Safety Measurement

White Paper

v 3.0 23rd January 2006

Prepared on behalf of the PSM Safety & Security TWG

Practical Software and Systems Measurement

Comments to:
John Murdoch
Computer Science Department
University of York
YORK YO10 5DD UK

44 1904 43 2749
jm48@york.ac.uk

This paper is subject to the following copyright restrictions:

- The PSM Support Center is the sole manager of all PSM products and services and is the only one authorized to modify them.

- General Use: Permission to reproduce, use this document or parts thereof, and to prepare derivative works from this document is granted, with attribution to PSM and the original author(s), provided this copyright notice is included with all reproductions.

- Supplemental Materials: Additional materials may be added for tailoring or supplemental purposes, if the material developed separately is clearly indicated. A courtesy copy of additional materials shall be forwarded the PSM Support Center, psm@pica.army.mil. The supplemental materials will remain the property of the author(s) and will not be distributed.

- Author Use: Authors have full rights to use their contributions in an unfettered way with credit to the technical source.

Table of Contents

List of Figures

List of Tables

Executive Summary

Safety is an important property of many kinds of product systems and services. Achieving acceptable levels of safety in a product depends on many people working in a range of specialties, on the tools and knowledge available to them, and on the organizational systems that coordinate and integrate the work. The levels of risk that are considered acceptable by users and others affected by the system have to be understood. The resources and processes needed to reduce residual risks to acceptable levels, like all other project resources, have to be planned, justified and managed. Resources allocated to achieving acceptable residual risk levels have to be used as efficiently as possible. Trade-offs have to be supported between safety and other types of system performance and between different safety risks. Users and others exposed to risks usually require assurance that risks are sufficiently mitigated. Regulatory authorities may require visibility of safety work to support product certification.

This White Paper applies the PSM ISO/IEC 15939 measurement framework to the safety domain. A companion PSM White Paper considers security measurement. A dual approach is taken: ‘top-down’, to identify information needs and measurable concepts; and ‘bottom-up’, to identify measurable entities and their attributes that are available in safety processes.

Initial proposals are made for additions to the existing PSM guidance materials. These are viewed as a starting point, from which technical management and specialist communities can negotiate and develop improvements, based on evolving practical experience.

Implicit in this White Paper is the proposition that it is valid and useful to apply PSM to the safety domain. The traditional concerns of project management (cost, schedule, product quality) are as relevant to safety processes as to other parts of a project. However, safety is intrinsically a risk-based concept, and this aspect is accommodated in the PSM framework. Assessment of risk will usually involve subjective judgment; this is accepted in the proposals of the report, with measurement viewed as supporting increasing objectivity as experience is accumulated by developer and operator organizations.

The objective of the work is to support the difficult technical and management decision-making that safety-critical projects and operations present. Many accident investigations identify weaknesses in project and operations management as root causes. PSM applied to the safety domain provides an opportunity to address such issues because it provides a framework to integrate measurement across technical, project and organizational levels.

PSM Safety & Security Measurement TWG

Workshop Contributors:

Dennis Ahern, *Northrop Grumman*
Jeff Allen, *LM*
Frances Anderson, *Aerospace Corporation*
Matt Ashford, *SEI*
Nadya Bartol, *BAH*
Molly Campbell, *US Army ARDEC*
Paul Caseley, *DSTL UK MoD*
Vivian Cocca, *DoD*
Erin Fitzsimmons, *Rockwell Collins*
Phil Flora, *Texas Guaranteed Student Loan Corp*
John Gaffney, *Lockheed Martin*
Gary Hafen, *LM*
Jan Janigan, *DoD*

Joe Jarzombek, *National Cyber Security Division, DHS*
Cheryl Jones, PSM, *US Army ARDEC*
Mike Kass, *NIST*

Greg Larsen, *Inst for Defence Analyses*
John Van Orden
Jim McCurley, *SEI*
Jim Moore, *Mitre Corporation*
John Murdoch, *University of York UK*
Dana Van Orman, *DCMA*
Sam Redwine, *JMU*
Don Reifer, *Reifer Consultants*
John Riedener, *US Army*
Rob Robason, *Wind River Systems*
Garry Roedler, *LM*
Amos Rohrer, *BAE Systems*
Ioana Rus, *Fraunhofer USA, University of Maryland*
David Seaver, *PRICE Systems*

Dave Zubrow, *SEI*

Thanks also to the additional reviewers of this report, including:
Fred Hall
Ken Astley, *Loughborough University, UK*
Antony Powell, *University of York, UK*

1 Introduction

1.1 Background: Purpose of the Safety & Security TWG

This White Paper is the result of work by the Safety & Security Technical Working Group of PSM, carried out during the period March – February 2004, and updated January 2006.

The objective of this work has been to propose additions to the existing PSM guidance materials appropriate for organizations and projects developing safety- and security-critical products. It is expected that the proposals will be improved and extended following wider consideration by the specialist communities and project trials.

The objectives of the PSM initiative are, broadly, to support 'measurement-based' technical management at project, capability and enterprise levels. PSM is reviewed in Appendix 2; further information is available in [1] and on the PSM website (www.psmsc.com).

The Safety & Security TWG has the objective of developing four additions to the PSM materials as follows:

1. Additions to the PSM *I-C-M Table* (**I**nformation Category – Measurable **C**oncept – Prospective **M**easure Table);
2. *Measurable Entity Model*, describing representative safety- and security-related entities, and their attributes, that are used in the Measurement Information Specifications;
3. *Measurement Information Specifications* for new measures introduced to serve safety & security; modifications/ additions to existing Measurement Information Specifications, where existing measures can be broadened to also serve safety & security needs;
4. PSM Safety & Security *Measurement Guidance Notes* on use of the above, consistent with the PSM *Measurement Process Model*.

These materials depend on developing sufficient understanding of the basic concepts involved in the engineering and operational delivery of safety and security properties.

PSM has been influential in the development of ISO/IEC 15939 [2] and related ISO standards. This establishes a common international language and concept for measurement. PSM may be viewed as a means for developing the measurement *experience base* that is part of the ISO/IEC 15939 model.

The capability maturity models (CMMs) emphasize *process stability* and *continuous improvement*. These models call for processes eventually to be *institutionalized* as *quantitatively managed*, an expectation now carried over to safety processes [3]. Safety and security extensions have been proposed for the CMMI model [4], informed in part by earlier work on +SAFE [5].

The motivation for the PSM project is derived mainly from the technical management and acquisition communities. PSM seeks to provide objective facts to inform the project manager, covering, for example, planning and estimation, cost and schedule control, timely detection of problems, resource allocation, and the monitoring of key performance indicators. In some areas, subjective judgment is an important input to measurement; explicit (and where possible,

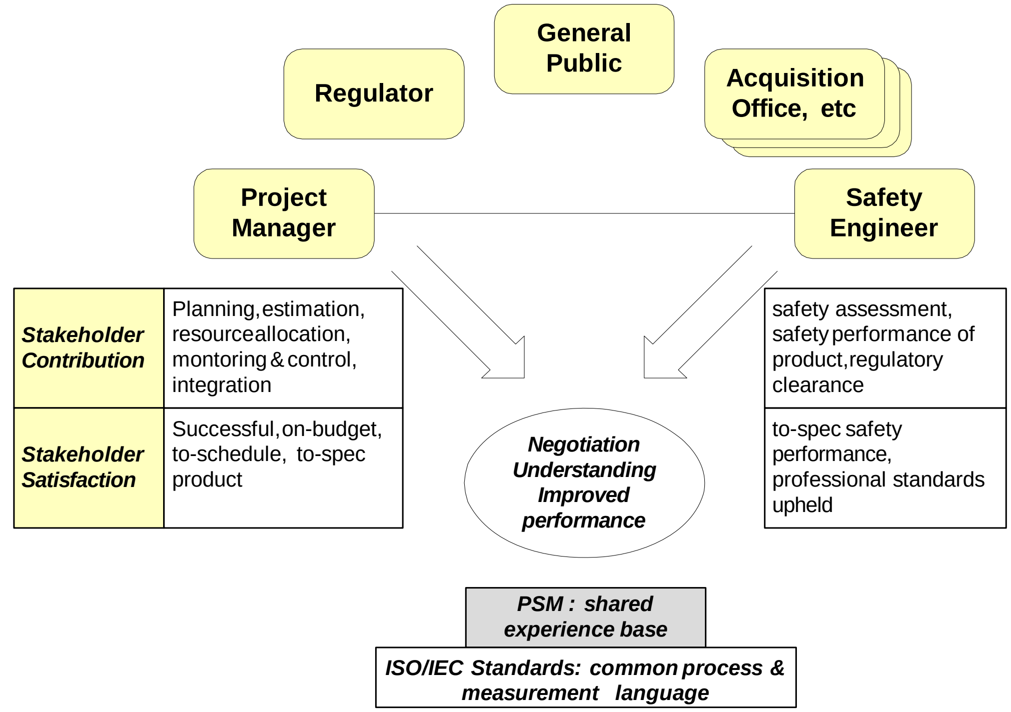

General Public
Regulator
Acquisition Office, etc
Project Manager
Safety Engineer
Stakeholder Contribution
Planning, estimation, resource allocation, montoring & control, integration
Stakeholder Satisfaction
Successful, on-budget, to-schedule, to-spec product
safety assessment, safety performance of product, regulatory clearance
to-spec safety performance, professional standards upheld
Negotiation Understanding Improved performance
PSM : shared experience base
ISO/IEC Standards: common process & measurement language

Figure 1 PSM and ISO/IEC 15939, viewed as a platform for measurement negotiation

quantitative) recording of such measures enable subjectivity to be tested and integrated with objective data.

Those working at technical/ specialty levels also have professional responsibilities and measurement needs. Engineering specialties involve activities, models and measurements of significant complexity. PSM may be viewed as a platform on which measurement needs can be negotiated between the stakeholders involved (Figure 1).

PSM was originally developed to support the management of software development projects. From version 4.0, PSM also supports systems engineering processes. Current work in conjunction with the INCOSE Measurement Working Group is extending PSM to include the technical performance measures and related indicators used by the systems engineering community [6]. Safety and security may be viewed as sub-specialties within the systems and software engineering domains; recommendations made here should integrate with the broader systems work (Figure 2).

The technical management of critical systems during development and operation is a challenging task. Safety-critical systems are costly to develop, usually involve high levels of interaction across the supply chain and with regulatory organizations, and are prone to high change and re-work costs. It can be difficult to argue for investment in risk reduction activity when successful outcomes are intangible (i.e. absence of failures). Measurement and estimation can provide the justification for such expenditures.

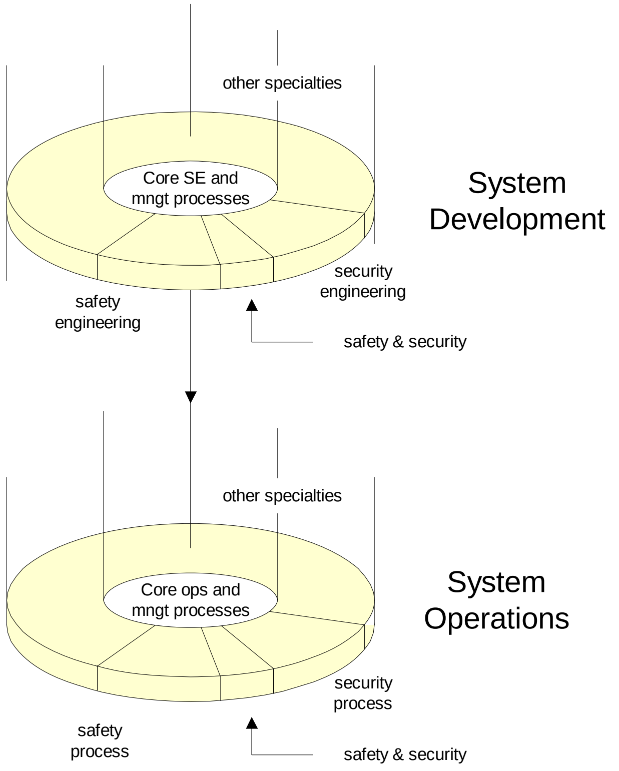


Figure 2 Safety and security processes viewed as specialist domains contributing to core systems engineering (SE), management and operations processes

1.2 Objectives: Purpose of this White Paper

This White Paper addresses safety measurement: a companion PSM White Paper [7] considers security measurement. A common measurement approach is developed for the two areas, based on the dependability and security definitions of [8]. The objectives of this White Paper are as follows:

- To propose an approach to the measurement of safety, consistent with the general objectives and approach of PSM, as a prototype of the PSM additions identified above;
- By this means, to provide a platform for dialog with the safety specialist community, leading to improvements in the proposals;
- To build on current proven practices in the safety specialty domain as far as we are currently aware of them, but to invite wider experience and comment;
- To enable consideration by the wider PSM community, to ensure consistency.

Figure 3 summarizes the role of this White Paper as a means for launching the establishment of a shared experience base for the measurement of safety processes, within the framework of PSM.

All aspects of this report are subject to review and questioning. The appropriateness of the PSM approach for supporting the technical management of safety work is a working hypothesis. The

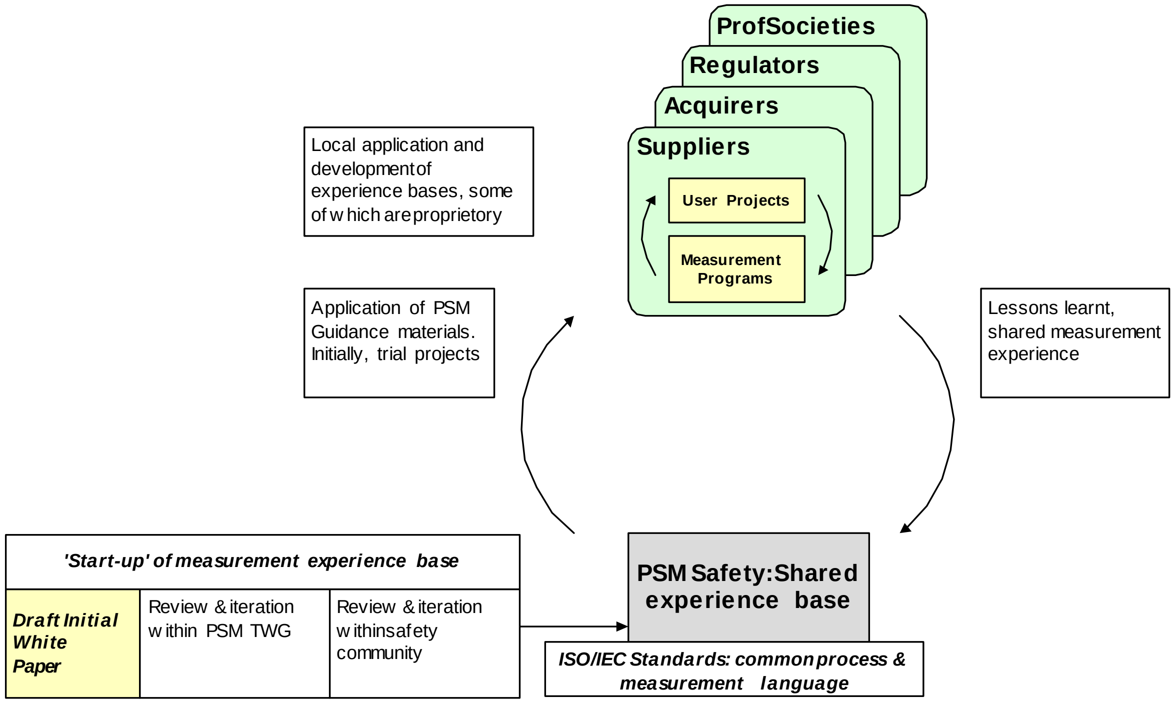

ProfSocieties
Regulators
Acquirers
Suppliers
User Projects
Measurement Programs
Local application and development of experience bases, some of which are proprietory
Application of PSM Guidance materials. Initially, trial projects
Lessons learnt, shared measurement experience
'Start-up' of measurement experience base
Draft Initial White Paper
Review & iteration within PSM TWG
Review & iteration within safety community
PSM Safety: Shared experience base
ISO/IEC Standards: common process & measurement language

Figure 3 Role of this White Paper in launching a measurement experience base for safety

approach to applying PSM, proposed in the following, is open to challenge and comment. Proposals for measurement concepts made here are to be validated by field trials. Contact details are given in Section 5.

1.3 Organization of the Paper

Section 2 briefly reviews the safety domain. Section 3 develops an approach to safety measurement using the PSM process. Draft guidelines for performing safety measurement are included in Section 4. A glossary of terms is provided in Appendix 1. The PSM framework and the method used to develop safety measures are reviewed in Appendix 2. Further Appendices provide definitions of selected terms, proposed additions to the PSM I-C-M Table, a proposed Measurable Entities Model and draft Measurement Specification Tables.

2 Overview of Safety

2.1 Fundamentals

Safety has been defined as the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [9]. Such concerns can arise in many kinds of application; here it is assumed our interest is the safety of software-intensive systems, for example, defense/ aerospace systems, including digital electronic hardware and software components.

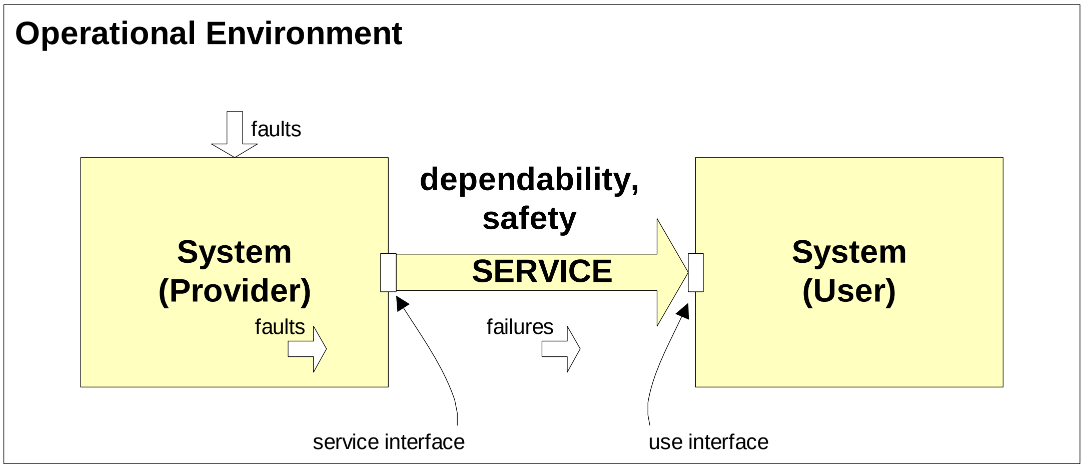


Figure 4 Context in which safety is defined: a provider system, a user system and a provided service [8]

It is generally recognized that complete freedom from such risks is unattainable; the objective is to reduce residual risk (that is, the risks remaining after purposeful risk reduction efforts) to acceptable levels. There are five fundamental concerns in product system safety:

1. How safe is safe enough? What levels of residual risk are acceptable to users and other affected parties?

2. How much should be spent to reduce risk levels?

3. What are the risks presented by the product system/service and what are the most efficient and effective means to reduce risks? Given the resources allocated to risk reduction, and other constraints, have the risks been reduced as much as possible?

4. Have all applicable standards and regulatory requirements been met?

5. How much should be spent to provide assurance to users and other parties? In regulated industries, how much should be spent to enable the regulatory authority to certify the system?

These concerns are inter-dependent; the level of acceptable residual risk may be determined in part by the estimated cost of further risk reduction (using the ALARP Principle – *As Low As Reasonably Practicable*). The estimated cost of further risk reduction depends on the feasible means of reduction that have been identified. Quantitative techniques can be applied to support many decisions of these kinds.

2.2 Safety and Dependability

Safety is a property of a *system* or *service.* A *system* is an entity that has internal structure and interacts with other systems. We are interested in systems that are engineered; i.e. are developed and then operated to achieve some useful purpose. Software-intensive systems tend to be complex, meaning that they are composed of many components of different types which interact with each other to create properties not exhibited by the individual components. The purpose of the system is implemented as the *service* the system, acting as a provider, delivers to a user system (Figure 4).

The user system is dependent on the provider system for the service. The delivered service usually will have many properties, depending on its type. Among these, the user system will be concerned about the *dependability* of the provider system, or, equivalently, of the provided service:

Definition:	**Dependability** (of a system delivering a service)
1	The ability to deliver a service that can justifiably be trusted. (calls for a justification of trust)
2	The ability to avoid service failures that are more frequent and more severe than is acceptable (implies criteria for deciding whether a service is dependable)
Source:	[8]

The second definition indicates a measurement approach to dependability, based on the likelihood and severity of service failures.

A particular service can fail in a variety of ways, resulting in dependability being a composite property, covering the following more specific properties (*more* of the property is indicative of *fewer* or *absence* of the corresponding failures):

Dependability Property of a System	**Associated Types of Service Failure**
Availability (readiness for correct service)	failures implied by the service being *incorrect*
Reliability	interruption or outage in correct service over a time interval
Safety	failures that cause catastrophic harm to users or the environment
Integrity	improper/unauthorized system alterations
Maintainability	service failures resulting from a system being difficult to successfully maintain during use

Treating safety within a dependability framework is useful because it enables integration with security measurement, developed in [7].

Definition:	**Safety** (of a system delivering a service)
1	The ability to deliver a service that can justifiably be trusted not to cause harm (calls for a justification of trust).
2	The ability to avoid harmful service failures that are more frequent and more severe than is acceptable (implies criteria for deciding whether a service is dependable).

2.3 Faults and Errors

A service failure implies that the provider system's external states (i.e. those states observable by the user at the provider's service interface) deviate from the external states associated with the provision of a correct service. This deviation is called an *error*. The adjudged or hypothesized

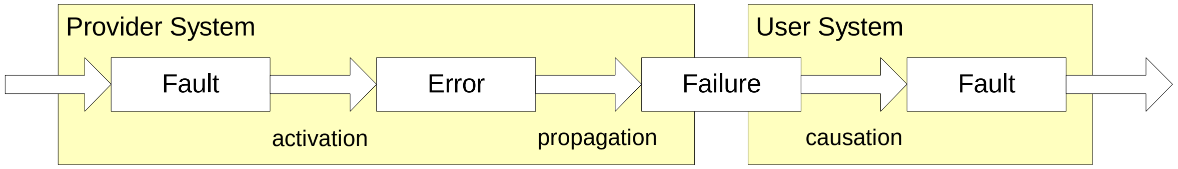


Figure 5 The propagation of the effects of a fault, from its activation to create an error in the system state, to propagation to a failure in a provided service, to causing a fault in a user system.

cause of an error is called a *fault*. Faults may be located within the provider system and/or in its environment.

Figure 5 shows the relationship between the definitions of faults, errors and failures, adapted from [8]. For brevity, the chain of threats represented by Figure 5 is called here a *fault path.* The recursive nature of this concept implies that the model can handle 'systems' failures, as developed below in terms of a systems theoretic model. The fault path is a simplified concept: a more detailed model might be in the form of a Fault Tree or Markov model. The relationship between the simplified fault path and Fault Trees is discussed further in [7].

The model is applicable to direct physical and logical cause-consequence chains, for example at component level. *Services* are usually viewed as *functions* in such cases. The model of Figure 5 can be applied to development processes; a fault in a component is the result of a failure in the service provided by its development process, which in turn, might be tracked back to a fault in the development system.

A service can fail in different ways, called *failure modes*. A system component might be analyzed and judged to present a specified set of failure modes to the system.

2.4 Hazards

Safety risk is usually expressed in the form of *hazards*, being those situations in which there is actual or potential danger to people or the environment. Hazards are described by their probability and severity. Hazards are error conditions that present the potential for a safety-related service failure, usually called an *accident* or *mishap*, to occur. The probability of a mishap occurring is expressed per unit of time, flight, event etc, depending on the context. The severity of a mishap might be expressed in terms of equivalent fatalities, or qualitatively in terms of a severity category (e.g. catastrophic, critical, marginal, negligible). Severity categories are defined in terms of the consequences involved (e.g. death, loss exceeding $1M etc). Applicable safety standards specify acceptable risk levels by means of probability-impact matrices. Those hazards that present unacceptably high risks have to be tracked and mitigated.

Both mishap probabilities and severities are difficult to assess early in projects. Current techniques in the safety field do not formally handle such uncertainties. A greater emphasis on safety measurement might support improvements in this area.

A significant effort is usually associated with the identification of hazards and also of potential failure modes and failure effect propagation paths that can cause hazards. Experience with

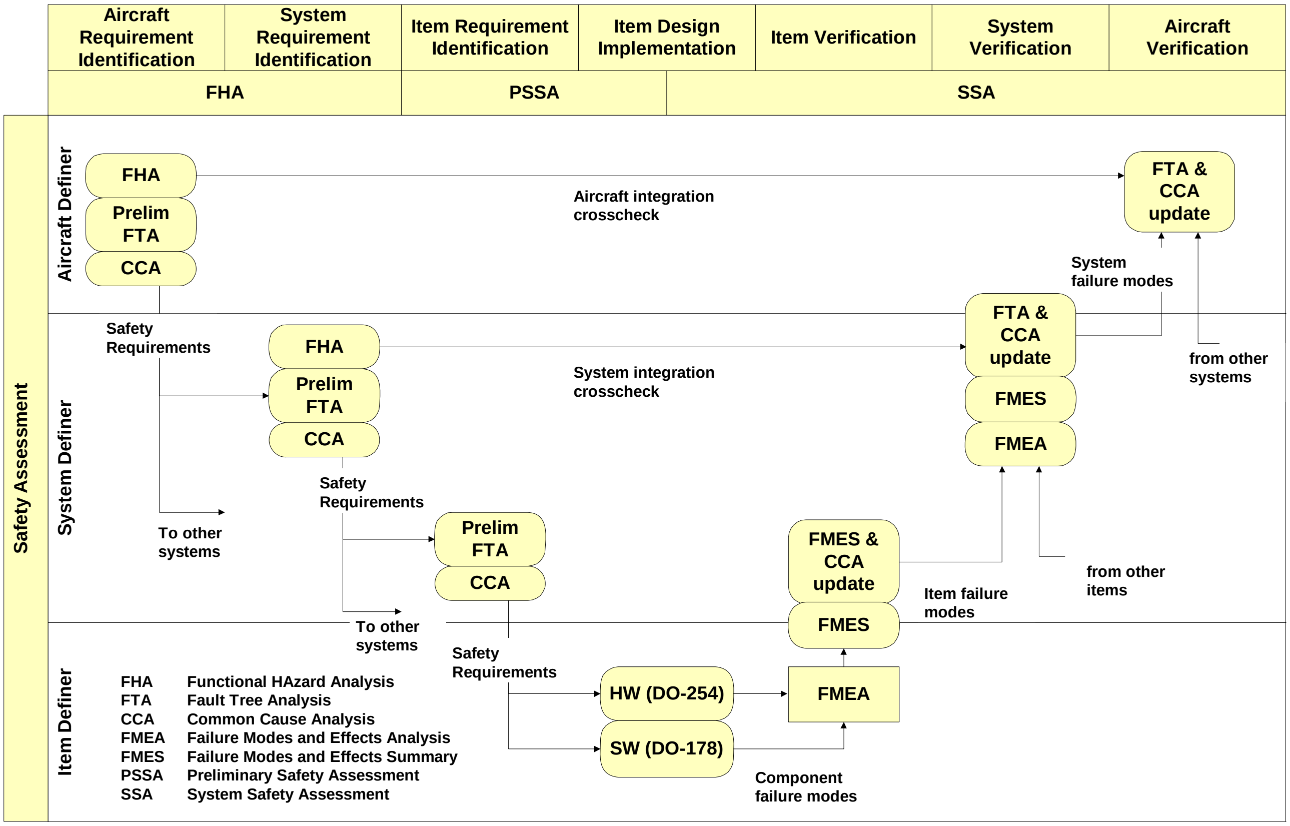


Figure 6 Example safety assessment process model (ARP 4754)

similar systems and technologies is usually needed and the application of lessons learnt is required by most standards and guidelines.   Care is required in assessing the productivity of such work; for example, a naïve count of identified hazards is not an indicator of the effectiveness of a hazard assessment activity.

2.5 System Safety

System safety engineering is the engineering discipline that addresses the achievement of safety of integrated systems; it supports *systems engineering*.   System safety develops safety requirements applicable to subsystems etc, based on customer safety requirements and system architecture. Safety assessment establishes that overall safety objectives will be met if subsystem developers meet the cascaded safety requirements. Subsequent verification activity establishes that safety requirements are met by manufactured and integrated systems.

The applicable US DoD standard is MIL-STD-882D [9] which cites the Systems Safety Engineering Handbook of the System Safety Society [10] as a source reference for methods and techniques used within the discipline. MIL-STD-882D defines system safety engineering as an engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk. System safety guides and integrates specialty safety engineering in different technologies, e.g. nuclear, structural, software etc. Other standards are applicable in other nation states; for example, the UK has MoD Defence Standard 00-56 [11] applicable to the safety management of military systems containing programmable electronic components.

Civil standards in this domain are more harmonized between the US and Europe. Developers of civil aerospace systems follow the guidelines developed by the SAE, namely ARP 4754/ARP 4761 [12] [13], which describe a model system safety assessment process and provide guidance on safety assessment techniques. These guidelines cite RTCA-EUROCAE DO-178B for software in airborne systems and DO-254 for electronic hardware.

Figure 6 shows the reference safety assessment process model of ARP 4754, illustrating some of the features reviewed here.

There are many other standards and guidelines in the safety field, at integrated process level (e.g. IEC 61508), at the level of safety assessment techniques (i.e. for FMEA, HAZOP) and applicable to different industries and technologies (e.g. nuclear, transportation, programmable controllers).

A combination of the assessment of safety risk and of the resources deployed in achieving risk reductions informs safety decision-making. The acceptability of a residual risk depends on the cost of further reduction; this may be a system-wide engineering judgment. While each hazard has to be assessed and its associated mishap risks reduced to acceptable levels, there are additional system-wide concerns; how can the total system hazard risk be reduced optimally, given the resources available? Work to reduce one hazard risk might be better re-directed towards another. Should resources being deployed to achieve a percentage improvement in a different performance parameter be better deployed in safety risk reduction? Safety measurement should provide the means to answer such questions.

2.6 Software Safety

Although software cannot by itself cause death or injury, software failure modes can give rise to system-level hazards. A software failure can result in an effect propagation path that traverses the host system and human operational system to cause hazards for users and the environment. Emphasis is placed on accuracy of the specifications of the required software behavior, on establishing that delivered software meets the specifications and that any side effects involved are acceptable.

The impossibility of exhaustively checking all possible execution paths of software components, has given rise to the use of *Safety Integrity Levels* (SILs). More rigorous and exhaustive techniques are required to be used for modules that are classified at higher integrity levels. This approach has been criticized on the grounds that there is little evidence that safety properties are improved by use of particular techniques etc.

A reference software safety process has been defined recently by the US Navy [14]; this is used in the following as an example source of measurable entities. The applicable UK standard for safety-critical software in military equipment is MoD Defence Standard 00-55 [15]. This standard, currently being updated, caused controversy some years ago because of its requirement to use mathematical formal methods in software specification.

Increased use of measurement in software safety may inform how better to allocate development and assessment resources.

2.7 Safety Management

Many accident investigations conclude that root causes are to be found at management levels in developer and operating organizations; the recent Columbia report [16] is an example. The PSM measurement framework is motivated by management and acquisition needs. If applied well, PSM will support safety management, by providing timely indicators of problems, and more visibility and transparency in decision-making.

2.8 Trust and Assurance

The user system of Figure 4 is *dependent upon* the provided service to some level, determined by the criticality of the service to the user's operations. To benefit from the service, the user must be prepared to place some level of trust in the provider system. Following [8], trust is defined as *accepted dependence*. The user's criteria for trusting the provider system are expressed in the terms of the dependability and safety of the system; i.e. failures in the provided service have to occur with acceptable frequency and severity. How does a user establish trust in (or assess the dependability of) a provider system? The user requires some evidence on which to assess the dependability of a product or service. The provision of such evidence is called *assurance*.

Both military and civil flight systems have to gain Flight Airworthiness certification from the respective military and civil governmental organizations. Certification is closely related to conformance with applicable standards, but also involves independent assessment of systems design and the mitigation of hazards. In the UK, certification has led to the requirement for *safety cases*, which document the safety justification of a system. Safety cases can be used throughout the system lifecycle, for example to document changes made during operational phases. If a safety process is producing a safety case, then the resources consumed and facets of the information produced are candidates for measurement. The concept of an *assurance argument* is being developed as a means to integrate the evidence of dependability of complex systems [17].

Assurance, as defined here, represents the risk mitigation needs of the customer (or party for whom assurance is developed). Developer organizations have a similar need to mitigate risks, but the set of risks would usually be different from, if overlapping, the user risks. Engineering usually has to consider a wider set of concerns and trade-offs, associated with all aspects of system development.

2.9 Safety as an Outcome of Collaborative Work

The achievement of acceptable levels of safety in a product is the result of collaborative effort between safety engineers, design engineers, systems engineers, managers at various levels and others. Work is typically distributed across a complex network of acquisition, regulatory, and supplier organizations. It follows that an assessment of progress within a project in achieving acceptable safety reaches outside the safety engineering specialty itself, to include aspects of other technical and management processes.

In applying PSM to safety, it is anticipated therefore that parts of the existing measurement framework are needed for safety measurement. We have to investigate whether additional measurable concepts and prospective base measures are needed and how these might be integrated within the existing framework to provide additional safety-related information.

The application of measurement principles has to address this diversity in an integrated way. An approach to measurement is proposed that associates measurement with ‘closing the loop’ between decision-makers and the effects of actions they undertake. A systems-theoretic approach has been developed in the safety domain [18] and has been adopted in the approach to security measurement proposed in [7].

2.10 Safety Techniques

The wide range of types of system and industry in which safety concerns arise has resulted in a large number (> 200) of safety techniques, differences in terminology and in practices. Even within the aerospace and defense industries, terminology and processes are not harmonized. The development of measurement guidance in the safety domain should be sensitive to these differences; guidance should be adaptable to different safety practices. However, to be of practical use, guidance must be specific *enough* to help with measure identification and selection.

Both qualitative and quantitative techniques are used in safety engineering. In a typical project, applied techniques might include:

- Functional Hazard Assessment (FHA)
- Fault Tree Analysis (FTA)
- Failure Mode Effects (and Criticality) Analysis (FMEA/ FMECA)
- Markov Analysis (MA)
- Event Tree Analysis (ETA)
- Common Cause Analysis (CCA)

Such techniques are fundamental to the identification of hazards and the assessment of probabilities and severities. From the technical specialty point of view, they involve the measurement of safety risk. The work activity and work products involved are measurable from a project management point of view.

2.11 Process Maturity Models

In addition to military and industry standards, organizations are using Capability Maturity Models (CMMs) to assess process capability and maturity. Use of CMMs allows an organization to assess their process implementation against a reference model, and baseline their performance against an industry benchmark. CMMs also provide a roadmap of best practices to guide process improvement within an organization. CMMs have been developed for a range of disciplines and domains, such as software, systems engineering and acquisition. Recently, the CMM Integration (CMMI) model [19] was developed, integrating multiple disciplines into a single reference model. The Australian Department of Defence sponsored work to extend the current CMMI to include safety [5]. Figure 10 shows the process framework recommended by the +SAFE project. Further efforts are currently underway to refine the +SAFE model and to extend it to include Security & Information Assurance.

A recent project undertaken by the FAA and DoD has drafted proposals for safety and security Application Areas within the CMMI framework [4].

3 Safety Measurement

This Section applies PSM to the safety specialty. The general approach adopted is described in Appendix 2.

3.1 Typical Information Needs

Table 5 (Appendix 2) distinguishes three levels of generic management responsibility: *enterprise*, *organization* and *project*. Figure 7 applies this to the safety domain and adds the following roles:

- *Specialty engineering*: the safety specialty works with design, software, and other specialty engineers to achieve safety performance in delivered systems; measurement of safety outcomes therefore involves processes additional to safety;
- *Systems Engineering*: integrating discipline that has responsibility for technical trade-offs with other kinds of technical performance;
- *Acquirer*: the PSM framework is motivated by improving communication between acquiring and developer organizations;
- *Developer*: for smaller projects, the developer organization needs to track product safety, possibly without an identified systems engineering process;
- *End User/ Operator*: the safety outcomes are for the benefit of end-users;
- *Supplier*: complex supplier networks are involved in large projects; this role is included to cover such relationships;
- *Regulator*: the safety domain is subject to governmental regulation and certification.

An important consideration in the safety domain is the allocation of safety responsibilities and authority within organizations and projects. MIL-STD-882D recommends that authority for accepting safety risks should be established through various levels of management. In considering safety information needs for a particular project, a refinement of Figure 7could be developed that identifies the roles that carry safety authority for different mishap risk categories.

Having identified the safety-related organizational roles involved in each of the organizations involved in the project, their responsibilities may then be described. This then provides a basis for identifying the kinds of questions asked and the information needs of each role. Table 1 sketches this approach for a selection of roles.

The information needs identified in Table 1 are rather wide-ranging. The approach adopted here is to select a few information needs, considered to be important, and to develop measurement constructs for them. Table 2 lists the selected *Information Needs* selected here for further development.

The report of the Columbia Accident Investigation Board [16] recently identified management and cultural shortcomings in NASA as important contributory factors leading up to the accident. An application of PSM to the safety domain provides an opportunity to address such issues through measurement. Application of PSM to serve the distribution of safety authority in an organization would amount to supporting the flow of information between those involved. The

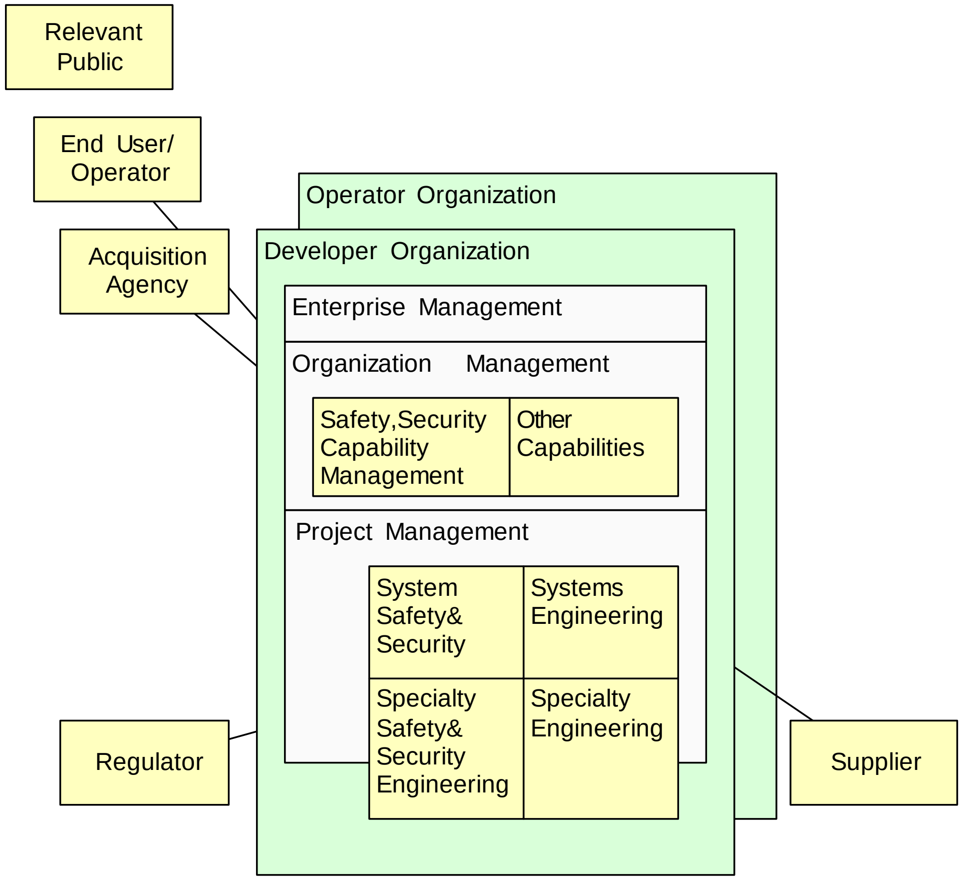


Figure 7 User model for safety measurement in a Developer Organization (similar models can be drawn for operations, maintenance and support organizations)

planning and explicit design of such safety information flows might be beneficial for organizations seeking to improve the management of safety-related projects.

3.2 Measurable Concepts

A measurable concept is an idea about how an information need can be satisfied. It identifies possible entities and attributes to be measured and how results can be used in decision-making. Each of the ten questions in Table 2 is considered below and a measurable concept is proposed. Prospective measures associated with these concepts are discussed in Section 3.3.

What is the (operator-perceived) safety performance of the system in operation?
The eventual desired outcome of a safety-critical project is the absence of accidents throughout the operational life of the product. This outcome is achieved by many processes and disciplines working together – not only safety staff. Safety performance as experienced in operations is considered to fall under the *Product Quality* Information Category of the existing PSM framework. A new Measurable Concept *Dependability – Safety* is proposed, analogous to the existing *Dependability – Reliability*. New base measures will be required involving the occurrence of incidents and accidents.

	Example Safety Role	**Typical Responsibilities**	**Typical Information Needs**
1	*System Acquirer*	Overall management of the project within the acquiring organization Acting on behalf of the end user.	Does the contractor have the required capabilities and maturities to successfully deliver on this project in areas of safety culture, organization, technical capability, process and personnel? Is the optimum balance being achieved between user requirements, technical constraints and developer resources? Are the residual mishap risk levels acceptable? Is the acquirer getting good value?
2	*System Operator*	Operator of the product system Safe operation of the system as specified and agreed to at acceptance Conformance with operational constraints as agreed, in order to maintain residual mishap risks at acceptable levels	Will the system be operable with acceptable levels of residual mishap risk? What is the degree of confidence that safety objectives will be met throughout the system life cycle? What is the safety performance of the system in operation?
3	*Business Manager (developer organization)*	Overall oversight of projects and capabilities Commercial/ financial viability, profitability, competitiveness Organizational strategy, investment Safety program effectiveness Performance assessment of safety work on project Costs and investment Value of Safety Program outcomes for stakeholders Acceptance authority for allocated risk	Can this project be taken on with acceptable commercial and technical risk? Do we have the system safety capability required? What are the costs of meeting safety objectives? What are the commercial risks of mishaps? Can I authorize acceptance of this particular risk? What is the remaining work needed to achieve safety certification?
4	*System Safety Capability Developer*	Strategy for system safety capability development Development of assets ready for deployment on projects Performance and effectiveness of safety processes Organizational and process maturity development Continuous process improvement/ learning/ lessons learnt Supplier, customer, regulator capability engagement	How effective is the System Safety Process? How productive/ efficient is it (outcomes versus costs)? What needs to be done to improve system safety capability?
5	*Program Manager (developer organization)*	Overall management of project Planning, estimating, monitoring & control Delivery of particular product system to schedule, budget, technical performance Acceptance authority for allocated risk Allocated safety responsibilities, as specified in applicable standards	How confident are we that we can meet the required safety performance? What is the current progress/ degree of completion of safety work as compared with the current Plan? Have we identified and tracked all safety requirements? Are hazards, failure modes and mitigation actions being tracked? Can I authorize acceptance of this particular risk? What is the remaining work to be done to meet safety requirements? What is the current status/ degree of completion of safety assurance work?

6	*System Safety Manager (developer organization)*	System Safety Program planning and estimating Managing safety work as executed on project; progress and performance Management and integration of safety work undertaken by specialist safety engineers, suppliers Work achieved and resources used against Safety Plan Managing evolving scope of safety work and estimating remaining work to completion Safety achieved in operations Acceptance authority for allocated risk	What is the technical scope of the safety work? How is this evolving as the project is enacted? What is the current progress/ degree of achievement of product safety as compared with the requirements? How confident are we that we can meet the required and/or acceptable risk level for *this* particular accident scenario? What is the current status of tracked hazards, failure modes, and mitigations? Can I authorize acceptance of this particular risk? What is the level of compliance of safety work with applicable standards and regulations?
7	*Safety Engineer*	Identification of mishap risks; likelihood and severity. Management/ mitigation of identified hazards. Management of unidentified hazards (completeness and coverage of analyses). Acceptability of residual risks. Maintenance of safety during operations Maintenance of safety during disposal Acceptance authority for allocated risk	What are the hazards/ failure modes/ mitigation strategies of this unit, subsystem/ function? What is the impact of *this* proposed change for safety work? What is the likelihood of this mishap/ failure mode; what is its effect/ damage? What is the progress on this particular mitigation action? Can I authorize acceptance of this particular risk?
8	*Regulator*	Certification of a product or system as acceptably safe, secure for use, acting on behalf of Government and general public.	Can the product be certified as acceptably safe, given the provided safety assurance argument and supporting evidence, data. Are the developer and operating organizations sufficiently capable to deliver safe system operations?
9	*General Public*	Two situations: (a) user of the system, for example as a passenger; responsibilities may include compliance with procedures, restrictions; (b) bystander role, in which case there are no responsibilities.	Is the system acceptably safe for it to be used, to have operating in society, given the benefits the system offers? Are professional standards being applied?

Table 1: Example safety roles, responsibilities and information needs

What is the (customer perceived) safety performance of the system in operation?
Safety performance as experienced by users/customers/relevant publics is considered to fall under the *Customer Feedback* measurable concept of the existing PSM framework. New base measures will be required involving the occurrence of incidents and accidents that affect these groups.

What is the mishap risk associated with this particular hazard?
This question lies at the heart of safety engineering and is an output of the safety technical process. Acceptance of residual risks usually involves management staff because of the consequential organizational risks. The measurable concept *Dependability – Safety* is proposed, applied in this instance to a single hazard. The intention of this measurable concept is to enable the consideration of safety risks throughout the technical and management structure of developer and acquiring organizations. Although an important system property, safety is only one aspect of performance. Trade-offs with other technical performance measures would normally be undertaken by the systems engineering function.

What is the mishap risk associated with the total system (all hazards)?
This question is similar to the last one, except that it concerns system-wide safety risk. The same measurable concept is proposed: Dependability – Safety, applied to all hazards of the system. Safety concerns at this level include the optimum distribution of risk and mitigation effort between identified hazards and the effort deployed on further hazard identification and trade-offs with other system properties in a resource-constrained project.

What is current status of the hazard mitigation for the system?
The work identified to reduce identified hazard risks to acceptable levels is tracked and monitored. There are two ways of thinking about this: (1) work progress in terms of completion of work packages compared with a plan and (2) currently achieved risk levels compared with target residual risk levels as expressed in safety requirements. The first interpretation would be informed by the existing *Work Unit Progress* measurable concept. The second interpretation would be informed by the *Dependability - Safety* measurable concept.

What is the current degree of completion of safety work, as compared with the current Safety Plan?
This question relates to the monitoring of work progress as defined by the Safety Plan. The existing PSM concept *Work Unit Progress* is suitable for this, provided it is understood that requirements, actions, etc include those sourced in the safety domain. In order for the work of the safety process to be distinguishable from other processes, it will be necessary to flag those requirements that are safety requirements, and those actions that are associated with hazard mitigations, for example. It is assumed that this measurable concept is measuring the progress of work against that which has been declared necessary (via the Plan). Assessment of progress is as declared by safety and other staff.

What is the remaining work needed to meet safety objectives?
This question relates to estimating the safety work that is needed on a project. It is determined by the customer/user safety requirements and the system design. It is proposed to introduce a new measurable concept *Scope – Safety* to inform this information need. The intention is that this measure will identify those parts of the system (units, modes, functions) that are safety-related and therefore subject to safety assessment and engineering. Assessment of safety scope

Safety Role	**Information Need** *Identify what the measurement user (e.g., manager or project team member) needs to know in order to make informed decisions.*	**PSM Information Category** *Identify the PSM standard information category name (such as Schedule and Progress), or indicate that this is a new category.*	**Measurable Concept** *Name or describe the concept (an idea for satisfying the information need by using relevant entities and their attributes).*
System Operator	What is the (operator-perceived) safety performance of the system in operation?	Product Quality	Dependability – Safety*
General Public/ end user	What is the (customer-perceived) safety performance of the system in use?	Customer Satisfaction	Customer Feedback
Business Manager (developer organization)	What is the mishap risk associated with this particular hazard?	Product Quality	Dependability – Safety*
Business Manager (developer organization)	What is the mishap risk associated with the system (all hazards)?	Product Quality	Dependability – Safety*
Business Manager (developer organization)	What is the current status of the hazard mitigation for the system?	Product Quality	Dependability – Safety*
Program Manager (developer organization)	What is the current degree of completion of safety work, as compared with the current Safety Plan?	Schedule and Progress	Work Unit Progress
System Safety Manager (developer organization)	What is the remaining work needed to meet safety objectives?	Product Size, Stability and Scope*	Scope – Safety*
System Safety Manager (developer organization)	What is the level of compliance of safety work with applicable certification regulations?	Product Quality	Assurance – Safety*
System Safety Manager (developer organization)	What is the degree of compliance of the performed processes?	Process Performance	Process Compliance
System Safety Capability Developer	How effective is the System Safety Process?	Process Performance	Process Effectiveness

Table 2: Example information needs, categories and measurable concepts arising in the safety domain

(* proposed modifications to PSM I-C-M Table v5.0d)

will evolve as the system is defined. It may be appropriate to consider scope at different integrity / assurance levels. It may be appropriate to consider the different safety specialties (e.g. nuclear, material, software) involved.

What is the level of compliance of safety work with applicable certification regulations?
Conformance with guidelines of standards is important in the safety field, mainly because of the need to establish a legal defense in the case of an accident. The Measurable Concept *Assurance - Safety* is proposed to inform this information need.

What is the degree of compliance of the performed processes?
Conformance with the requirements and guidelines of standards is important in the safety field, mainly because of the need to establish a legal defense in the case of an accident. The existing measurable concept *Process Compliance* is appropriate for this information need.

How effective is the System Safety Process?
This question relates to the need to assess the effectiveness of safety processes in an organization. The existing measurable concept *Process Effectiveness* is appropriate for this information need. However, we need to select new base measures. It is proposed that the effectiveness of the safety process can be detected (in part) from the actions that are taken as a result of safety assessment (e.g. associated with risk mitigations). These actions may be triggered across a wide range of product processes, depending on the mitigation strategies adopted.

Table 2 summarizes the proposed mapping between information needs and measurable concepts.

Many of the measurable concepts existing in the PSM framework can be applied to safety work.

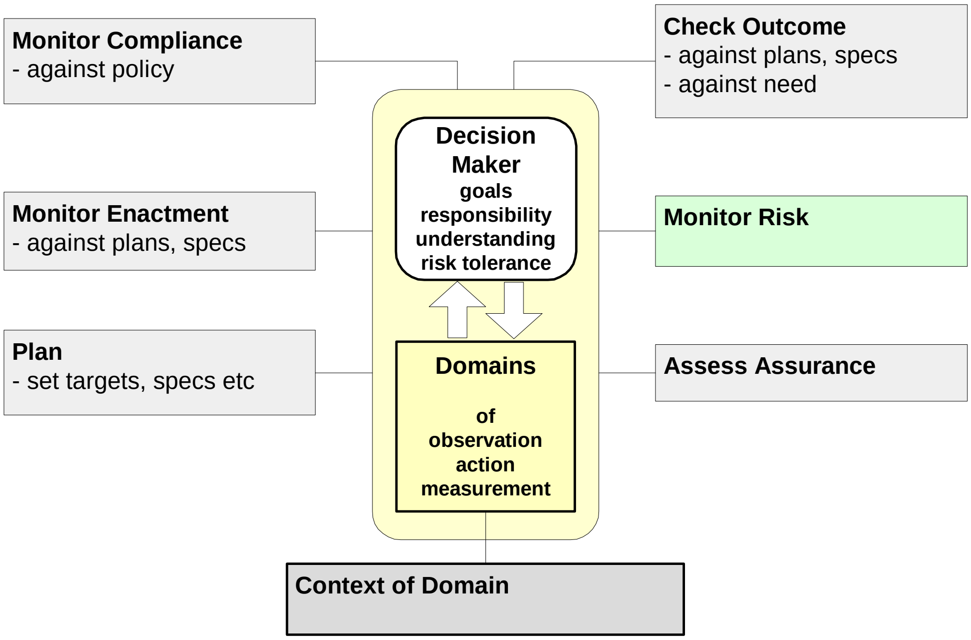


Figure 8 Generic information needs arising when a plan is enacted under uncertainty

In addition, three new measurable concepts are proposed:

Scope – Safety: to measure the ‘size’ of the safety task, in terms of the scope of the product system that is safety related and is subject to a safety process. This measure can be interpreted in several ways, depending on life cycle phase and purpose, for example, *estimated* and *actual*. Uncertainty about required scope of assessment early in a project implies a multi-pass approach with varying depths of assessment, depending on safety risk. Scope could be linked to depth of assessment.

Dependability – Safety: to measure the main technical concern of safety assessment processes in terms of identified hazard risks. This measure can be interpreted in several ways (for example target, expected, contingency, achieved residual and achieved operational levels); choice of measurement construct will depend on information needs. Risks can be treated on a per-hazard basis and integrated across the system. This measurable concept is directed at serving engineering and technical management trade-offs and progress monitoring.

Assurance – Safety: to measure progress in achieving regulatory approval of safety-critical products. This measurable concept is applicable to assurance work products such the safety case and certification data.

Assessing the effectiveness and efficiency of safety work will require combining these measures with other existing PSM measures, particularly measures of resources deployed to achieve risk mitigation. Additional relevant measures will be associated with processes other than safety; it will be necessary to flag work in a design or test process, for example, as being associated with safety risk mitigation work, if the full costs of safety are to be detected.

3.3 Safety Measurement Map

Safety measurement needs arise in a wide range of decision situations. We would like to have an entry point to measurement guidance that is applicable to all safety-related decision situations that arise in the development and operation of software-intensive systems.

A set of categories of measurements is developed that aims to be complete, in the sense that all issues that arise in safety are covered by the single categorization. Subsequent research and practical experience will then develop guidance linked into this framework, including the development of constructs from measurable concepts etc. If the categorization is found to be incomplete, it can be extended.

The systems-theoretic approach proposed in [7] starts with the identification of a decision-maker (assumed to have the information need) and the type of information need involved, which amounts to an identification of the type of decision process and measurement. The generic model of Figure 8, based on the classic PDCA cycle, with the addition of *compliance*, *risk* and *assurance*, is proposed as an underlying rationale for developing measurements in the safety domain.

Figure 9 shows the implied safety measurement map, which corresponds to the security measurement map proposed in [7].

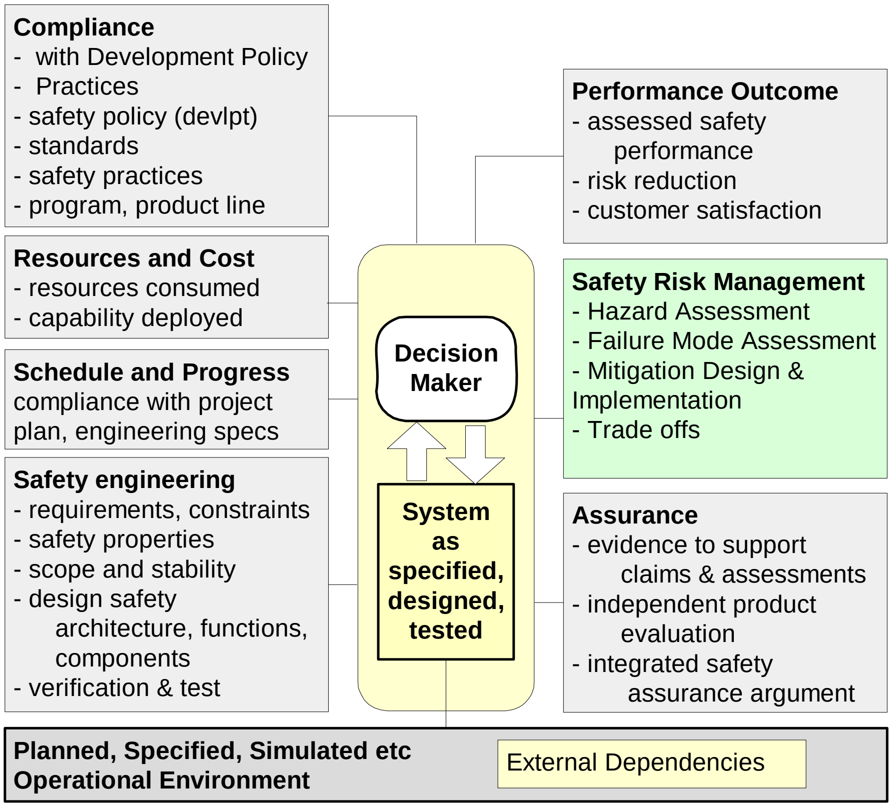

Compliance
- with Development Policy
- Practices
- safety policy (devlpt)
- standards
- safety practices
- program, product line
Resources and Cost
- resources consumed
- capability deployed
Schedule and Progress
compliance with project plan, engineering specs
Safety engineering
- requirements, constraints
- safety properties
- scope and stability
- design safety architecture, functions, components
- verification & test
Performance Outcome
- assessed safety performance
- risk reduction
- customer satisfaction
Safety Risk Management
- Hazard Assessment
- Failure Mode Assessment
- Mitigation Design & Implementation
- Trade offs
Assurance
- evidence to support claims & assessments
- independent product evaluation
- integrated safety assurance argument
Decision Maker
System as specified, designed, tested
Planned, Specified, Simulated etc Operational Environment
External Dependencies

Figure 9 Safety Measurement Map - system development

The following seven measurement headings cover the types of measurement needed to support decision-making during system development at project management level:

1. Safety Engineering (includes product size, stability and scope relating to safety; also aspects of product quality);
2. Schedule & Progress;
3. Resources and Cost;
4. Compliance (includes process compliance);
5. Performance Outcomes (includes process effectiveness and customer satisfaction);
6. Safety Risk Management (includes aspects of safety product quality);
7. Assurance (relating to safety).

3.4 Prospective Measures

This Section considers prospective measures for the measurable concepts of Table 2.

Scope – Safety

Product Size, Stability and Scope	Scope - Safety	Safety Requirements
		Safety-Critical Functions
		Safety-Critical Components
		Safety-Critical Interfaces
		Safety-Critical Modes
		Safety Zones
		Safety Change Workload

This measurable concept is intended to provide technical input to the estimation and planning tasks at the beginning and throughout a safety-critical project. It addresses the ‘size’ of the safety-related parts of the total system, i.e. those components etc. that are involved in carrying safety-related functions (Figure 10). This will be unknown initially for unprecedented systems or parts of systems. However, in most practical projects, previous experience can be applied to assess the needs for safety assessment and engineering. The proposal seems to match the intent of the existing PSM concept of *Product Size and Stability*. Prospective base measures would include:

Safety Requirements: Count of safety requirements and derived safety requirements versus total requirements; categorized by level of acceptable risk level, risk category or SIL.

Safety-critical Functions: Count of those functions that are safety related versus total functions.

Safety-critical Components: Count of those subsystems, units and components that carry safety-related functions versus total number of components.

Safety-critical Interfaces: Count of those interfaces over which safety-related flows are carried versus total number of interfaces.

Safety-critical Modes: Count of those modes, mission phases etc during which safety-related functions are delivered versus total number of modes.

Safety Zones: Count of those (spatial) zones of the system that are judged to require safety zonal analysis.

Safety integrity levels may be used as an input to assessing safety scope. For example, a system might be assessed as more safety-complex if it involves; (1) higher numbers of safety-related components/ zones, (2) higher levels of required integrity and (3) greater dispersal of safety-related components across the system. Such an indicator might be useful for estimation and resource planning purposes.[1]

Dependability – Safety

Dependability - Safety	Hazards
	Hazard Risk
	Hazard Scenario Risk
	Failure Modes
	Safety Assessments & Assumptions
	Mitigation Status
	Safety Incidents & Accidents

This measurable concept carries the assessed risk information that is central to safety-critical projects. There seem to be two basic sources of safety risk: (1) the mishap risks associated with identified hazards; (2) the risks associated with hazards and mishaps that have *not* been

[1] Proposal suggested by Matt Ashford

identified.   Ultimately, safety risks have to be managed such that residual risks are judged to be less than agreed thresholds or are otherwise acceptable.

Hazards: Tracking and monitoring the status of identified hazards is a fundamental task in safety processes. MIL-STD-882D, for example, requires a *Hazard Tracking System* to be set up. The number of hazards and their status (open, closed, priority level) during a project are candidate base measures.

Hazard Risk: The fundamental measure of interest is the risk associated with each hazard. Current practice in the safety field treats mishap risk as a function of the probability of the mishap occurring and the severity of its consequences. These assessments are usually highly subjective and are dependent on assumptions about the system operational environment and other factors.   Operational data (past accidents) are used wherever available, but field data is sparse for severe events. It is useful to treat subjectively judged risks as quantitatively as possible.   A hazard will usually be associated with more than one mishap or hazard scenario.

Hazard Scenario Risk: A hazard (or accident, mishap) scenario is a measurable entity proposed as a means of aggregating sets of failure modes, operational modes and other factors involved in a potential accident or mishap. A particular hazard may have many accident scenarios associated with it. *Hazard Scenario Scope* measures the scope of a particular hazard scenario. (This is related to the concept of a *cut set* in Fault Tree Analysis.) Risk reduction strategies may result in modifications to a potential accident scenario, for example, system responses and/or operator actions introduced to limit the propagation of failure effects. Such strategies may introduce additional potential accident sequences.

Failure Modes: The potential and actual failure modes of product components and subsystems are usually managed as a complement to hazards. Each identified failure mode has an assessed probability of occurrence and consequence for the system. Failure modes that raise safety concerns are linked to further investigation and/or mitigation strategies. Single point failures and common mode failures are of particular concern. The acceptability of a failure mode within a system is judged on the basis of the hazard scenarios in which it is active. We cannot be completely confident that we have identified all failure modes that carry safety risks. However, confidence can be assessed on the basis of safety scope and depth of assessment deployed. Confidence may be reduced by system changes, operational changes and reduced depth of assessment.

Safety Assessments & Assumptions: 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. Monitoring the number, scope and nature of safety assessments undertaken provides information on the depth of analysis that has been conducted.

Mitigation Status: a mitigation is a proposed action, analysis, or requirement that reduces a mishap risk to an acceptable level, or is likely to do so. This measure provides information on the risk reduction achievable and cost of a proposed mitigation.

Safety Incidents and Accidents: this measures the safety performance of a product system during the operational phase of its life cycle.   Incidents and near-miss events are usually important sources of information on evolving safety risks.

Process Effectiveness and Efficiency

The effectiveness of a safety process is determined by (1) the degree to which it has contributed to the reduction of identified hazard risks to acceptable levels and (2) the proportion of all system hazards that are identified. Safety engineers working with others achieve the successful mitigation of risks; the effectiveness of a safety process can be assessed from the number of actions taken across all processes that are triggered by safety process outputs. It is not possible to know if all system hazards have been found. However, indicators of the effectiveness of hazard assessments can be assessed from the distribution of hazard discoveries through the project lifecycle, and from comparisons with similar projects.

The safety performance of the product in operation is the ultimate measure of effectiveness of all processes working together to achieve system safety. Counting incidents (near misses), accidents and assessing the severities of damage sustained, should be undertaken. Lessons learnt can inform system upgrades, maintenance actions, operations design and the development of future projects.

An effective safety process reduces residual risks to acceptable levels, given the resources allocated and other constraints (e.g. other system performance requirements). Efficient mitigation strategies are developed in collaboration with other technical processes (design etc). A safety process is efficient if it consumes minimum resources in achieving the required safety assessments and assurance tasks.

Assurance – Safety

Assurance - Safety	Safety Argument

Safety assurance activity provides the visibility and integrated assessment required by customer organizations and regulatory authorities to enable system products to be certified for use. Assurance places emphasis on the provision of a safety case and supporting evidence to establish that the system is acceptably safe for operation.

Safety Argument: A measure is proposed that tracks the degree of completion and confidence in the system safety argument and supporting data, as submitted for certification. Progress against a planned argument structure is one possibility. Confidence assessment, or residual risk assessment would provide a more direct measure of technical progress; it is not clear how best to do this at present.

The Security Measurement White Paper [7] proposes using selected fault paths as a means of aggregating risk over a system. The selection decisions are taken by identified roles; the selection judgments can be challenged and reviewed as understanding increases or following change. A safety argument can be viewed as a type of assurance argument which integrates risk mitigation evidence for specified types of failure risks. In these terms, assurance is indicated by the residual risks as perceived by users.

Figure 10 summarizes the concepts proposed for the safety domain: these concepts are intended to support dialog between safety specialists and other stakeholders. The chart amounts to a measurable concept model to support the translation of information needs to measurable entities.

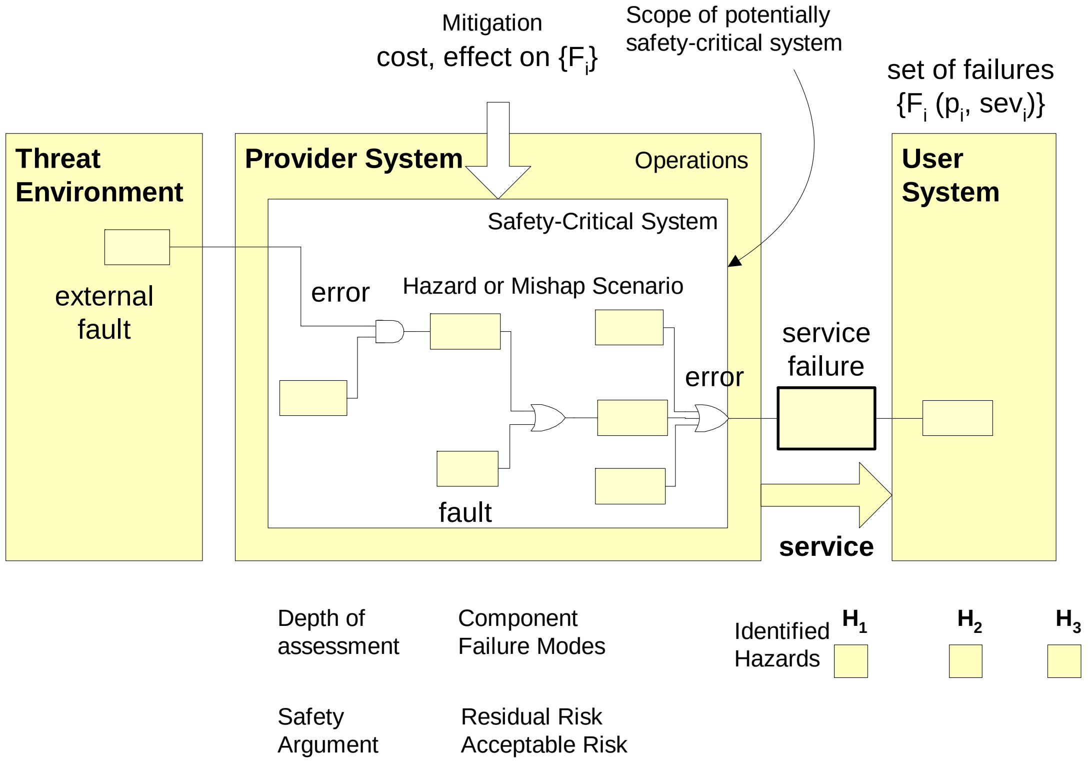


Figure 10 Safety concepts used as a basis for safety measurement

The next Section identifies typical measurable entities at practical level, independently of information needs concerns.

3.5 Measurable Entities

The measurable entities of a safety process (like other processes) fall into the following categories: *inputs*; *outputs*; *activities*; *interactions with concurrent processes*; *resources deployed*; and *outcomes* (Figure 11). Safety techniques, terminology and work products vary across industrial sectors and types of technology, although fundamental principles are common.

This White Paper develops initial PSM guidance material by identifying representative work products from applicable standards. The following have been considered:

1. Applicable system safety process model (MIL-STD-882D);
2. Civil airborne electronic equipment safety recommendations (ARP 4754/4761);
3. +SAFE extensions to CMMI [5];
4. Safety and security extensions under development for the CMMI models [4];
5. A reference process model for software safety (the ‘Weaver Team’ software safety process model developed in the US naval community [14]).

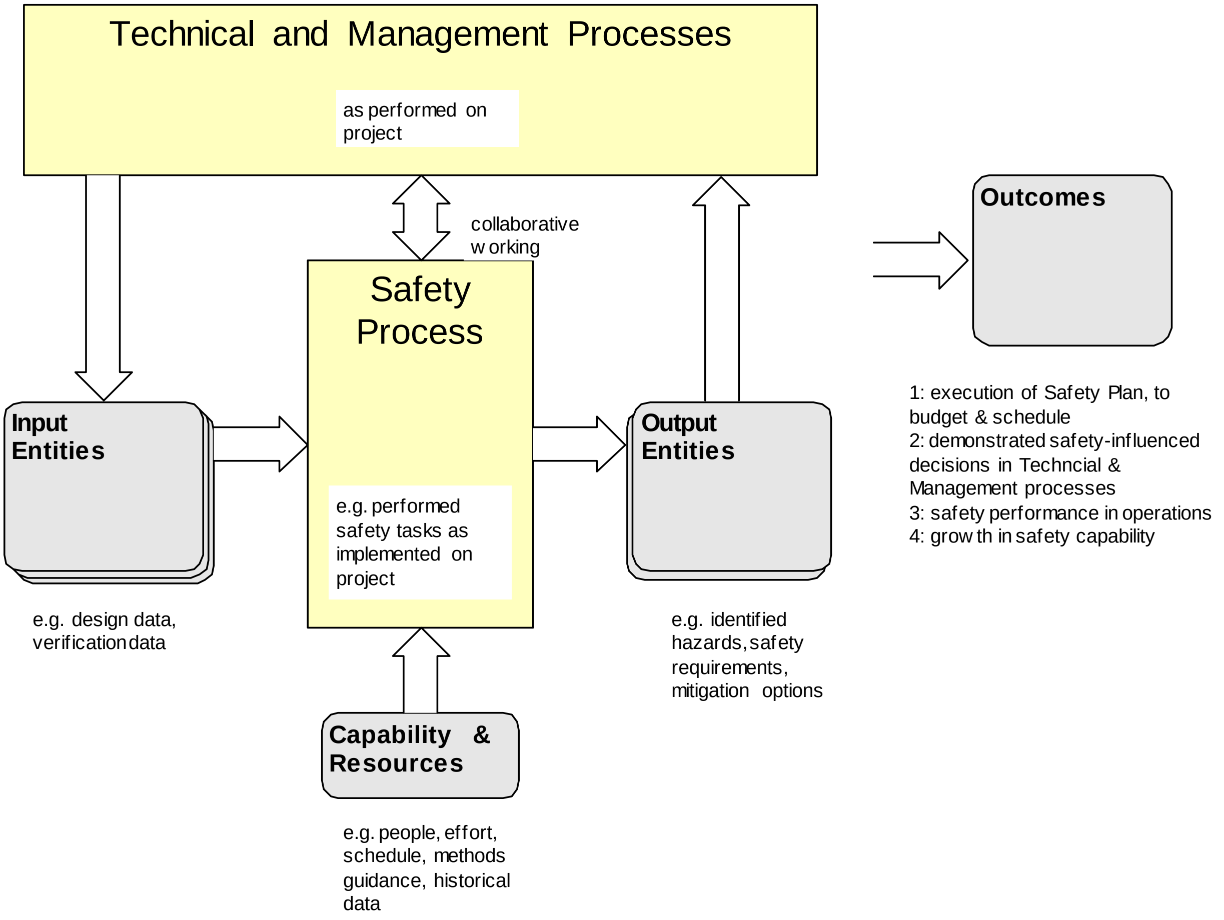

Technical and Management Processes
as performed on project
collaborative working
Safety Process
e.g. performed safety tasks as implemented on project
Input Entities
e.g. design data, verificationdata
Output Entities
e.g. identified hazards, safety requirements, mitigation options
Capability & Resources
e.g. people, effort, schedule, methods guidance, historical data
Outcomes
1: execution of Safety Plan, to budget & schedule
2: demonstrated safety-influenced decisions in Techncial & Management processes
3: safety performance in operations
4: grow th in safety capability

Figure 11 Safety process artifacts: inputs, outputs, resources

This is viewed as constructing a Measurable Entities Model; Table 7 of Appendix 4 summarizes the measurable entities identified in this preliminary study. Identified entities and attributes are then used to define Measurement Constructs; these are described in Measurement Information Specifications. Example draft specifications are included in Appendix 5.

3.5.1 MIL-STD-882D

The general requirements of this standard imply several measurable entities. The most important is a *Hazard Tracking System* or *Log*, in which identified hazards, their status, closure actions and residual mishap risks are recorded. This is required to be maintained throughout the system life cycle.

Measurable attributes include the number of hazards in different status conditions (e.g. open/awaiting risk analysis, open/ awaiting mitigation strategy, open/mitigation in progress, mitigation verified, closed), and the more detailed status of mitigation actions (work progress against plan).

The central task of assessing mishap risks (in terms of severity and likelihood) calls on the specialty knowledge and skills of safety engineers, designers and others. Application of PSM should support this work and the communication of risk information to risk acceptance and management structures.

Assessment of mitigation alternatives may also require management participation; mitigation costs, risk reduction, etc are attributes managers may be concerned with. Mitigations will vary across technologies and product types.

The standard also requires documentation of the system safety approach; a Safety Plan is recommended, specifying milestones, a system safety organization, and so on. Generally, aspects of work progress will be measurable against such plans. The safety analyses undertaken, their scope and outputs provide possible measures. Different assessment techniques have different outputs and attributes. Most output actions or recommendations that may be tracked. These techniques form the core of the safety specialist’s tools and underpin the safety-related decision-making at all management levels. It is proposed that PSM can provide a platform for negotiation between specialists and managers, in which key indicators can be identified.

It is also required that programs make use of lessons learnt and experience of previous projects. The experience and proficiencies of project staff (and those making risk acceptance decisions) are measurable, in terms of years worked on similar projects, courses taken, etc. If a lessons-learnt database is used, then measures of rate of growth and referencing may be considered.

The standard stipulates a system safety design order of precedence for mitigating identified hazards; a possible measure of the effect of a safety process is to track the ‘citations’ of such mitigation choices.

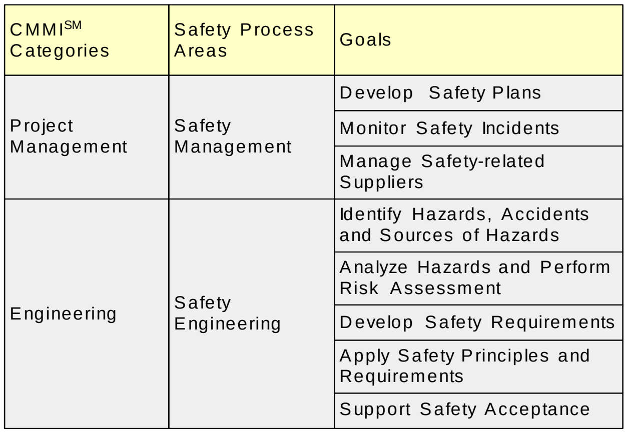
3.5.2 ARP 4754/4761

The ARP recommendations are based on a V-Process model (Figure 6) that distinguishes between Preliminary System Safety Assessment (before manufacture & integration) and System Safety Assessment (following manufacture and during integration to delivery). Both are informed by Functional Hazard Assessments at aircraft and major aircraft system levels, and by other supporting analyses. Similar to the System Safety Handbook, ARP 4761 provides guidance on the application of several assessment techniques. A prominent technique in the ARPs is Fault Tree Analysis, used to support the apportioning of a safety risk budget down through the system structure. These techniques involve tabular results, providing various measurable attributes. Such measures would aggregate to (1) underpin the mishap risk assessments recorded in the Hazard Tracking System and (2) the development and tracing of safety requirements.

The main ARP approach is top-down; in practice, potential failure modes at component and unit levels have to be identified and assessed before safety requirements are developed from the total-system hazards. If a project were using a failure mode tracking system, this would also provide measurable attributes (number and status of identified failure modes, mitigation action status).

3.5.3 +SAFE Extensions to CMMI

A further source of advice on measurable entities is the ongoing work to extend the CMMI framework to the safety domain. The concept of a *work product* is central to CMMI; an organizational process (at Process Capability Level 1) is expected to have identified input and output work products. The information components of CMMI include lists of typical work products. The +SAFE report identifies many typical work products associated with the safety management and safety engineering process areas.



CMMI^{SM} Categories	Safety Process Areas	Goals
Project Management	Safety Management	Develop Safety Plans
		Monitor Safety Incidents
		Manage Safety-related Suppliers
Engineering	Safety Engineering	Identify Hazards, Accidents and Sources of Hazards
		Analyze Hazards and Perform Risk Assessment
		Develop Safety Requirements
		Apply Safety Principles and Requirements
		Support Safety Acceptance

Figure 12 +SAFE extensions to CMMI, Australian Dept of Defence

The following entities are selected from the +SAFE Report:

Selected Measurable Entities from +SAFE Report
Independent Safety Assessment Plan and Report
Safety Requirements Specification
System Requirements Specification (with safety annotations)
Project Organization Chart, showing safety responsibilities
Skills and Experience Matrix
Training Plan
Minutes of meetings of the Safety Management Group
High-Level Safety Argument
Supporting Evidence
Accident List
Incident Reports
Supplier Agreements (with safety requirements)
Supplier Management Plan
Subcontract Management Plan
Review Minutes
Audit Records
Technical Data Package that addresses safety

Table 3: Selection of measurable entities arising in the +SAFE model

Each of these entities presents measurable attributes, of the following types:

- Counts of instances (number of safety requirements, hazards, failure modes, mitigations, actions etc);
- (Qualitative) status of instances (open, closed, verified, validated etc); number in each category;
- Times of opening, closing, etc of actions; times of discovery of requirements, hazards, etc
- Numerical attributes of instances, e.g. mishap risk;
- Scopes of instances, i.e. number of system components associated with a mishap;

- Work progress against plans, in a conventional project management sense; resources consumed.

The +SAFE Report identifies inputs to the safety process, including:

- Product Specification
- Product Requirements Specification
- System Environment and Boundary Definition
- System Functional Model
- System Architecture Document
- System Design Document
- Project Lifecycle Model
- Safety Objectives
- Alternative Solutions
- Implemented Design
- Change Proposals, records

Assessments of the effectiveness and productivity of safety work should take into account the quality and timeliness of such input data.

3.5.4 Safety and Security Assurance Application Areas of CMMI [4]

Draft Application Areas have been proposed by a joint FAA/DoD study on safety and security assurance extensions to CMMI [4]. Sixteen Application Practices are proposed, each with associated typical work products. The practice descriptions provide a valuable integration of current standards and practices, applicable to safety and security. An initial appraisal indicates that the approach proposed in this White Paper is broadly consistent with the CMMI extension proposals. It would be useful to harmonize terminology and the Measurable Entity Model proposed in this paper, with the Application Area terminology.

3.5.5 Example Software Safety Certification Process

Software engineering is a specialty technical discipline that presents particular challenges for safety assessment. The failure modes and risk mitigation options available are specialized to the software domain. MIL-STD-882D requires that hazards arising from software component failures should be incorporated and managed within the system safety hazard tracking process.

The US Navy has recently proposed a reference process for software safety certification, providing an example set of measurable entities in this domain. The following work products are involved in the process:

Output Work Products	**Measurable Attributes**
Perform Requirements Analysis	
Software Safety Requirements	Number of safety requirements
Criticality Matrix	Related to scope. Also hazard risk level. Acceptable risk.
Traceability Matrix	Scope

Preliminary Hazard Analysis	Number of hazards
Safety Requirements Criteria Analysis	Number of derived safety requirements. Target risk levels (acceptable risks)
Hazard Control Records	Hazard Status
Computer Program Change Requests	Number of safety-related changes. Change scope. Number of safety-sourced changes.
Design Analysis	
Criticality Matrix Update	
Traceability Matrix Update	
Safety Test Requirements	Safety scope. Test status.
Subsystem Hazard Analysis	Residual risk level, compared with target
Hazard Control Records	
Computer Program Change Requests	
Code Analysis	
Criticality Matrix Update	
Traceability Matrix Update	
Subsystem Hazard Analysis Report Update	Number of Subsystem hazards etc. Residual risk level. compared with target
System Hazard Analysis	
Hazard Control Records	Hazard status
Computer Program Change Requests	
Operations & Test Analysis	
Operating and Support Hazard Analysis	Number of operational hazards etc.
Safety Assessment Report	Safety scope
% Test Coverage	MCDC, Branch/ Decision coverage
Safety Test Verification Report	
Hazard Control Records	Residual risk level compared with target.
Computer Program Change Requests	

Table 4: Measurable entities associated with the Weaver Team process

Software developers have a range of risk reduction options available, including architectural design choices, defensive programming techniques and formal methods (to mathematically prove that programs implement specifications). These options present measurable attributes (e.g. progress in terms of proofs completed against those planned).

Software is usually subject to many changes during development; cyclic or evolutionary development processes are often adopted.   Safety measurement overlaps with more general software measurement at this level.

3.5.6 Summary Measurable Entity Model

Table 7 of Appendix 4 proposes a set of representative entities and measurable attributes, based on the review above. This is offered as a preliminary model. Improvement and specialization to particular products and technologies are expected. Harmonization with the CMMI Application Area for Safety and Security Assurance would be useful for organizations using CMMI as a model of current practice.

Table 7 is rather complicated: it is worth remembering that its purpose is to provide a basis for the specification of measurement constructs. Only a selection of attributes will feature in a particular measurement construct.

3.6 Additions to the PSM Materials

Table 6 of Appendix 3 summarizes a set of proposed additions to the PSM I-C-M Table, suitable for the safety domain.

- *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* could 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*
  Hazards
  Hazard Risk
  Hazard Scenario Risk
  Failure Modes
  Safety Assessments & Assumptions
  Mitigation Status
  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 report.

Draft Measurement Information Specifications are provided in Appendix 5.

4 PSM Safety Measurement: Draft Guidelines

4.1 Technical/ Specialty

Local practices will determine the safety activities, work products and interactions with product development and other processes. Local standards and guidance materials will include those measurements used within the safety specialty. The Safety and Security Assurance Application Area (extension to CMMI) provides a reference for practices and typical work products.

4.2 Project Management

Early safety work on a project will determine the applicable regulatory and other standards that are to be followed. Most safety standards require the drawing up of a Safety Plan. It is recommended that safety measurements be considered as part of this planning. Early negotiation with regulatory authorities should also negotiate agreed measures.

Measures developed for safety may then be integrated with systems engineering technical measures, as developed as part of the systems engineering planning for the project.

Safety measures may be considered in a Measurement Workshop, if the project chooses to develop an integrated approach to measurement design, by this means.

Safety measurement will involve the tracking of hazard risks. Each hazard that is assessed to present an unacceptable risk will generate additional mitigation-related work, which is also subject to measurement. Although most projects start with a Generic Hazard List (based on similar past projects), new hazards may be identified as work progresses. The safety measurement approach should accommodate such potential growth in measured entities.

Effort deployed on the safety process has to be synchronized appropriately with work on other processes. For example, resources can be wasted if detailed safety assessment is carried out on a design, which subsequently changes. Measures may be required to achieve appropriate synchronization between processes.

4.3 Organizational Management

Many organizations are using the process maturity models as an approach to achieving improved capability. While associating particular measurement sets with maturity levels should not be taken as prescriptive, we might expect to see different kinds of measurement being introduced as more attention is directed towards the institutionalization of safety practices. For example:

Level 1-2 Organizations would probably emphasize measures that indicate basic safety capability and work progress against a Safety Plan on a project, for example:

- Start up measures: Safety Plan (draft, review and issue), appointment of staff, responsibility allocation; allocation of budgets, tool support (e.g. certified);
- Basic recording measures: Safety Requirements, mishaps and hazards, Hazard Log/ Tracking System;
- Conformance of performed process with Safety Plan.

*Level 3 Organization*s would probably introduce measures that indicate progress of safety work in a managed safety process on a project, at the level of identified safety-related risks, for example:

- the maturation of hazards (risk reduction to acceptable levels);
- the maturation of safety models/ safety case (completeness of and confidence in 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 Organizations would probably introduce measures to support continuous improvement in safety processes, for example:

- performance of the safety process; use of resources, productivity;
- effectiveness of the safety process;
- effectiveness of the integrated development process (including safety) in achieving operational safety performance;
- safety capability benchmarking/ audit against standard models and other organizations.

These are indicative only; selected measures will depend on local objectives and conditions.

4.4 Enterprise Management

Safety is a risk management process; measures of the productivity and effectiveness of the safety process should recognize the benefits of risk reduction. The case for investment in early risk reduction on projects can include statistical (expected) outcomes from many projects.

5 Conclusion

PSM can provide a platform for improving communication between managers, safety specialists and other technical specialties so that better safety-related decisions are made. PSM has been applied to the safety domains; additional measures have been proposed to support managers and others who need to estimate, monitor progress and improve safety processes. Measuring safety is not straightforward, partly because these system properties are achieved as a result of many different technical and management specialties working together. Furthermore, safety engineering is a form of risk management and is concerned mostly with potential future events. Measurement must support the treatment of subjective judgment and uncertainty. Safety risk is assessed by technical specialist processes but is of importance at all levels of developer and operating organizations. Clear assessments of risks, including uncertainties, together with cost estimates of mitigation options are the core information needs of project managers and others. The effectiveness and efficiency of specialist processes are the concerns of organizational managers.

Proposals made in the paper have to be tested through field trials. A project interested in participating would apply the PSM measurement process to an area of information need related to safety management. The measurable concepts proposed here would be tailored to the local project context. Measurement constructs would be developed and data collected to test the effectiveness of the approach and the measurement guidance material. The approach will stand or fall on the basis of the benefits provided to decision makers involved in safety-related projects.

The PSM Technical Working Group on Safety & Security invites comments on this White Paper. Organizations and projects that are interested in field trials of safety measurements are also invited to contact the PSM Project Office.

Information on PSM and discussion of field trials (US)	Comments on this White Paper and discussion of field trials (UK)
Cheryl Jones, AMSTA-AR-QAT Bldg 62, Picatinny Arsenal, NJ 07806-5000. Tel: 973-724-2644 Fax: 973-724-2382 cljones@pica.army.mil	Dr. John Murdoch, Computer Science Department, University of York, YORK YO10 5DD UK. Tel: 44 1904 43 2749 Fax: 44 1904 43 3431 jm48@york.ac.uk

6 References

1. McGarry, J., *et al.*, *Practical Software Measurement; objective information for decision makers*. 2001, Boston: Addison-Wesley. 277.
2. ISO/IEC, **ISO/IEC 15939:2002(E),** *ISO/IEC 15939:2002(E) International Standard Software engineering - Software measurement process*, 2002-07-15, ISO/IEC.
3. Bofinger, M., *et al. Experience with Extending CMMI for Safety Related Applications*. in 12th International Symposium of the International Council on Systems Engineering (INCOSE'02). 28th July - 1st August 2002 . Las Vegas, Nevada: INCOSE. 2002.
4. Ibrahim, L., *et al.*, *Safety and Security Extensions for Integrated Capability Maturity Models*, September 2004, US FAA & DoD.
5. Bofinger, M., **CA38809-364,** *+SAFE - A Safety Extension to CMMI*, 19th December 2001, Australian DoD.
6. Roedler, G.J., *Technical Measurement*, July 2003, PSM.
7. Murdoch, J., **PSM White Paper v3.0,** *Security Measurement*, 13th January 2006, University of York.
8. Avizienis, A., *et al.*, *Basic concepts and taxonomy of dependable and secure computing*. IEEE Trans. Dependable and Secure Computing, 2004. **1**(1): p. 11-33.
9. DoD, *MIL-STD- 882D Standard Practice for System Safety*, 10th February 2000, Department of Defense.
10. SSS, *System Safety Engineering Handbook*. 2nd ed. 1998: System Safety Society.

11. MoD, *Def Stand 00-56,58,31*,

12. ARP-4754, *Certification Considerations for highly integrated or complex aircraft systems*, . 1994, Society of Automotive Engineers Inc

13. ARP-4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, . 1995, SAE Committee S-18

14. Weaving-Team, *Software Safety Certification Weaver Group Integration*, 23rd May 2003,

15. MoD, *Interim Defence Standard 00-55 Requirements for the Procurement of Safety-Critical Software in Defence Equipment*, UK Ministry of Defence.

16. CAIB, *CAIB Report Volume 1*, August 2003, Columbia Accident Investigation Board.

17. ISO/IEC, *ISO/IEC 15026 Assurance.* 2005.

18. Leveson, N.G., *A systems-theoretic approach to safety in software-intensive systems.* IEEE Trans. Dependable and Secure Computing, 2004. **1**(1): p. 66-86.

19. Ahern, D.M., A. Clouse, and R. Turner, *CMMI Distilled: a practical introduction to integrated process improvement*. SEI Series in Software Engineering. 2001: Addison-Wesley. 306.

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

21. Clark, G., *et al. Measurement of System Safety Processes*. in International Symposium on Systems Engineering. Washington. 2003.

22. Kuettner, H.D. and M.A. Emery. *Practical Application of Software Safety Metrics*. in 21st International System Safety Conference. 2003.

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

24. SAE, **SAE J-1739,** *Potential FMEA Reference Manual*, SAE.

Appendix 1 Glossary

Acceptance	Agreement to receive and use, that contract terms are met, to take on risk
Assurance	The basis on which trust is placed in a system or service. The provision of the basis, usually in the form of evidence and analysis
Assumption	Statement, principle and/or premise offered without proof. (ARP
Certification	The legal recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or other documents as required by national laws and procedures. (ARP)
Dependability	The ability to deliver a service that can justifiably be trusted. (calls for a justification of trust). The ability to avoid service failures that are more frequent and more severe than is acceptable (implies criteria for deciding whether a service is dependable). Dependability properties comprise availability, reliability, safety, integrity and maintainability.
Dependence	Of a system on a service; the reliance of a system's operations on a provided service.
Error	Deviation in actual system state from correct or intended state. Errors are caused by faults and give rise to service failures.
Functional hazard assessment (FHA)	A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity. (ARP)
Failure	In a provided service; the service is not as intended, causing a fault in the user system.
Failure mode (FM)	The way in which the failure of an item occurs. (ARP)
Fault	The adjudged or hypothesized cause of an error. A fault may or may not have safety implications. Also called a defect, flaw.
Hazard	Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. (MIL-STD-882) A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof. (ARP)

Mishap
An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (MIL-STD-882)

Mishap risk
An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence. (MIL-STD-882)

Mitigation
Reduction in risk achieved by some action. Security risks during development can be reduced by better requirements, design, improved manufacture and test and countermeasures. During operation, security risks can be reduced by improved policies, better enactment and countermeasures.

Mitigation
Means by which a mishap risk is reduced to an acceptable level.

Preliminary system safety assessment (PSSA)
A systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items. (ARP)

Residual mishap risk
The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence. (MIL-STD-882)

Return on Safety Investment
Benefit achieved, usually expressed in financial terms, arising from expenditure on safety. (ROSI)

Risk
The frequency (probability) of occurrence and the associated level of hazard. (ARP)

Safety
The ability to deliver a service that can justifiably be trusted not to cause harm (calls for a justification of trust).
The ability to avoid harmful service failures that are more frequent and more severe than is acceptable (implies criteria for deciding whether a service is dependable).

System
A general term indicating an entity that provides some useful functionality or service and that is developed and operated. The provided service may require the system to hold assets that are to be protected from attack.
A specific IT installation, with a particular purpose and operational environment. – ISO/IEC 15408.

System safety management
All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the development, test, acquisition, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities. (MIL-STD-882)

System safety assessment (SSA)
A systematic, comprehensive evaluation of the implemented system to show that the relevant safety requirements are met. (ARP)

Appendix 2 Applying PSM to the Safety Domain

General Approach

PSM and ISO/IEC 15939 are based on a general Measurement Process Model comprising two 'core' activities, *Plan Measurement* and *Perform Measurement*, and two 'supporting' activities; *Evaluate Measurement*, and *Establish and Sustain Commitment*. The PSM process serves the *Technical and Management Processes*; these are the sources of information needs and the users of the measurement data provided.

The development of PSM and ISO/IEC 15939 can be traced back to the *Goal Question Metric* approach of Basili and co-workers [20]. They are based on a Measurement Information Model (Figure 13) that establishes relationships between the information needs of the user processes and the measurable entities and attributes of the measured processes. Base Measures are assigned values by applying a Measurement Method to an Attribute of an Entity. A Derived Measure is assigned a value by applying a Measurement Function to two or more values of Base Measures. An Indicator is assigned a value by applying an Analysis Model to Base and/or Derived Measures. An Information Product is the outcome of the measurement process that satisfies the Information Needs, developed from an Interpretation of the Indicator. The Interpretation explains the quantitative information of the Indicator in the language of the information user, relating it to the Information Needs. The overall mapping of an Information Need to relevant Entities and Attributes is called a Measurable Concept.

PSM goes further than ISO/IEC 15939 by providing more detailed guidance on developing measures. It provides additional guidance on:

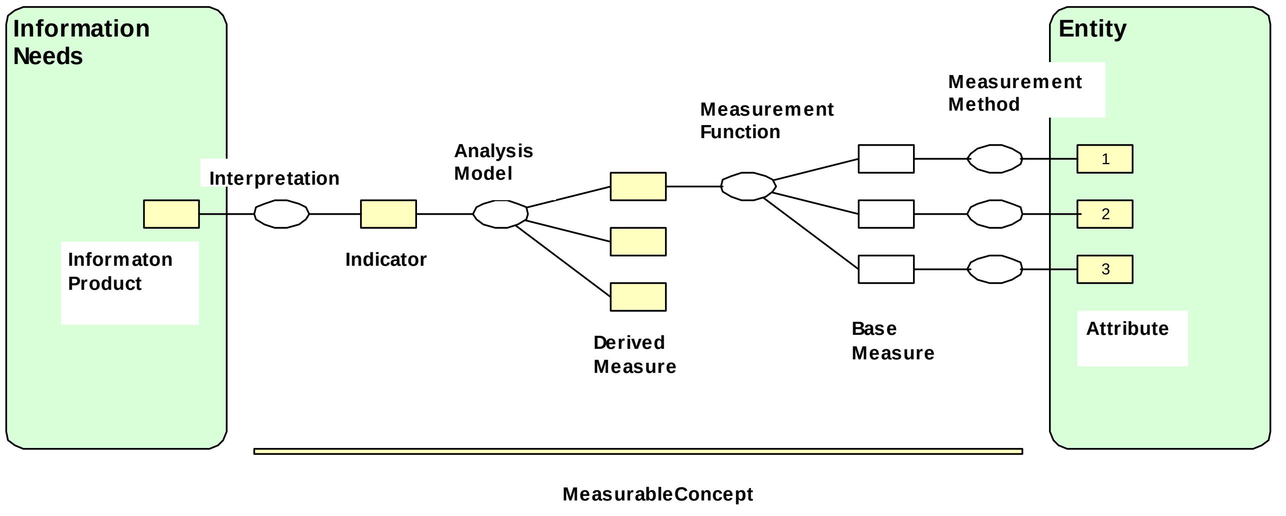


Figure 13 PSM and ISO/IEC 15939 Measurement Information Model

- the identification of *information needs*;
- the interpretation of an information need as being within an *information category*;
- the identification of *measurable concepts* associated with information categories;
- the identification of *prospective measures* associated with measurable concepts.

The mapping between Information Categories, Measurable Concepts and Prospective Measures is recorded in the I-C-M Table.

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 analyzer, or as a particular field in a project database.

PSM provides further guidance by means of Measurement Information Specifications that comprise reference specifications for measurements, measurement attributes, data collection procedures and data analysis procedures. The fields of the template provide the information implied by the Measurement Information Model of Figure 13

If safety additions were already available in PSM, a user would follow the recommended measurement process; identify information needs, select prospective measures and then map these to the measurable artifacts available. 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). 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.

PSM guidance is based on two kinds of generalization: (1) typical information needs, as expressed through the information categories and (2) typical measurable and relevant entities,

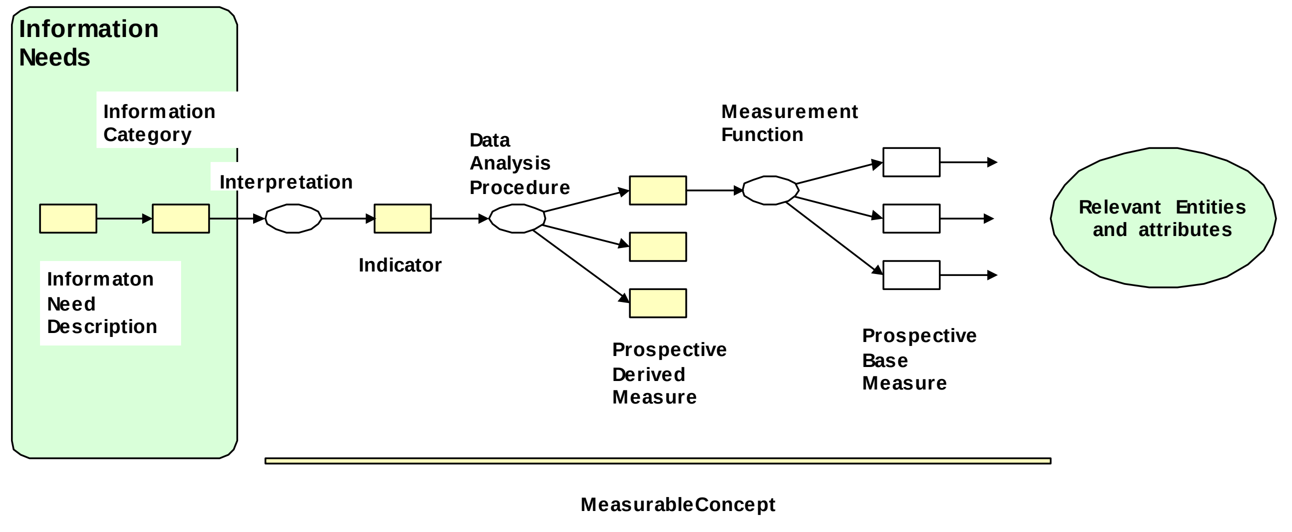


Figure 14 Top-down development of prospective easures from information needs

and their attributes, as expressed in the Measurement Information Specifications. Developing guidance material involves parallel assessments at the information need and measurable entity levels:

Top-down (Figure 14):

1. identify roles involved in safety work and its management; who are the sources of information needs?
2. consider their information needs, and its categorization; what are the information needs of the identified roles? Does the current PSM I-C-M table cover these, or would we recommend additions or modifications? Are there measurement guidance needs arising in safety work, not met by existing PSM guidance materials? What additions are needed?
3. identify measurable concepts that are candidates for meeting the information needs; what are the measurable concepts that link available base measures with information needs? What analysis models are implied?
4. What measures are currently used i.e. are of proven benefit? Are there measurement and information needs not met by today's practices, but which can be envisaged as feasible?
5. identify relevant prospective measures;
6. propose augmentations to the PSM I-C-M Table and modifications to existing Measurement Specification Tables where appropriate. Also outline Measurement

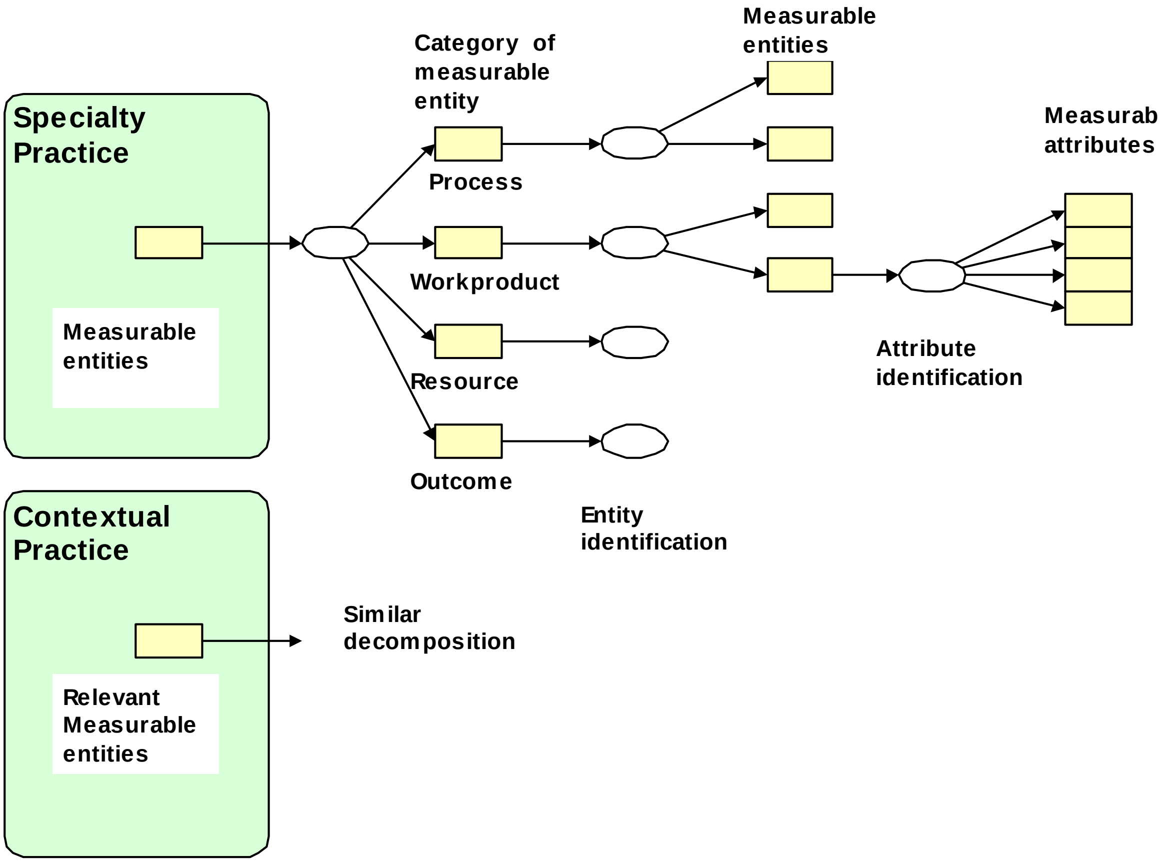


Figure 15 Bottom-up development of measurable entities and their attributes

Specification Tables for new measures proposed for safety measurement.

7. Is it appropriate to combine the safety and security domains into a single set of guidance materials? How should such guidance be expressed?

Bottom-up (Figure 15):

1. identify typical activities, work products and their measurable attributes, based on industry practice, standards and +SAFE/ CMMI safety extensions; What are the available base measures in safety work? Are these already identified in the PSM guidance, or are domain-specific measures needed?
2. develop a set of *representative* entities and attributes; develop as a Measurable Entity Model;
3. identify representative data collection and analysis procedures;
4. complete *sample data collection* and *analysis* sections of the newly proposed Measurement Specification Tables.

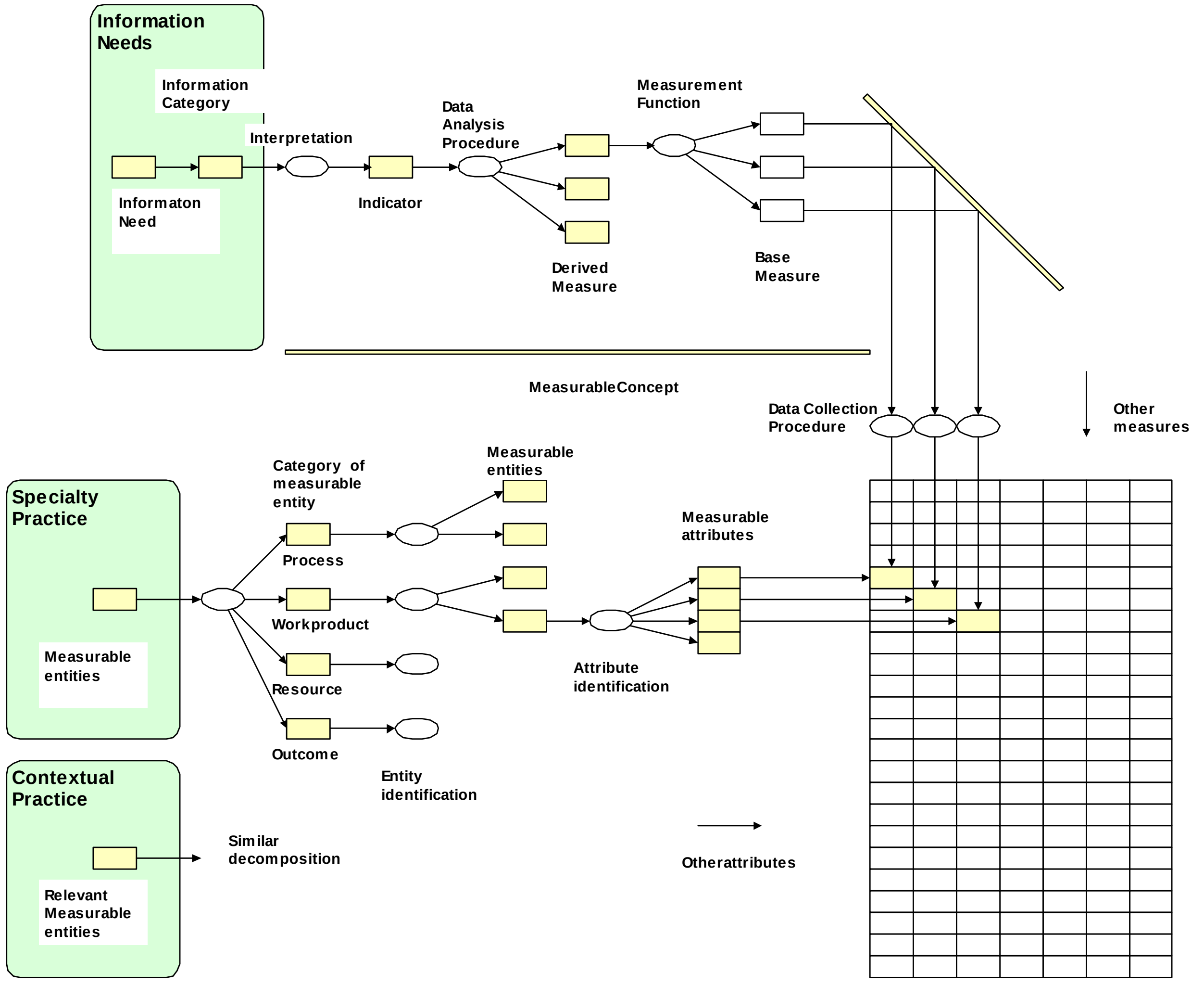


Figure 16 Mapping from prospective measures to measurable entities and attributes

The top-down approach ensures that measurable concepts are developed that serve information needs (assuming sufficient stability in the needs). However, it has the disadvantage of not considering the feasibility of base measures, e.g. whether suitable measurable entities are actually present in an area of work. Top-down thinking emphasizes the need for a limited number of key indicators that give the information needed by the users.

The bottom-up approach ensures that base measures are feasible and driven by the actual entities and attributes present. However, it has the disadvantage of not considering the purpose of measurements. Bottom-up thinking tends to generate large numbers of measurable attributes, which can seem over-complex for information users.

Measurable entities are categorized into four types: *process*, *work product*, *resource* and *outcome*. Examples of these are given in the following Sections. Relevant measurable entities might be identified that are associated with other (non-safety) processes.

Proposed measurable concepts and completed Measurement Information Specifications will require establishing mappings from the prospective measures to the identified set of measurable entities and attributes (Figure 16).

User Model

Taking the perspective of a system developer organization, four broad constituencies of 'measurement users' can be identified, with areas of concern centered on different aspects of system development (Table 5). Similar roles exist in acquirer and supplier organizations.
The enterprise level is mainly concerned with the business case, or the financial justifications for investments and engagement in projects. Many measurements at the other levels will map to the enterprise level, since this is where strategy is developed and overall organizational 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 productivity of safety work in terms of both performance of the product throughout its operational life and in terms of achieving regulatory clearance.

	Typical Concerns
Enterprise Management	Productivity, cost, strategy, litigation, commercial viability and growth. Effectiveness of safety management systems
Organizational Management	People, learning, effectiveness, efficiency, process improvement, integration of standardized activity, portability, institutionalization
Project Management	Delivery to plan, schedule, cost, meeting requirements, product performance, product maturity (or design stability) Monitoring, team volatility
Technical/ Specialty	Professional practice (e.g. safety engineering), learning, 'actual' project work, effectiveness of techniques

Table 5: Various roles with different, but related, needs for measurement

Inevitable tensions exist between the constituencies of Table 5. 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 on resource allocation and progress towards particular deliverables. However assessment of technical progress often depends on the judgment of specialty 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. Managers require few but powerful measures. Specialists often work with many detailed measures.

Such tensions are present for the safety specialty. It is recognized 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 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 have valid concerns and responsibilities to discharge. Providing managers with greater visibility of the effectiveness of safety work and the means to monitor it seems reasonable. Enabling better management decision-making about safety is needed. With recognized 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 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.

Measurable Entity Model

The original PSM guidelines were developed for software projects. The common properties of software (lines of code, requirements, functions) naturally appear in the I-C-M Table and measurement information specifications. There are two challenges in applying PSM to other domains: (1) establishing the key measurable concepts in the domain that are relevant for management and other processes and (2) proposing a reference model for measurable entities at practical working level. It is proposed to make explicit the assumptions about what measurable entities are available by recording a *Measurable Entity Model*. Entities and attributes recorded in the model would match those appearing the specification tables. It is proposed that this will make it easier for users to map the PSM guidance material to their particular process situation, and to map terminology where local practice differs from that assumed by PSM.

It is not the purpose of such a model to provide a complete description of measured processes; this is covered in standards and other materials. The entity model would be limited to describing the measurable entities that are assumed to be available in the measurement information specifications.

The MEM is constructed from industry practice. In the safety domain, safety standards are the obvious source of measurable entities, since developers are required to comply with them. The MEM can evolve as practical experience with safety measurement grows.

Learning and Improvement

Organizations seek to improve performance at all the levels of Table 5:

- *Enterprise management:* responsiveness to market, competitiveness, productivity, investment;
- *Organizational management*: integrated capabilities, institutionalization, human resources;
- *Project management*: cost/ schedule management; risk/uncertainty management, performance, delivery;
- *Technical/ specialty*: effectiveness, efficiency, innovation, professional engineering practice.

Measurements are used in the management of current operations (viewed as projects here) and also of improvement. The PSM measurement process requires that measures be developed to serve information needs; PSM materials describe such needs as arising from risk management and financial management processes, the most important quantitative management processes at project level.

Initially, an organization may choose to implement a simple-as-possible measurement system, focused on the highest-priority information needs. Typically, such measures would serve essential tasks at technical, project and enterprise levels. Organizations that purposively manage learning and capability improvement would need additional information and develop measures to provide it. The process maturity models provide a framework for managing improvement at organizational level.

Appendix 3 Proposed safety additions to the PSM I-C-M Table v 5.0d

Information - Concept - Measure Mapping		
Information Category	**Measurable Concept**	**Prospective Measure**
Schedule and Progress	Milestone Performance	Milestone Dates
	Critical Path Performance	Slack Time
	Work Unit Progress	Requirements Traced
		Requirements Tested
		Problem Reports Opened
		Problem Reports Closed
		Reviews Completed
		Change Requests Opened
		Change Requests Resolved
		Units Designed
		Units Coded
		Units Integrated
		Test Cases Attempted
		Test Cases Passed
		Action Items Opened
		Action Items Completed
	Incremental Capability	Components Integrated
		Functionality Integrated
Resources and Cost	Personnel Effort	Staff Level
		Development Effort
		Experience Level
		Staff Turnover
	Financial Performance	BCWS, BCWP, ACWP
		Budget
		Cost
	Environment and Support Resources	Quantity Needed
		Quantity Available
		Time Available
		Time Used
Product Size and Stability	Physical Size and Stability	Database Size
		Components
		Interfaces
		Lines of Code
	Functional Size and Stability	Requirements
		Functional Changes
		Function Points

… and Scope	Scope - Safety	Safety Requirements
		Safety-Critical Functions
		Safety-Critical Components
		Safety-Critical Interfaces
		Safety-Critical Modes
		Safety Zones
		Safety Change Workload
Product Quality	Functional Correctness	Defects
		Age of Defects
		Technical Performance Level
	Supportability-Maintainability	Time to Restore
		Cyclomatic Complexity
	Efficiency	Utilization
		Throughput
		Response Time
	Portability	Standards Compliance
	Usability	Operator Errors
	Dependability - Reliability	Mean Time to Failure
	Dependability - Safety	Hazards
		Hazard Risk
		Hazard Scenario Risk
		Failure Modes
		Safety Assessments & Assumptions
		Mitigation Status
		Safety Incidents & Accidents
	Assurance - Safety	Safety Argument
Process Performance	Process Compliance	Reference Maturity Rating
		Process Audit Findings
	Process Efficiency	Productivity
		Cycle Time
	Process Effectiveness	Defects Contained
		Defects Escaping
		Rework Effort
		Rework Components
Technology Effectiveness	Technology Suitability	Requirements Coverage
	Technology Volatility	Baseline Changes
Customer Satisfaction	Customer Feedback	Satisfaction Ratings
		Award Fee
	Customer Support	Requests for Support
		Support Time

Table 6: Proposed additions to the PSM I-C-M Table, covering safety measurement needs

Appendix 4 Measurable Entities Model for Safety Processes

Phase	Measurable Entity	Attributes	Notes
Context: Capability	Reference Process Model	Strengths and Weaknesses Practice Characterizations Goal Ratings PA ratings Capability Profiles	CMMI measures relating to the institutionalization of processes.
Start Up	Safety Plan	Safety Process Definition Tasks Schedule Resources Work Products	Planning and deployment of safety process assets on a particular project. The measurement of deployed effort in a safety-critical software application has been reported by [21]
		Roles, responsibilities	Including independent safety checks
		Staff Competencies Skills and Experience Matrix	
		Reporting Arrangements	
		Contractual Agreements	
		Dispute Resolution Provision	
Product Development; Pre-manufacture	Safety Requirements Log or database	Requirement Count Requirement Scope Requirement Source Status	Summary record of safety requirements, including customer sourced, derived requirements as developed by the safety process and safety requirements placed on suppliers. An example of measurement using software safety requirements has been reported by [22].
	Safety Scope Log	Product Components Product Functions Product Modes Mission Phases Process Resources	Possibly at different SIL/DAL levels. This is important because it acknowledges the open, changing nature of safety engineering. This is a speculative proposal of this paper.
	Hazard Log or Tracking System	Hazard Count Hazard Status Hazard Scope Hazard Risk	Would be repeated for each organization involved. Risk is usually expressed as the product of probability and consequence. The practical application of such a measure has been reported by [23], applied to the assessment of safety program effectiveness.
	Failure Mode Log or Tracking System	Failure Mode Count Failure Mode Status Failure Mode Scope	More applicable to hardware components: complements the top-down approach of hazard assessment. Includes record of single point failures. Includes failure modes of supplied components, declared by suppliers. 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 [24] provides an example process.

	Common Mode Failure Log	Count Status Scope	Important as an adjunct to mitigations that involve redundancy and alternative functions/ components/ paths.
	Safety Assumption Log	Assumption Count Assumption Status Assumption Scope	Supports concurrent development by independent teams. Records assumptions made to enable safety tasks to be conducted.
	Safety Action/ Mitigation Log	Action Count Action Status	Summary record of all actions generated by the safety process, including mitigations.
Post Manufacture: assembly, integration and test	Verification Test Log	Verification Count Verification Status Action Status Action Scope	Summary records of the tests and other data that demonstrate safety requirements have been met.
	Acceptance Test Log	Validation Count Validation Status Action Status Action Scope	Summary record of the validation tests and other data that are agreed as acceptance criteria across customer/supplier interfaces.
Operations	Accident Log	Count Type/ severity Action Status Accident Scope	
	Incident Log	Count Type/ severity Action Status Incident Scope	
	Maintenance Action Log	Count Type Action Status Maintenance Scope	
Safety Assurance	Safety Case	% completion against planned argument structure	Summary argument that demonstrates compliance with regulatory requirements and structures supporting safety evidence.
System Disposal			Not developed here.

Table 7: Measurable entities for the safety domain

Appendix 5 Draft Measurement Information Specifications

Draft Measurement Information Specifications are included for selected measures. Information at the level of data collection is not included at this draft stage.

Information Need Description	
Information Need	The scope of the safety assessment task on a project, in terms of the system functions currently assessed, their safety criticality and needs for further assessment.
Information Category	Product Size, Stability and Scope
Measurable Concept	
Measurable Concept	Scope - Safety
Entities and Attributes	
Relevant Entities	System Functions as specified in requirements and design documentation.
Attributes	Status of functions in terms of required safety assessment, as assessed by safety process: for example, (integrity level, not safety-related); also depth of safety assessment applied to date: for example, (integrity level, initial).
Base Measure Specification	
Base Measures	Safety-Critical Functions: safety status of all system or product functions, as developed in the system engineering and component technical processes.
Measurement Methods	Access appropriate documentation and records of safety process activity.
Type of Method	Objective in terms of counting functions in each category; may involve subjective judgment of the level of assessment required and achieved.
Scale	Nominal for each function; integer counts of numbers of functions.
Type of Scale	Categories, integer values
Unit of Measurement	
Derived Measure Specification	
Derived Measure	Aggregated status from all identified functions.
Measurement Function	Percentages of functions in each category. Progress of safety assessment in terms of depth of assessment applied compared with that required.
Indicator Specification	
Indicator Description and Sample	Graph of numbers of functions in each category plotted against project elapse time. Distinguish between required and achieved assessments.
Analysis Model	
Decision Criteria	Scope measures can be used to estimate required future safety work and to track progress against planned assessments.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	Supports a multi-pass approach in which all functions are assessed initially, with subsequent effort deployed in areas of high risk. Supports change in which new data can result in re-assessment and re-allocation of resources. Recorded scope of assessments performed can input to confidence measures about presence of unknown hazards etc.
Implementation Considerations	To be used in conjunction with other scope measures.

Information Need Description	
Information Need	The status of the safety assessment task on a project, in terms of the current recorded status of all identified hazards.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Dependability - Safety
Entities and Attributes	
Relevant Entities	Hazard Records in a Hazard Tracking System
Attributes	Hazard status: for example, (open: risk undetermined; open: risk greater than target; open: risk subject to trade; closed: risk acceptable)
Base Measure Specification	
Base Measures	Hazards: number of hazards in each recorded category
Measurement Methods	Access appropriate fields in Hazard Tracking System.
Type of Method	Objective in terms of counting hazards in each category; may involve subjective judgment at the level of hazard status assessment.
Scale	Nominal for each hazard; integer counts of numbers of hazards
Type of Scale	Categories, integer values
Unit of Measurement	
Derived Measure Specification	
Derived Measure	Aggregated status from all identified hazards.
Measurement Function	Percentage closed indicator of progress of safety work.
Indicator Specification	
Indicator Description and Sample	Graph of numbers of hazards in each category as functions of project elapse time.
Analysis Model	Reasons for non-closure of hazards may be fully justifiable, e.g. system requirements volatility, design volatility etc.
Decision Criteria	Hazard status objectives may be linked with life cycle phase gates, test and acceptance milestones and regulatory assurance objectives.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	The *Hazard Count* measure is based on the number status of identified system hazards. Undiscovered hazards are not considered by this measure.
Implementation Considerations	An effective and efficient safety process may not necessarily be indicated by early closure of hazards.

Information Need Description	
Information Need	Safety risk of a particular potential mishap; the probability of occurrence and the severity of the consequences.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Dependability - Safety
Entities and Attributes	
Relevant Entities	Hazard Tracking System
Attributes	Recorded risk associated with the mishap. May be associated with a particular scenario, that is, a sequence involving one or more root failures, failure effects, mitigation actions and conditions.
Base Measure Specification	
Base Measures	Hazard Scenario Risk: the risk associated with a particular mishap or hazard scenario
Measurement Methods	Risk is treated as a combination of probability of occurrence and severity of consequences. Probability is estimated on the basis of past data, analytical models and subjective judgment. Severity is estimated on the basis of past data, analytical modes and subjective judgment. Uncertainty in occurrence probability and severity can be treated quantitatively by replacing single figure values with probability distributions.
Type of Method	Quantitative, objective data is used where available, subjective judgment is usually required. These can be combined.
Scale	Probabilities are reals in the range (0..1.0). Severity units of measure depend on context, but are generally reals (e.g. expected value of 3.5 equivalent fatalities). Severity is expressed in dollar terms in order to trade-off with mitigation costs. Severity is also expressed in ordinal (rankings).
Type of Scale	Probability of occurrence is expressed as a real in the interval (0 … 1). Severity is expressed as a ratio (numeric data 0 … infinity) or as ordinal (rankings).
Unit of Measurement	Probability of occurrence is expressed as a probability per hour, per flight or per activation, etc. Severity is expressed in terms of equivalent fatalities, or as a qualitative category (catastrophic, etc). Severity may also be expressed in dollar terms, under specified assumptions.
Derived Measure Specification	
Derived Measure	Risk: combination of probability of occurrence and severity of consequences.
Measurement Function	Various approaches are possible: simple product of probability and severity (where these are treated as expected values); use of categories defined in probability-impact matrices published in applicable standards; treatment within an uncertainty management framework.
Indicator Specification	
Indicator Description and Sample	Risk can be expressed as a single number, or as cumulative probability distributions in probability of occurrence and severity. The mishap scenario to which the measures apply must also be clearly specified, including all scope and mitigation assumptions being made.
Analysis Model	The objective of the safety process, working in collaboration with other technical processes, is to achieve reduction in risk to a level acceptable to users and other stakeholders. The risk of a particular mishap may be traded-off with risks of other mishaps, and/or with other system performance parameters.
Decision Criteria	Risk levels determine whether mitigation actions are required. They are also used to determine System Integrity Levels. Risk levels also form the basis of safety assurance arguments and are used by regulators to make certification decisions.
Indicator Interpretation (sample chart)	
Additional Information	

Additional Analysis Guidance	Risk data as recorded in a Hazard Tracking System may be derived from extensive analysis and system modeling, performed by safety specialists. Assessing the risk of a scenario and identifying ways to reduce risk are central tasks of safety engineers. Care has to be exercised when assuming independence of events and conditions within scenarios.
Implementation Considerations	A risk measurement associated with a particular potential mishap may be: (1) a target value; (2) an expected value based on current understanding and knowledge; (3) a committed-to value, as expressed in an agreement with a customer or acquisition office.

Information Need Description	
Information Need	Safety risk of a particular hazard; the probability of occurrence and the severity of the consequences.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Dependability - Safety
Entities and Attributes	
Relevant Entities	Hazard Tracking System.
Attributes	Recorded risk associated with the hazard. A hazard is usually associated with more than one potential mishap scenario.
Base Measure Specification	
Base Measures	Hazard Risk: the risk associated with a particular hazard.
Measurement Methods	Based on the recorded risk of each hazard or mishap scenario associated with the hazard.
Type of Method	Quantitative, objective data is used where available, subjective judgment is usually required. These can be combined.
Scale	As for Hazard Scenario Risk measure.
Type of Scale	As for Hazard Scenario Risk measure.
Unit of Measurement	As for Hazard Scenario Risk measure.
Derived Measure Specification	
Derived Measure	Risk: combination of probability of occurrence and severity of consequences.
Measurement Function	Occurrence probabilities associated with the hazard scenarios are usually added. Severities associated with different scenarios may differ. Expected values and distributions of severity and occurrence probability for the hazard can be calculated.
Indicator Specification	
Indicator Description and Sample	As for Hazard Scenario Risk measure.
Analysis Model	The objective of the safety process, working in collaboration with other technical processes, is to achieve reduction in risk to a level acceptable to users and other stakeholders. The risk of a particular hazard may be traded-off with risks of other hazards, and/or with other system performance parameters.
Decision Criteria	Risk levels determine whether mitigation actions are required. They are also used to determine System Integrity Levels. Risk levels also form the basis of safety assurance arguments and are used by regulators to make certification decisions.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	
Implementation Considerations	The acceptability of a hazard risk may be determined in part by the benefit obtained from accepting the risk and the cost of further risk reduction.

Information Need Description	
Information Need	The status of the safety assessment task on a project, in terms of the current recorded status of all identified failure modes.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Dependability - Safety
Entities and Attributes	
Relevant Entities	Failure Modes as recorded in a Failure Mode Tracking System
Attributes	Failure Mode status: for example, (open: potential; open: risk greater than target; open: risk subject to trade; closed: risk acceptable or removed)
Base Measure Specification	
Base Measures	Failure Modes: number of failure modes in each recorded category
Measurement Methods	Access appropriate fields in Failure Mode Tracking System.
Type of Method	Objective in terms of counting failure modes in each category; may involve subjective judgment at the level of status assessment.
Scale	Nominal for each failure mode; integer counts of numbers of failure modes
Type of Scale	Categories, integer values
Unit of Measurement	
Derived Measure Specification	
Derived Measure	Aggregated status from all identified failure modes.
Measurement Function	Percentage closed indicator of progress of safety work.
Indicator Specification	
Indicator Description and Sample	Graph of numbers of failure modes in each category as functions of project elapse time.
Analysis Model	Reasons for non-closure of failure modes may be fully justifiable, e.g. system requirements volatility, design volatility etc.
Decision Criteria	Failure Mode status objectives may be linked with life cycle phase gates, test and acceptance milestones and regulatory assurance objectives.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	The *Failure Mode Count* measure is based on the status of identified system Failure Modes. Undiscovered failure modes are not considered by this measure.
Implementation Considerations	An effective and efficient safety process may not necessarily be indicated by early closure of failure modes.

Information Need Description	
Information Need	The status of one proposed means to reduce identified hazard risks to acceptable levels.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Dependability - Safety
Entities and Attributes	
Relevant Entities	Mitigations proposed to reduce identified risks to acceptable levels.
Attributes	Mitigations have three main kinds of attributes (1) reduction in hazard risk achieved, (2) effects on other risks and performances, if any and (3) cost/schedule implications.
Base Measure Specification	
Base Measures	Mitigation Status: status of a particular mitigation. Assume the following attributes are recorded: risk reduction, cost.
Measurement Methods	Access appropriate fields in a Safety Management System or documentation.
Type of Method	Estimates of risk reduction achievable and costs would usually involve subjective judgment.
Scale	Ratio
Type of Scale	Reals and ordinals.
Unit of Measurement	Risk expressed typically in probability of equivalent fatalities per event; cost in dollars.
Derived Measure Specification	
Derived Measure	Quality indicator of a mitigation in terms of risk efficiency for the particular hazard risk addressed. Also implications for system-wide risk efficiency. Also implications for other system performances, if any.
Measurement Function	
Indicator Specification	
Indicator Description and Sample	
Analysis Model	
Decision Criteria	Comparison between quality indicators of alternative mitigation proposals.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	A particular mitigation may reduce the risks of more than one hazard: the system safety specialty addresses these issues.
Implementation Considerations	The costs of available mitigation strategies are an important input to risk acceptance decisions. Usually, the acceptability of a risk is judged on the basis of the cost of avoiding one more life through risk reduction means, the financial consequences of the life being lost (or equivalent) and the benefits offered by accepting the risk.

Information Need Description	
Information Need	The degree of completion and confidence in the safety case, as provided to a certification authority.
Information Category	Product Quality
Measurable Concept	
Measurable Concept	Assurance - Safety
Entities and Attributes	
Relevant Entities	System Argument and supporting certification data.
Attributes	Status of argument compared with planned safety argument, in terms of required claims that are substantiated and confidence level.
Base Measure Specification	
Base Measures	Safety Argument: claims established, confidence.
Measurement Methods	Access appropriate documentation and records of safety process activity.
Type of Method	Objective in terms of counting claims established and comparing with plans. Subjective judgment involved in confidence assessment.
Scale	Nominal for each claim; integer counts of numbers of claims.
Type of Scale	Categories, integer values.
Unit of Measurement	
Derived Measure Specification	
Derived Measure	Aggregated status of safety argument.
Measurement Function	Percentage of claims established compared with plan. Progress of safety assessment in terms of certification data provided and claims supported.
Indicator Specification	
Indicator Description and Sample	Graph of numbers of claims in each category plotted against project elapse time. Distinguish between claims required for the safety argument to hold, and claims established by evidence.
Analysis Model	
Decision Criteria	Resource allocation based on progress of safety argument development.
Indicator Interpretation (sample chart)	
Additional Information	
Additional Analysis Guidance	These proposals are tentative.
Implementation Considerations	