Measuring Safety: Applying PSM to the System Safety Domain

John Murdoch, Graham Clark, Antony Powell
Department of Management Studies
University of York
York YO10 5DD UK
jm48@york.ac.uk

Paul Caseley
DSTL Malvern
St Andrews Road
Malvern Worcestershire WR14 3PS UK
PRCASELEY@dstl.gov.uk

Abstract

Preliminary work on the development of measures appropriate for the safety domain is reported. Measures are expressed in the style of the Practical Software and Systems Measurement (PSM) approach, a programme sponsored by the US DoD. Proposed measures are integrated with the PSM measurement framework. Reported work has been informed by discussions within the PSM community and by concurrent work on the safety extensions to CMMI[SM], derived from the +SAFE safety extensions project, sponsored by the Australian Department of Defence. The paper discusses the background to the work, locates it within a measurement framework for the safety domain and proposes a set of measures, with justifications. The paper closes with an assessment of progress in safety measurement and identifies areas needing further work.

Keywords: safety measurement

1 Introduction

The effectiveness, productivity and assurance aspects of safety work continue to be of concern in complex system applications. System acquirers are now responding to these concerns in several ways, including:

1. Developing the means to assess the capability of suppliers against reference models of good safety practice;
2. Fostering improved collaboration between acquirers and suppliers, through both 'systems' and 'people' aspects;
3. Increasing demands for safety assurance, for example requiring greater volumes of safety evidence.

System developers are naturally concerned about the high initial and change-related costs of developing safety-critical systems. This paper considers the deployment of measurement systems that support the management and coordination of safety processes, as implemented on projects. More specifically, the paper discusses the application of the Practical Software and Systems Measurement (PSM) framework of the US DoD (McGarry, Card et al. 2001) to the safety domain.

The PSM measurement framework is reviewed in Section 2, followed in Section 3 with some observations on the characteristics of safety processes. A rationale for considering PSM for safety program management is sketched in Section 4. Section 5 provides a short description of the proposed method for developing safety measures within the PSM framework. Sections 6 and 7 provide initial proposals for safety measures, using 'top-down' and 'bottom-up' approaches respectively. Section 8 proposes a set of augmentations to the PSM framework, with an example measurement specification. Section 9 summarises the status of the work and discusses future development.

The proposals made in this paper are initial and tentative and not formally part of PSM (transitioning to formal PSM materials is discussed in Section 9).

2 Practical Software and Systems Measurement

The PSM program originated at project management level, having been developed to give acquirers and project managers greater visibility of software development activity. PSM has recently been extended to include systems development. It has been influential on several current ISO standards in the software and systems domains (ISO/IEC 15939, 12207 15288, 9126 and 14598). Recently, via ISO/IEC 15939, PSM has informed the measurement component of the CMMI (CMMI Team 2002) models.

PSM has its roots in the *Goal Question Metric* approach of Basili and co-workers (Basili and Weiss 1984). It is based on a general process that encourages:

1. the identification of *information needs*;

2. the interpretation of an information need as being within an *information category*;
3. the identification of *measurable concepts* within each information category;
4. the identification of *prospective measures*, associated with each measurable concept.

A prospective measure is used as a guide to implement an *actual* measure in terms of one or more attributes of actual work products or other entities existing, or introduced, within a project. For example, the prospective measure *lines of code* might be implemented as a specific output of a particular source code analyser, or as a particular field in a project database. Figure 1 illustrates the basic measurement information model that underlies PSM; an information need is met by an indicator, derived from a set of base measures. Figure 2 illustrates the implied mapping from prospective base measures to actual project entities and their attributes.

PSM recommends a general measurement process comprising two 'core' activities, *plan* and *perform* measurement, and two 'supporting' activities; *evaluate measurement*, and *establish and sustain commitment*.

The measurement information model and measurement process have been incorporated in the ISO/IEC Standard for a software measurement process (ISO/IEC 2002). These general models and associated terminology are therefore now established (for the software domain) as an international standard.

PSM goes further than ISO/IEC/15939 by providing a Table (the 'ICM Table') that associates information categories with measurable concepts and prospective measures. Further guidance still is provided by means of Measurement Specification Tables that comprise reference specifications for measurement constructs, measurement attributes, data collection procedures and data analysis procedures. These PSM materials effectively form elements of a measurement experience base (ISO/IEC 2002), and would be specialised to different application domains.

This paper discusses initial work on developing augmentations to the PSM guidance materials to cover safety processes. Before considering some detailed proposals, general characteristics of safety processes are reviewed followed by a rationale for considering PSM for safety.

3 Some Characteristics of Safety Processes

Taking the perspective of a system developer organisation, four broad constituencies of 'measurement users' can be identified, with areas of concern centred on different aspects of system development (Table 1). Similar roles exist in acquirer and supplier organisations.

The enterprise level is mainly concerned with the business case, or the financial justifications for investments and engagement in projects. It is important for measurements at the other levels to map to the enterprise level, since this is where strategy is developed and overall organisational performance monitored. The resources consumed by a safety program have to be justified at this level; senior managers will be interested in the effectiveness and

Constituency	Typical Concerns
Enterprise Management	Productivity, cost, strategy, litigation, commercial viability and growth.
Capability Management	Effectiveness, process improvement, integration of standardised activity, institutionalisation, learning, people
Project Management	Delivery to plan, schedule, cost, meeting requirements, product performance, monitoring
Technical/ Specialty	Professional practice (e.g. safety engineering), learning, 'actual' project work.

Table 1: Various constituencies with different, but related, needs for measurement

productivity of safety work in terms of both performance of the product throughout its operational life and in terms of achieving regulatory clearance.

The capability maturity models have their roots in the quality movement in manufacturing and they drive process stability and continuous improvement. These

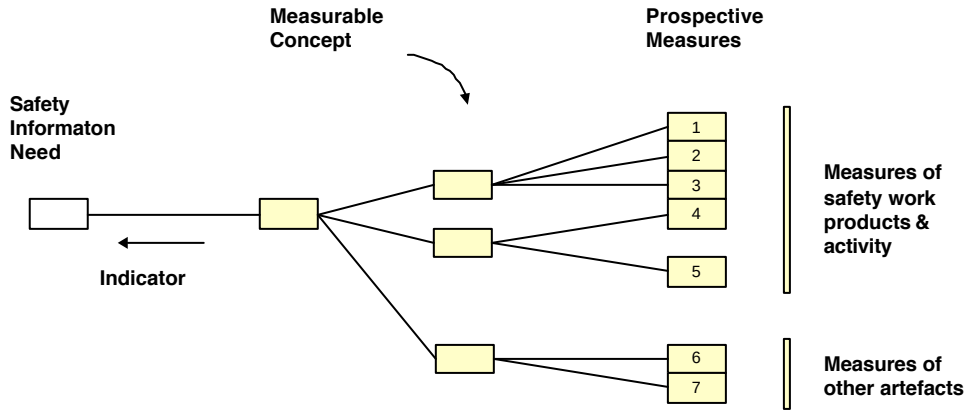

Figure 1: Measurement construct in PSM

models call for processes eventually to be institutionalised as *quantitatively managed*, an expectation now carried over to safety extensions (Bofinger 2001). Work is currently in hand to integrate a safety application area into the CMMI model, using the +SAFE (Bofinger, Robinson et al. 2002) work as input.

Industrial sectors that develop safety-critical systems develop and promote standard models of safety processes. These provide descriptions of required or advised activities, work products and certification evidence.

Project management has traditionally used measurement for monitoring progress and for planning & control purposes. The monitoring of costs and schedule are typical concerns. Monitoring technical progress of work is more problematic; recent developments such as PSM, can be viewed as striving to provide greater visibility of technical progress to managers.

Technical work has always involved measurement as an intrinsic part of the activity; products are developed with properties that can be demonstrated to meet numeric and other requirements. Each discipline specialty has a measurement 'world' that enables design, analysis and test of the properties of concern. These tend to be organised at a speciality level and are used to perform the engineering work, rather than for informing management or acquirers.

Safety engineering is a form of risk management; the likelihood and severity of possible accident scenarios are assessed and, in collaboration with other specialties, actions are taken to reduce risks to acceptable levels. Probabilistic risk assessment and other statistical techniques and models are used. A significant effort is associated with the identification of hazards, failure modes and failure effect propagation paths, through assessment of design and test data.

Probabilistic risk assessments are subject to the 'zero-infinity problem'; risk numbers become meaningless for very rare events with catastrophic consequences and it is here that engineering judgment is required. Safety considerations usually result in conservatism in development. Risk management involves predicting the future; we are not so interested in the accuracy of prediction, but more in thresholds. This is sometimes expressed as a need for 'dependable' measurements rather than accurate ones.

System safety, in the sense of MIL-STD-882 (DoD 1999), is a multi-disciplinary field. Mixed hardware, software and people aspects are involved. Many different techniques and methods exist, developed in different industries. Software safety is a specialised domain, with an emphasis on meeting requirements. Probabilistic techniques are less appropriate for software; greater emphasis is placed on formal modelling. Software safety assessment is conducted in the context of a system safety process, to define safety-related software requirements and to investigate failure effects.

Safety assessment is a 'design-like' process, rather than a 'manufacturing-like' one, to use the terminology of (Reinertsen 1997); work tends to fill the time available. This is often justifiable because safety deals with open-ended, open world problems. Care is required in assessing the productivity of safety activities. A naïve count of identified hazards is not an indicator of effectiveness of a hazard assessment activity.

In many industries, long lifecycle times dictate that feedback on the outcomes of safety processes is slow. Given that accidents are undesirable events and we are reasonably successful in avoiding them, opportunities for

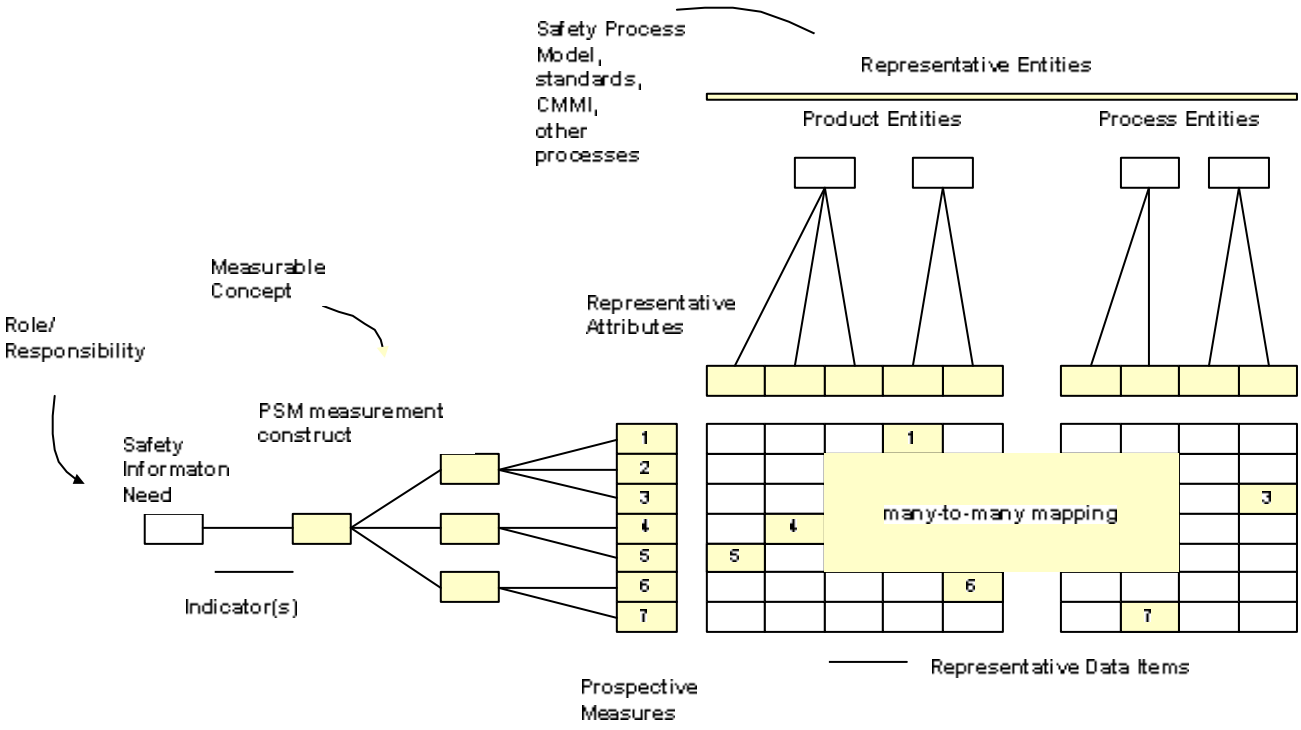

Figure 2: Mapping prospective measures onto representative entities and their attributes

'refutation' of safety claims are rare. This increases emphasis on system development (pre-operational) phase measures

The safety process supports other processes, mainly the 'core' product development processes, receiving work products from them and returning assessments, requirements and advice. Tracking progress in safety-related work may involve measurements deployed in non-safety processes, e.g. progress in design work that is part of the mitigation of a safety risk. The effectiveness of safety work is dependent on other processes and interactions.

Safety processes are required to achieve regulatory certification, a form of assurance. There are variations between national governmental requirements, for example whether a safety case is required or not to aggregate certification evidence. Practices in safety engineering are varied in terms of the methods, work products and standards used, but there are common fundamentals and it is these that generic measurement guidance must build on.

distant in the future. The characteristics of safety work sketched in the preceding section present management challenges.

Both the managers of safety work and the safety specialists themselves have just concerns and responsibilities to discharge. Providing managers with greater visibility of the effectiveness of safety work and the means to monitor it seems reasonable. With recognised beneficial outcomes, for example, in terms of design improvements resulting from actions arising in the safety process, experience will be developed to justify investment in safety. Mutual visibility of other properties, e.g. timing of assessment tasks, quality of input data to them and current status of safety work, would also support more enlightened and flexible management practice. Safety tasks that do not provide benefit, perhaps enacted for historical reasons, would also be easier to identify and discuss.

PSM (and its embodiment in ISO/IEC 15939) is an existing measurement framework developed from the technical management perspective. It fosters a rational

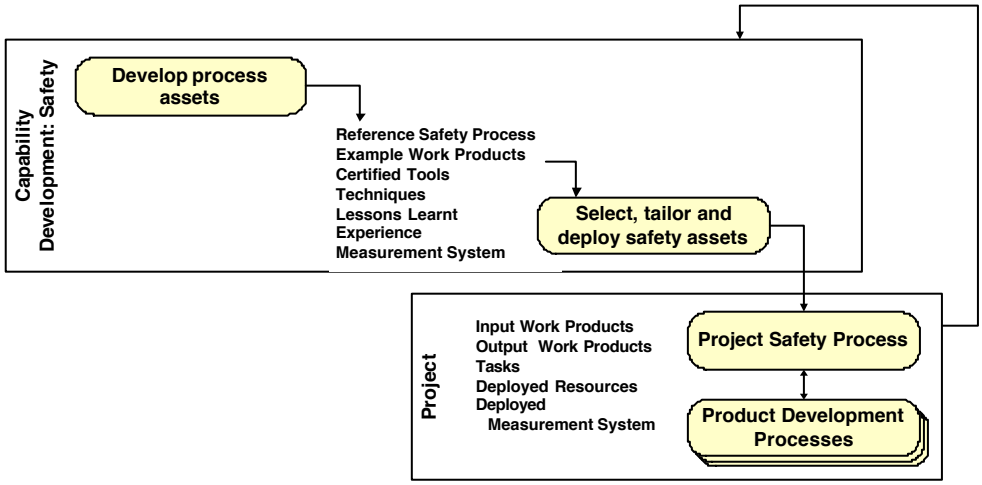

Figure 3: Measurable entities in a safety process as applied on a project

4 Rationale for Considering PSM

Inevitable tensions exist between the constituencies of Table 1. Business managers are driven to reduce costs to improve business performance; technical specialists have professional responsibilities to observe in the conduct of their work, responsibilities that may incur costs. Project managers focus exclusively on resource allocation and progress towards particular deliverables. However assessment of technical progress often depends on the judgment of specialist staff, raising issues of trust and visibility. Managers of capability have medium term concerns that may conflict with the immediate priorities of projects and some senior management.

Such tensions are present for the safety specialty. It is recognised that safety-critical systems are costly to develop, but justifying cost levels can be difficult, especially when the outcomes are 'null', i.e. the absence of accidents, and relate to system performance at times

development of information needs and measure selection and design. The ISO standard provides a common terminology and a simple guide for developing measures. PSM offers a platform for managers and specialist staff to support negotiations and the building of shared measurement experience in the particular domain. Deployed wisely, such an approach could serve the needs of both managers and specialty staff, providing a means to assess performance and make visible the value achieved by specialty work.

5 Method for Developing Safety Measures

If safety additions were available in PSM, a user would follow the recommended measurement process; identify information needs, select prospective measures and then map these to the measurable artefacts available within the organisational processes. In practice, a user has to balance the top-down view (information needs driving prospective measure selection) with the bottom-up view (consider what is available to measure on the project as-is

or possibly as-modified). Figure 3 illustrates a safety process as enacted on a project, indicating the measurable entities as the tasks undertaken, the input and output work products and the resources deployed. A feasible and useful measurement system would normally derive from a compromise between the information need developed top-down, and the identification of measurable entities developed bottom-up. Existing data and measurement systems would be used as much as possible.

In developing PSM guidance material for the first time in the safety domain, we can adopt a similar procedure:

Top-down:

1. identify roles involved in safety work and its management;
2. consider their information needs, and its categorisation;
3. identify measurable concepts that are candidates for meeting the information needs;
4. identify relevant prospective measures;
5. propose augmentations to the PSM ICM Table and modifications to existing Measurement Specification Tables where appropriate. Also outline Measurement Specification Tables for new measures proposed for safety measurement.

Bottom-up:

1. identify typical activities, work products and their measurable attributes, based on industry practice, standards and +SAFE/ CMMI safety extensions;
2. develop a set of *representative* work products and attributes;
3. identify representative data collection and analysis procedures;
4. complete sample data collection and analysis sections of the newly proposed Measurement Specification Tables.

Proposals would then be published for consideration and improvement by the safety community. This effort would then launch a platform for a shared experience base for safety measurement.

6 Safety Measures: Top-Down

6.1 Information Needs and Categories

Organisational roles that carry safety responsibilities include *general business managers*, *the safety process owner* (developer of safety capability), *project safety engineer*, responsible for safety of a particular product or system, *safety engineer*, *safety assurance staff*, *regulatory certification organisation*, *system acquirer*, *safety staff working for subcontractors*, *system operators* and *maintenance staff* and so on. Typical information needs can be expressed as a series of questions, for example (proposed ICM information categories are indicated in brackets);

1. Have we identified and tracked all safety requirements? (Schedule and Progress)
2. How confident are we that we can meet the required and/or acceptable safety performance? (Product Quality)
3. How confident are we that we can meet the required and/or acceptable risk level for *this* particular accident scenario? (Product Quality)
4. What is the current progress/ degree of achievement of product safety as compared with the requirements? (Product Quality)
5. What is the current progress/ degree of completion of safety work as compared with the current Plan? (Schedule and Progress)
6. What is the technical scope of the safety work? How is this evolving as the project is enacted? (Product Size and Stability?)
7. What is the impact of *this* proposed change for safety work?
8. What is the remaining work to be done to meet safety requirements? (Resources and Cost)
9. What is the current status/ degree of completion of safety assurance work? (Schedule and Progress)
10. What is the level of compliance of safety work with applicable standards and regulations? (Process Performance)
11. What are the cost, productivity and effectiveness of the safety program? (Process Performance)
12. What is the process maturity of the safety process in our organisation? What is the capability maturity level of the organisation (in CMMI/ +SAFE terms)?

6.2 Measurable Concepts

Many existing measurable concepts in the PSM ICM Table are applicable to safety work, for example *Milestone Completion*, *Work Unit Progress* and *Personnel Effort*. Prospective measures associated with these concepts would need slight modifications to their specification tables to indicate that they embrace safety work. For example, the *Requirements Traced* measure could include a note to the effect that requirements sourced from the safety process are included. Similar adjustments could be made to *Problem Reports Opened*, *Reviews Completed*, *Test Cases Attempted*, *Action Items Opened*, *Staff Experience Level* and others.

Three new 'measurable concepts' (i.e. additions to the PSM ICM Table) are tentatively proposed:

1. *Dependability – Safety*, analogous to the existing PSM concept *Dependability –Reliability*;
2. *Assurance – Safety*, to cover certification activity;

3. *Scope – Safety*, to cover estimation and technical scope aspects of safety assessment work.

6.3 Prospective Measures

The following prospective measures are proposed for consideration:

A *hazard count*: there are two aspects - for each identified hazard, how confident are we that we can meet the required risk level, or achieve an acceptable level of risk? And secondly, how confident are we that we have identified all hazards?

The safety risk of a hazard is formally the product of the probability of the accident occurring and the severity of its consequences. Both assessments are dependent on assumptions about the system operational environment and timescales. Probabilistic risk assessment has its critics; it should not be used without supporting engineering judgement.

consideration of modes, mission phases and external vulnerabilities.

An *assumption count,* where assumptions are made in the conduct of safety work; this concept would enable concurrent safety work, but with flagged action items, effectively to check that assumptions made are correct.

A *hazard scenario count:* proposed as a means of aggregating sets of failure modes, operational modes and other factors involved in a hazard. There are two views of a hazard; the *external* view which assesses the external risk, and the *internal* view, which determines the 'causal reach', that is the components, functions internal to the system that are involved in the hazard resulting in an accident. This is equivalent to the concept of a cut set in Fault Tree Analysis.

A *failure scenario count*: proposed as a means of aggregating sets of conditions and other factors involved in the propagation of failure mode effects with the system; similar to an Event Tree or Probability Tree, showing the events in an accident sequence.

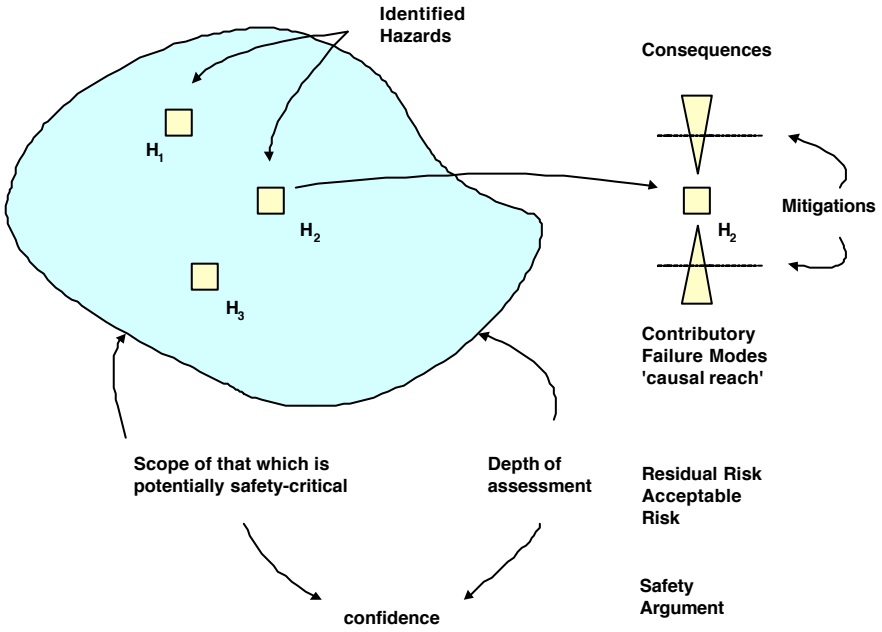

Figure 4: Concepts of *safety scope* and *causal reach* of a hazard

A *failure mode count*: of each identified failure mode, how confident are we that the associated safety risk is acceptable? How confident are we that we have identified all failure modes that carry safety risks? Single point failures and common mode failures are of particular concern.

Safety scope: count of those parts of the system assessed as potentially safety-critical. The concept of *scope* of a safety-related product and process would enable the estimation and measurement of coverage of safety work. It is suggested this can be modelled on *Product Physical and Functional Size*, but only counting safety-related parts of the system. Safety scope might include

A *mitigation count*: a mitigation is a proposed action, analysis, or requirement that renders the hazard risk acceptable, or is likely to do so. The ALARP (SAE 1995) principle is sometimes evoked to assess the acceptability of risk levels.

Safety argument status: measurement of current state of safety argument and evidence as compared with a planned argument and required certification data.

An *accident*, *incident count*: safety as achieved in operations is also important, although feedback often arrives too late to inform the current project.

Other measures of safety processes are similar to existing PSM prospective measures, e.g. verification against

safety requirements; the degree of completion of planned safety tasks; the *safety actions* arising from the safety process; effort costs as measured by a conventional time booking system and so on.

Figure 4 illustrates some of the concepts discussed above; the scope of safety assessment, the identified hazards, their causal reach and mitigations, and the breadth and depth of safety assessment undertaken to achieve confidence that all 'important' hazards have been found.

Organisations will choose to have different levels of 'sophistication' in their safety processes, presenting different opportunities for measurement. Furthermore, an organisation may choose to implement a simple-as-possible measurement system, determined by its chosen management approach. One way of responding to these variations is to consider the measurement sets typical of different levels of safety process maturity. For example:

Level 1-2 Organisation: basic safety measures, for example:

Start up measures: Safety Plan (draft, review and issue), Appointment of staff, Allocation of budgets, Are the tools for safety appropriate, e.g. certified

Basic recording measures: Safety Requirements, Detailing mishaps and hazards, Hazard log/ repository

Level 3 Organisation: measures that indicate progress of work in a managed safety process, for example:

Monitoring the maturation of hazards, the maturation of safety models/ safety case, safety requirements growth, estimating and monitoring proportion of the project that is safety related, measuring safety processes to determine if they are behaving as predicted

Level 4-5 Organisation; use of measurement to support continuous, measurable improvement of safety processes.

7 Safety Measures: Bottom-Up

Safety techniques, terminology and work products vary across industrial sectors and types of technology, although fundamental principles are common. In developing PSM guidance material, it is proposed to express typical practical measures in terms of representative work products, attributes and tasks. These are to be derived from:

1. Applicable standard safety process models (e.g. MIL-STD-882);
2. Reference process models developed within a sector (e.g. the 'Weaver Team' software safety process model developed in the naval community (Weaver Team 2003));
3. The safety extensions under development for the CMMI models, and the inputs to them (the +SAFE extensions).

A list of representative work products (and published examples of their use in measurement) include:

1. A *Safety Plan*: Safety Process Definition, Tasks, Schedule, Resources, Work Products, Roles, responsibilities, Staff Competencies; Skills and Experience Matrix Reporting Arrangements, Contractual Agreements, Dispute Resolution Provision. The measurement of deployed effort in a safety-critical software application has been reported by (Clark, Caseley et al. 2003);
2. A *Safety Requirements Log* or database: Requirement Count, Requirement Scope, Requirement Source, Status; an example of measurement using software safety requirements has been reported by (Kuettner and Emery 2003);
3. A *Safety Scope Log*: Product Components, Product Functions, Product Modes, Mission Phases, Process Resources; this is a speculative proposal of this paper;
4. A *Hazard Log* or *Tracking System*: Hazard Count, Hazard Status, Hazard Scope, Hazard Risk. The practical application of such a measure has been reported by (Watt 2003), applied to the assessment of safety program effectiveness;
5. A *Failure Mode Log* or *Tracking System*: Failure Mode Count, Failure Mode Status, Failure Mode Scope, Common Mode status; this is equivalent to a hazard tracking system but at the level of subsystem and component failure modes. The Potential FMEA process developed in the automotive industry (SAE 1995) provides an example process;
6. A *Safety Assumption Log*: Assumption Count, Assumption Status, Assumption Scope;
7. A *Safety Action Log*: Action Count, Action Status;
8. *Verification and Acceptance Test Logs*: Verification Count, Verification Status, Action Status, Action Scope;
9. *Accident & Incident Logs*: Count, Type/ severity, Action Status, Accident Scope;
10. A *Maintenance Action Log*: Count, Type, Action Status, Maintenance Scope;
11. A *Safety Case*, % completion against planned argument structure, certification data requirements.

As a measurement framework, PSM expresses no expectations about what an organisation *should* implement in terms of these work products and measurable attributes; rather, the prospective measures developed on the basis of information needs would guide measure selection. For example, a Level 1 company, in the sense of the previous section, might choose to have only a register of safety requirements and a hazard tracking system. Conformance with regulatory requirements and/or best practice models would normally determine work products.

8 Example Augmentations to PSM Materials

Previous sections have discussed the measurement of safety processes in forms compatible with the PSM approach. A further consideration is how best to integrate safety measurement guidance into the PSM framework and materials. For example, the question arises: is it better to encompass safety requirements within the existing requirements measures, or to separately distinguish safety requirements as a prospective measure?

Such questions are currently under consideration. The following is a tentative augmentation to the PSM ICM Table:

Schedule and Progress: The measurable concepts are unchanged. The prospective measures are unchanged except that specifications are adjusted slightly so as to include references to safety requirements, safety-sourced action items etc.

Resources and Cost: Similarly, the measurable concepts and prospective measures are unchanged, except that specifications are adjusted slightly so as to include references to safety experience etc.

Product Size and Stability: It is proposed to insert the measurable concept *Scope – Safety* within this information category, with the following prospective measures:

Scope - Safety

Safety Requirements

Safety-Critical Functions

Safety-Critical Components

Safety-Critical Interfaces

Safety-Critical Modes

Safety Zones

Safety Change Workload

A re-naming of the information category to *Product Size, Stability and Scope* should be considered.

Product Quality: It is proposed to introduce the measurable concept of *Dependability - Safety* under this category, with the following prospective measures:

Dependability - Safety

Hazard Count

Hazard Scenarios

Failure Modes

Safety Assessments & Assumptions

Mitigations

Safety Incidents & Accidents

It is proposed to also introduce the measurable concept *Assurance – Safety* under the information category *Product Quality*, with the prospective measure *Safety Argument*.

The remaining information categories (*Process Performance*, *Technology Effectiveness* and *Customer Satisfaction*) may also require modification so as to embrace safety process performance, but are not discussed further in this paper.

Measurement Specification Tables are under development for the proposed measures; initial drafts will be revised following consultation and trials. For example, the prospective measure *Hazard Count* might have the following text in selected fields of the Measurement Specification Table:

Title: Hazard Count

Description: The *Hazard Count* measure is based on the number, severity, and status of identified system hazards. A *hazard* is a system state that presents actual or potential harm to humans or the environment. A hazard will be associated with one or more potential *accident scenarios*, implying that additional conditions may need to occur for a hazard to result in an actual accident. A potential accident may be assigned a risk, usually expressed as the product of the likelihood of the accident and the severity of its consequences. Hazards are usually categorized into severity levels determined by the risks of the associated accident scenarios. Regulatory authorities in an industrial sector usually define categories of hazard severity levels in terms of general risk levels and required or recommended degrees of safety assurance (e.g. safety assessment tasks, provided certification evidence).

Information Need: The *Hazard Count* measure is used to provide visibility of progress in the mitigation of identified hazards and of the effectiveness of related aspects of the safety process.

Information Category: Product Quality

Measurable Concept: Dependability - Safety

Relevant Entities: Hazard Log, Hazard Tracking System

Attributes: Number of hazards recorded (Rows in a Hazard Log, Records in a Hazard Tracking System database); data recorded in the columns/ fields of each row/ record.

Base Measures: number of tracked hazards; assessed residual risk (mitigation) and status of each hazard

Measurement Methods: count 'rows' in the hazard log; read the status and severity fields in each row; count the number of Hazard Records in a Hazard Tracking System; count records with particular status values.

9 Summary and Future Development

The paper discusses preliminary work in developing augmentations to the PSM measurement framework, applicable to the safety domain. Three measurable concepts are proposed and several candidate prospective measures have been identified. A top-down approach, driven by the information needs of technical managers, is complemented with a bottom-up approach that identifies the measurable artefacts that are typically available in safety processes.

Measurement proposals discussed in this paper are initial suggestions, and have the status of work-in-progress of the PSM Technical Working Group on safety and security. A PSM White Paper will be published towards the end of 2003 for wider consultation with the safety and security communities. Subsequent work will address the security domain in a compatible manner. Project trials are planned for 2004. All those with comments, potential trial projects or with an interest in being involved with the work are welcome to get in touch with the authors.

10 Acknowledgements

Work in the UK has been supported by the Defence and Aerospace Research Partnership in High Integrity Real Time Systems, with industrial sponsors BAE SYSTEMS, Rolls-Royce plc and DSTL/ QinetiQ. Thanks are expressed to Cheryl Jones and the other members of the PSM Office, and to the members of the PSM Technical Working Group on Safety and Security. Thanks also to the reviewers of the first draft of this paper.

11 References

Basili, V. and D. Weiss (1984): A methodology for collecting valid software engineering data. *IEEE Transactions on Software Engineering* October.

Bofinger, M. (2001): +SAFE - A Safety Extension to CMMI. Australian DoD.

Bofinger, M., N. Robinson, et al. (2002): Experience with Extending CMMI for Safety Related Applications. *Proc. 12th International Symposium of the International Council on Systems Engineering (INCOSE'02)*, Las Vegas, Nevada.

Clark, G., P. Caseley, et al. (2003): Measurement of System Safety Processes. *Proc. 13th International Symposium of the International Council on Systems Engineering (INCOSE'03)*, Washington.

CMMI Team (2002): *Capability Maturity Model Integration (CMMI) v 1.1*. Pittsburgh, Software Engineering Institute, CMU.

DoD (1999): MIL-STD-882D. US DoD.

ISO/IEC (2002): ISO/IEC 15939 Software engineering - Software measurement process. Geneva, ISO/IEC.

Kuettner, H. D. and M. A. Emery (2003): Practical Application of Software Safety Metrics, *Proc. 21st International System Safety Conference*, Ottawa, System Safety Society.

McGarry, J., D. Card, et al. (2001): *Practical Software Measurement; objective information for decision makers*. Boston, Addison-Wesley.

Reinertsen, D. G. (1997): *Managing the Design Factory: A Product Developer's Toolkit*. New York, The Free Press.

SAE (1995): *Potential FMEA Reference Manual*. Society of Automotive Engineers.

Watt, G. T. (2003): Metrics for Assessing Safety Program Effectiveness in Hazard Identification and Resolution. *Proc. 21st International System Safety Conference*, Ottawa, System Safety Society.

Weaver Team (2003): *Software Safety Certification*. Weaver Group Integration, US Navy.