cause-effect relationships to inform decision-making from 'leading' indicators? This becomes more difficult the more a property is 'emergent' from many aspects of a system.
6	How can we judge effectiveness of safety work? Efficiency? Productivity? Does the discovery of many potential failure modes signal an effective or a poor safety process?
7	Do we develop specific measures for the specialty, re-use existing PSM measures, or

	both? The safety/security extensions to CMMI elected to develop separate practice areas. In developing measurement systems, do we have more flexibility? Can we use measures that are serving other information needs, across all project activities?
8	What are the aggregation structures appropriate for safety and security? (Probably several; FTs, Event trees, safety arguments, scenarios, product models functional and structural and timing). Fault Trees etc. rely on interpretations of system behaviour in normal and failure conditions. They have to be used in conjunction with product models. This is why FTs and Event Trees do not guarantee correct analysis; they depend also on the step from understanding the system to modelling the probabilities of events within it, and their consequences. Ultimately, risk assessment rests on familiarity and understanding of similar past systems
9	Is safety a property also of the usage environment? Is it an 'interactive' property? Risk has a subjective aspect to it, for example, risk assessment is influenced by the benefits on offer
10	Is security also a property of the environment, for example the types and strategies of potential threats
11	Safety and security are quality attributes related to future system performance. Essentially predictive. Is this different from e.g. product size measures and other quality attributes? Do safety and security attributes accumulate like product size?
12	We can only measure achieved safety/ security by detecting performance in the field. But is this possible for very low probability events? Or for hazards that depend on accessing particular combinations of system states, driven by particular environmental demands? Testing also contributes, but not possible to test for long enough to validate very low probabilities
13	Measurement of severity of hazards is similarly limited; we can only estimate the consequences of hazards. How do we develop continuously improving confidence in our understanding of consequences?
14	We can measure certain things about processes, based on required deliverables etc. But this can be at the 'container' level, without engaging with the substance of the work e.g. document contents. Measurement of container artefacts tells us something about the processes, though.

Proposed Workshop Approach

It is proposed to address the Workshop objectives as follows:

1	Identify typical issues, or areas of concern, which arise in relation to managing and conducting safety and security work on aerospace/ defence projects
2	Consider the characteristics of safety and security specialist work at the levels of methods, tools, and fundamental practice
3	Consider the aggregation of measurements to meet information needs; we propose to address these by considering aggregation structures and process integration, including the CMMI +SAFE work
4	Develop augmentations to the PSM materials

The following sections are intended to be used with the pre-read material, providing additional notes.

7. Session 1: Issues

Stakeholder Analysis

Stakeholders include:

- Certification authorities
- Safety specialists
- Program/ project managers
- Designers/ engineering specialists
- Customers
- Suppliers
- Maintainers
- Testers
- Users/ operators
- Disposers

Possible worksheet for stakeholder assessment:

Name of Issue or sub-Issue	***Definition and/or description***	***Questions asked/ information needed***
Regulatory clearance	The product has to be approved for flight airworthiness by the FAA	How confident are we that the design will achieve clearance?
Any Further Information		
Stakeholders involved. Project phase. Nature of source of issue.		

Example list of questions that might be asked of the safety/security work on a project.

1	How safe/ secure is the product, as-operated?
2	How safe/ secure will the product be as-operated, as assessed during the development process?
	How confident are we that the product will meet its safety/security requirements?
3	How much resource have we invested in safety/security so far? What has it bought us? What will it buy us in the future (c.f. Rienertsen's concept of 'Design In Progress', as an analogy of the accountants' 'Work in Progress')?
4	How much further resource do we need to invest to complete the project?
5	What are the 'control levers' on the safety/ security process? What are the cause/effect linkages between decisions now and outcomes at the end of the project?
6	How repeatable are/ should be safety/ security processes? Repeatable at what level of description?
7	What are the task scheduling issues for safety/ security work; logical ordering of work within the specialty and synchronisation with other precesses?
8	How does the customer know that the product is safe and that he has obtained value for money?

9	In safety/ security, do we measure progress against a specification? Or against customer wishes?
10	Can we actually measure safety/ security? Can we obtain leading indicators of likely-to-be-achieved safety?
11	Is safety/ security risk subjective? Does it depend on viewpoint and perceived benefits?
12	How should we design our organisations and processes to deliver efficient and effective safety/ security work? Is emphasis on efficiency damaging, bearing in mind queuing issues? How can we tell if our safety/ security processes are efficient or effective?
13	How do we know our suppliers are delivering safe products?
14	
15	

Solution Suggestion

The main stakeholders are likely to have the following concerns:

Stakeholder	Concern/ Issue	Typical Questions	Comments
Customer, User	Safety achieved Remaining risks and their acceptability	How safe is the product? What are the residual risks? Are these acceptable?	Basic safety of the product is really everyone's concern
Project Manager	Progress of safety work Risk management Productivity/ efficiency of safety work	Are we on track to meet the Safety Requirements? Are all identified risks being addressed? What is the safety plan moving forwards? Are we on track to achieve certification?	Progress against Plan Project risk Estimation and prediction Marginal costs/benefits
Safety Engineer	Quality of safety work Interfaces with development processes Coverage	How confident are we all hazards have been identified? Are safety issues and actions being dealt with in other processes? Have we covered all aspects? Is the data we've analysed correct and up-to-date?	Concerns focus on the basic safety work
Safety Capability Manager	Quality of safety work Capability development	Do we have the safety capability/ resources needed for the project? Where is investment needed? Are lessons-learned being used? Updated methods? Training? Tools?	Resources deployable on projects Lessons learned
Regulatory Authority	Certifiability of product	Can the product be certified as complying with all regulatory requirements?	

We would like to distil the range of questions and concerns identified into a small set of key issues. The following are proposed as the key issues for safety:

	Key Issue	Description
1	Safety Engineering core concern	Measurement of safety-related risks, involving likelihood and severity. Management of identified hazards. Management of unidentified hazards, through coverage. Risk management. Acceptability of residual risks.

2	Safety Program Management: progress and performance on a project	Measurement of work achieved against plan and estimated achievement etc. Measurement of the effort and other resources used in the Safety program, and estimated to completion. Project Performance
3	Safety Program Effectiveness	Measurement of the safety achieved in operations. Measurement of the value of safety program outcomes to stakeholders.
4	Safety Compliance	Measurement of progress towards regulatory compliance, certification. Compliance with process and methods advice and requirements.
5	Safety Capability	Measurement of organisational capabilities that contribute to quality and productivity of safety work CMMI compliance. People level, Method level, Safety Process level, Organisation level, Product lifecycle level.

A similar set should be drawn up for security. These headings seem to be generic: core technical work, how to manage it when applied to a project, how to measure its effectiveness in the 'customer' domain, how to manage compliance with regulations and how to manage investment and growth in the capability.

Notes on Key Issues

1	Safety engineering is distinguished from safety compliance. Safety engineering at heart involves an open, creative search for potential failure modes, hazards etc.
2	The safety / security core concern is fundamental and underpins the other issues. Measurement under this heading supports the professional practice within the specialties.
3	Safety compliance seeks to ensure certification/ flight approval through working with regulators etc, informed by safety engineering. Safety Cases (not mentioned in the above table) support compliance.
4	Establishing acceptability of risk, for example through ALARP assessments, may alternatively be assigned to the compliance concern.
5	PSM seems to be based in the project management area. Project management traditionally is concerned with the implementation of a project plan; progress is assessed against the Plan in terms of technical work, cost and schedule.
6	Safety program effectiveness is manifested in operational performance. This can, in principle, be measured. Problems arise with catastrophic events because their rarity means that we cannot accumulate data over typical system lifetimes to demonstrate their unlikelihood. However, we can measure other events, including near-misses, contributory events in hazard scenarios etc.
7	Product safety is achieved by many processes working effectively together. For example, safety concerns raised by a safety process may place requirements on the product design process. Risk reduction may depend on the design modifications made.
8	Safety capability measurement is arguably the objective of the CMMI +SAFE work. This area should be guided by their work, in the PSM application.

An observation is made here about PSM. The PSM methodology treats Issues as 'atomic' concerns received from other processes. However, in technical and project management there is a need for coherent measurement systems, which ensure sufficient coverage of all key management issues. This points up a need for organisation, process and job design,

supported by a compatible measurement system. If this is in place, then additional Issues can be handled in the PSM way.

'What's Different/ Special?' Assessment

As an independent view on safety and security measurement, the Workshop may wish to have a group consider the differences between these specialties and the core software and system development processes, or define what's special about these disciplines. How are safety and security different from software and systems processes? What are the fundamentals of safety and security? What is implied by viewing them as types of risk management? By looking at differences, we seek to draw up a list of measurement-related problems/ issues. Also potential limitations, cautionary comments, opportunities of measurements systems.

Example output:

What's Different/ Special?	Description	Measurement Implication, if any
Open-ended	We can never know if we have found all failure modes, hazards, whereas we can know if we've delivered all required functionality.	Need indicators throughout the lifecycle: 'Eternal vigilance' Feedback
Issues uncovered within managed process	PSM approach views issues as arising in a separate process.	Flexibility, adaptability
Multi-disciplinary	Safety and security are achieved by many processes delivering successfully Effectiveness of safety process not entirely in the hands of safety engineers	Measure other processes as well, inter-working
Aggregation Structures are different	'Hazard Scenario', which connects root failures, via failure effect propagation paths etc, to hazards and potential accidents. Includes protections and mitigations. FTs, Event Trees. Reliability models.	Indicators of safety and security rely on integrating many disparate measures?
Safety and security properties 'emerge'	Success depends on getting a lot of things right throughout the lifecycle and especially in operation and maintenance	May have to measure other processes.
Risk management is iterative	Often involves development of a risk model or models, in which failure probabilities etc can be understood. Often linked to particular events of concern or hazards. Can cut across other kinds of aggregation structure	Support 'growth' of understanding, modelling, learning
Dependent on other models	Models used in safety assessment (FTs, Event Trees, Markov models) do not 'stand alone', but must be interpreted with system models etc for full understanding.	Progress in safety work is dependent on progress in other processes, especially the design process.
External environment dependency	Safety and security dependent on external environment/ stress etc. Openness to this	Risks are assessed under assumed operational conditions.
Acceptability of risk is partly subjective	Perception of risk is viewpoint-dependent. So need to consider these	Risk acceptability criteria set by standards.

	(stakeholders) and the way risk analysis results are presented to different communities of interest.	May need to support ALARP assessment.
Regulated by Government agencies	Safety engineers are required to demonstrate flight airworthiness etc. to 'external' teams	Measure progress towards certification

1	Application of PSM to safety and security will focus on project management issues. We do not have to get involved in the details of the specialties. However, we need to understand their characteristics, in order to identify key measures of performance.
2	Although safety and security are challenging areas to 'measure', it does not follow that we should not strive to apply PSM principles to them.
3	The characteristics of the safety/ security specialty are shared by other specialties.
4	

8. Session 2: Methods

Method Assessment

This session will consider the typical methods and properties of the specialties and identify candidate measures, that may be useful for the PSM framework. A later session will review, combine and select from those identified. This is rather a 'brainstorming' approach; the objective is to generate a variety of measures etc. Participants may wish to consider relevant measures of related processes.

Worksheet:

Name of Measure	***Definition and/or description***	***Questions answered***
Potential failure modes	Count of number of potential failure modes identified during FMEA	How confident are we about the design meeting safety requirements?
Any Further Information		
Applied during preliminary and detailed design phases		

Example output:

Method	Measures
Hazard Analysis	Number of hazards identified
	Severity of hazards (catastrophic, major, minor)
	Exposure time
HAZOP	Number of outstanding actions or investigations
	Number of links/ interactions assessed
FMEA	Number of failure modes at different aggregation levels of the system design
	Risk Priority Number
	Number of outstanding actions or investigations
FTA	Number of top-level events
	Probabilities of top-level events
	Number of cut sets per top level events
	Number of base events in cut sets
Markov Analysis	Number of hazardous end states
	Number of state transition sequences leading to hazards
	Number risks identified and being assessed
Particular Risk Assessment	
Zonal Analysis	Number of zones assessed
Vulnerability Assessment	
Damage Assessment	

Specialty Assessment and Organisational Context

A second Workshop task is proposed to assess attributes of the areas of professional practice *not* covered by the Method Assessment. Practical measures useful to project management are sought that might contribute to indicators of progress, quality, confidence etc.

Organisational, staff and cultural measures may be raised in this task. Some of these may be assigned to the capability issue.

Questions and comments about method assessment:

1	This session is intended to explore the knids of things which are countable or measurable in the safety and security domains.
2	The PSM application will involve, in the next session, selecting or aggregating a few key measures of technical performance/ progress.
3	We distinguish between the measures involved within a technical specialty and measures involved in the management of the specialty work. It seems that PSM is concerned mainly with selecting a few key measures of technical work that support management.
4	This approach seems to be about making the '% complete' assessment of work package owners more transparent/ objective/ open to scrutiny.
5	There is also an overlap with the approach used in traditional systems engineering, namely the identification of 'Technical Performance Measures' (TPMs) to support the achievement of 'Measures of Effectiveness' (MoEs). See, for example, EIA-632.
6	

9. Session 3: Processes

This session addresses the selection and aggregation of the measures identified in Session 2 to provide the information needs identified in Session 1.

The principle proposed here is that each of the five key issues identified above will have its own set of base measures and aggregation structures. There will be overlaps.

It is proposed to address three issues in the Workshop:

Key Issue 1	Technical performance measures derived from the specialty core concerns
Key Issue 2	Process measures for project management
Key Issue 5	Measures to support capability development

Technical Performance Measures

The first key issue, namely the fundamental technical concerns of the specialties, underlies the other issues.

This task considers the aggregation of measures from a technical/ engineering viewpoint. The basic proposal being made here is that safety and security specialties are types of risk management. The identification and management of safety and security risks are the fundamental outputs of the work. So measurement should be directed at these hazards/ vulnerabilities.

An assessment of coverage depends on 'scoping' the safety critical parts of the system. This amounts to an estimate of 'product size' (in terms of PSM categories) for the safety/ security specialties. Assessments of safety critical product size are an output of safety assessment work.

The PSM material (Part 2) provides three examples of Aggregation Structure: Component Structure, Functional Structure and Activity Structure. What structures are appropriate for safety/ security? Possibilities include:

1	Fault Trees
2	Event Trees
3	'Hazard scenarios', which connect root failures, via failure effect propagation paths etc, to hazards
4	Reliability models
5	Safety Argument Structures

The proposed solution is to adopt 'hazard scenarios' as the aggregation structure for safety work. This is not well-established practice however and may be rejected by the Workshop.

Process Measures

This task will identify aggregated measures suitable for managing safety/ security work as integrated into projects.

The following issues arise in considering the aggregation of safety/ security work:

1	Allocation of safety responsibility; representation of the safety/ security specialty on teams
2	Supply chain management, organisational interfaces
3	Method/ Process integration aspects of the coverage of assessment; who's doing what, are information flows in place, do responsibility/ accountability arrangements provide coverage?
4	Consider coverage in terms of managing work to cover product functionality, architecture, components, dynamics, operational environment
5	Integration of the various safety/ security techniques deployed
6	Integration of safety/ security processes with other project processes (especially the core design, development, test and maintenance processes)
7	Integration of safety/ security assessment and certification/ regulatory compliance processes.

Capability Measures

This task will also examine the CMMI + SAFE models of the Practice Areas involved in the safety/ security specialty. How can we develop measures of performance in these Process Areas, associated with the generic and specific goals and practices? What information needs and measures arise from implementations based on the CMMI models?

CMMI-related questions include:

1	In the CMMI models, a Practice Area is associated with just one goal. Is this compatible with, for example, an engineering design practice serving both functional and safety goals?
2	What is a *repeatable* process? Any process is repeatable at a high level of abstraction. But a design or safety process can look very different at detailed levels, depending on the problems being addressed. Maybe this is a difference between software and safety – software processes are always roughly the same – you don't need different skill sets for each project, perhaps. But systems and safety assessments can vary a good deal depending on the problem.
3	We distinguish between the audit of a process against a standard or best practice model, which is a form of measurement, and the measurement systems called for to support process improvement, which are part of the subject of an audit.
4	

Worksheeet for Session 3

Indicator or Information Need served	***New Measure or Aggregation of base measures***	***Aggregation Structure or principle; analysis required***
Estimated 'top event' probability	Failure mode rates	Fault Tree, System Model
Severity Assessment	Severity level (Catastrophic, Major, Minor)	Damage Assessment
Risk management	RPN	RPN = Prob x Severity

		Level

Any Further Information
Applied during preliminary and detailed design phases. Measurement Category identification.

10. Session 4: Augmenting PSM Materials

This session will develop augmentations of the PSM materials on the basis of the work done in the previous sessions.

The following augmentations were proposed as a strawman modification for the safety and security specialties.

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

The Workshop should also draft a Measure Description table for selected measures.

These are ‘strawman’ solutions and offered to support discussion. The rationale for the safety measures proposed is as follows.

1	Existing PSM measures cover the regular cost/ schedule aspects
2	Work Unit Progress applied to safety work involves safety subsets of the requirements and action items
3	Product size and stability are interpreted as measures of the those parts of the product system that are assessed as safety critical, at different risk levels. For example, a count could be maintained of those components, functions, items etc that are involved in Hazard Scenarios.
4	All parts of the product system would have to be assessed at some level, in order to distinguish the safety critical parts.
5	Operational scenarios/ modes and environment characteristics would be included in measurements of hazard risk.
6	The basic safety hazard risk is measured as a count of hazards (at different risk levels), a count of the hazard scenarios associated with each hazard, a count of functional and/or parts failure modes and nominal conditions relevant to each scenario. Also a count of Common Causes that may defeat other redundancy-based assessments.
7	A measure of coverage might be a count of those functions and systems/components/items/modes that have been subject to safety assessment. Also a count of single point failures that lead to hazards at defined risk levels.
8	Depending on the technology and application etc, a count of Particular Risks that have been assessed.
9	Process conformance is interpreted as compliance with regulatory or industry standard process models etc.
10	Certification is also interpreted in terms of compliance. The gathering and structuring of certification data is measured in terms of completeness against standards.
11	The effectiveness of the safety process is interpreted here in terms of counts of operational events which are safety-related.
12	Technolgy effectiveness is interpreted in terms of safety experience with the technology in similar applications.
13	An additional issue *Regulator Satisfaction* has been added.