Notes from the PSM Safety and Security Workshop, 17 July 2003

Attendees:

Frances Anderson
Matt Ashford
Dennis Ahern
Paul Caseley
Dana Van Orman
John Murdoch

Agenda:

- 13:00 – 13:15 Introduction & Background
- 13:15 – 14:00 Current Status of work
  - TWG results
  - Proposed ICM tables
- 14:00 – 14:30 Structure and Content of White Paper
  - authors, review, timeframe
- 14:30 – 15:00 Implementation Strategy
  - 'Publication' of White Paper
  - Introduction to wider safety & security communities
  - Trials
  - Enhancement to PSM
- 15:00 – 15:30 Break
- 15:30 – 16:30 Optional!
  - Measurement Descriptions and Data Items
  - Process improvement

Introduction

There was a brief introduction to the issues of measuring safety and security by Paul Caseley, it included general objectives of the workshop:

- To identify measures appropriate for the safety and security disciplines, in the spirit of the measurement approach of PSM;

- To draw up augmentations to the PSM materials, in particular the Issue-Category-Measure, Measurement Category and Measure Description Tables, with the objective of guiding users in developing measurement systems for these disciplines;

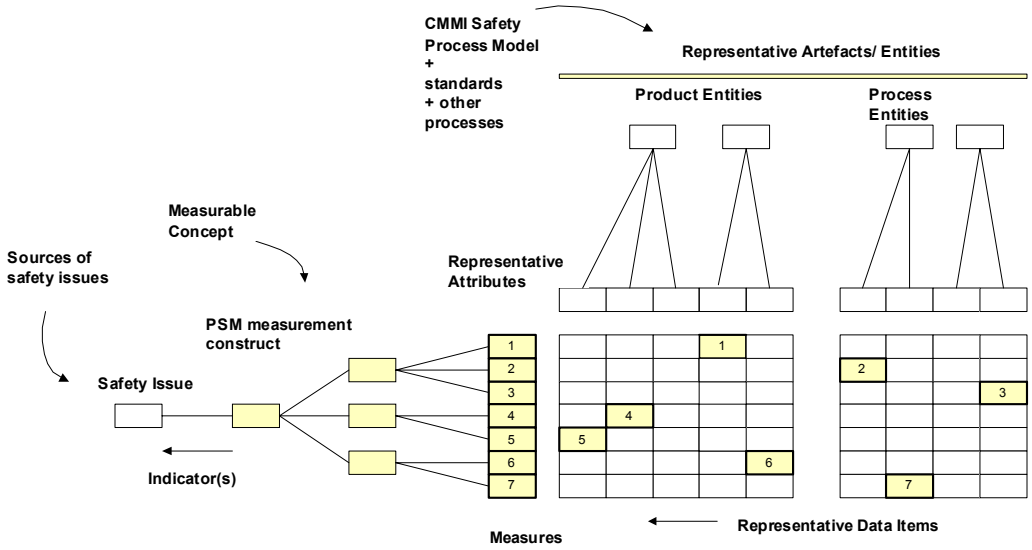
- To provide measurement support to the CMMI and +SAFE integration initiative;

- Secondary objective was to understand how we can improve Safety and Security processes through their measurement.

Current Work

John Murdoch walked the group through a presentation inviting responses and comments. The presentation was an overview of a white paper he had drafted for the PSM conference (note the presentation is available from the PSM website).

The draft outlined a mapping the of the existing safety attributes to the PSM version 4 measurement model. This is illustrated by the following reference measurement diagram:



In the diagram above the measurement construct has been placed on its side. Product entities are attributes such as vulnerabilities and hazards. Process entities are attributes such as effort or personnel involved in the process. The attributes must be used to derive a useful indicator that models an aspect or behaviour of safety and security process being measured. A useful measure could be an indicator that showed whether a safety or security process is being carried out to early or late to influence the design.

This raised questions in the workshop on whether John was driving the measures from the bottom up and was the information needs being truly met. John explained that this was both top down and bottom up. John further explained that an aim is to get practical measurements from existing attributes. Issues like:

- What are the fundamental measures we need from the safety critical project?
- Has the safety and security program been carried out?
- How are we doing with regards to the safety or security plan?
- Have we captured all the safety and security requirements?
- What is the impact of the proposed safety and security change?

John then outlined the main strategy for safety and security measures. This was to use as much of the existing PSM materials as possible. To illustrate his point an existing PSM measure "requirements status" was used as an example. Below is an extract of the example:

Functional Requirements	**Safety Requirements**
Category: Functional Size and Stability **Issue: Product Size, Stability and Scope**	Category: Scope - Safety **Issue: Product Size, Stability and Scope**
The Requirements measure counts the number of requirements in the system or product specifications. It also counts the number of requirements that are added, modified, or deleted. The measure provides information about the total number of requirements and the development risk due	The Safety Requirements measure counts the number of safety requirements in the system or product specifications arising from safety needs of the Customer and from the safety process itself. It also counts the number of safety requirements that are added, modified, or deleted. The measure

to growth and/or volatility in requirements.	provides information about the total number of safety requirements and the development risk due to growth and/or volatility in safety requirements.

John suggested that some existing PSM measurements only needed slight word changes. The above shows table shows a safety and security requirement description next to the general requirements PSM 4b description. This stimulated some debate as other domains such as reliability or testability may also need to be identified. Others argued it added little value.

John showed some other examples of the changes (these are attached to the end of this document and extracts from the proposed draft paper). Where possible the example was placed next to an existing PSM version 4 example, e.g:

Some saw problems with this in that we now work to version 5, which defines measurement specifications.

Structure and Content of the White Paper

The content of John's proposed a draft white paper was debated.

It was suggested that rather than propose actual changes to PSM that an alternate would be to provide an interpretation model utilising the existing PSM. Thus the white paper would be a supplement/interpretation of the PSM model rather than a proposed amendment. This supplement could then be tested (a trial project perhaps).

The supplement should contain practical indicators that are based on real data. The safety engineers and safety program managers should then validate these indicators. The CMMI work could help identify the typical work products.

One of the challenges in the safety world is the number of techniques and terms so, where possible, the paper should use generic representatives. Additionally, the PSM safety and security measurement should be aid the measuring the compliance of the safety and security processes against the appropriate standards.

Thus the white paper should provide guidance on how to measure safety and security processes within a PSM framework. The white paper should be seen as supplemental and not an amendment. Furthermore the format of the measurements should be in accordance with version 5 and use measurement specifications. The white paper should also contain practical indicators and explain the benefits and use.

Implementation Strategy

It was agreed that a draft of the white paper should be available by the end of September 2003. This draft will be distributed to the technical working group (the workshop members) for review. Note all that attended the workshop kindly agreed to review the paper.

By mid November the reviewed paper will be distributed to safety and interested measurement practitioners for further comment and review. The authors (John Murdoch/Paul Caseley) should liase with other PSM authors (e.g. Garry Roedler) to keep a common format. It was suggested that an outline of the strategy and some of the paper be submitted for an Australian conference to get buy in of safety practitioners.

If the white paper proves successful trials should be held in 2004.

AOB

The CMMI extension team were seen as an important stakeholder.

It was suggested that the DDX project (see Kevin Richards) may be a potential project.

Security members of CMMI extension team were identified as important stakeholders.

Francis Anderton was tasked with trying to identify a security POC.

It was also suggested that Paul Caseley contact Joe Jarzombek to for additional the security POCs.

Functional Size and Stability	**Scope - Safety**
Common Issue Area: Product Size, Stability and Scope	Common Issue Area: Product Size, Stability and Scope
Functional Size and Stability measures quantify the functionality of a system or product. Functional size may be used to estimate development schedule and cost. These measures also provide information about the amount and frequency of change to the system's functionality, which is critical late in development. Functional changes generally correlate to effort, cost, schedule, and product size changes.	Scope - Safety measures quantify the safety-critical parts of a system or product. Safety scope may be used to estimate safety assessment schedule and cost. These measures also provide information about the amount and frequency of change to safety-critical parts of the system. Scope may cover functional, component, mode and interface views of the system. Separate measures may be developed corresponding to different safety integrity levels.
Project Application • Applicable to all sizes and types of projects • Applicable to all process models	**Project Application** • Applicable to all sizes and types of projects that are safety-critical • Applicable to all process models
Measures Included in this Category • Requirements • Functional Change Workload • Function Points	**Measures Included in this Category** • Safety Requirements • Safety-Critical Functions • Safety-Critical Components • Safety-Critical Modes • Safety-Critical Interfaces • Safety Change Workload • Safety Zones • Safety Argument
Limitations • Functional size does not generally address the quality of the product or system measured. • System-level functional size measures do not always map directly to the effort required to build the system (especially when NDI/COTS/GOTS is used). • Functional size is hard to measure consistently. Clear counting standards are required (such as the IFPUG Counting Practices manual).	**Limitations** • Safety scope does not generally address the achieved safety properties of the product or system measured. • System-level safety scope measures are indicative of safety resources needed, but the implications of safety requirements for components can vary. • Although safety scope can be estimated at the beginning of a project, it may be modified as safety assessments are undertaken.
Related Measurement Categories • Work Unit Progress • Physical Size and Stability	**Related Measurement Categories** • Work Unit Progress • Physical Size and Stability • Functional Size and Stability
Example Indicator(s) • Requirements Stability (PSM Part 5, Section 2.14) • Requirements Stability by Type of Change (PSM Part 5, Section 2.14) • Multiple Indicators for Change Requests (PSM Part 5, Section 2.15) • Change Requests by Priority (PSM Part 5, Section 2.15)	**Example Indicator(s)** • Safety Scope Log; multiple indicators •

Dependability - Reliability	**Dependability - Safety**
Common Issue Area: Product Quality	Common Issue Area: Product Quality
Dependability - Reliability measures estimate the probability that an item will continue to function for a specified period of time under certain conditions. Reliability is the probability that an item will function without failure for a specified period of time under certain conditions. Availability is related to dependability - Reliability. Failures that occur during operation either degrade or completely eliminate certain functions, some of which could be mission critical or safety hazards. These measures monitor the quantity and severity of failures, and determine if the expected frequency of failures is acceptable. Estimated probabilities of failures and consequences can be determined through modeling, analysis, and/or testing.	Dependability - Safety measures estimate the safety of an item for a specified period of time under certain conditions. Safety is interpreted as an acceptably low level of risk of a serious accident, where 'serious' is dependent on the context but generally involves injury and loss of life. Safety is assessed on the basis of (1) the reduced risk achieved from mitigations of identified hazards and (2) the degree of confidence that all hazards have been identified. Each hazard is associated with (1) a probability of an accident occurring and (2) a severity of the consequences. Mitigations can take a variety of forms. Safety measures are used in the development phases of a product or system in order to control the safety risks presented to users and the environment during operations. Safety measures are used during operations to support maintenance processes and to inform ongoing and future safety assessments. Integrated safety arguments are developed for purposes of assurance and certification.
Project Application • Applicable to all sizes and types of projects • Applies mostly to systems that have mission critical or safety considerations	**Project Application** • Applicable to all sizes and types of projects that are safety critical.
Measures Included in this Category • Failures • Fault Tolerance	**Measures Included in this Category** • Hazards • Failure Modes • Hazard Scenarios • Safety Assessments and Assumptions • Mitigations • Safety Incidents and Accidents
Limitations • In complex systems, it is difficult to determine all possible failures and associated impacts. • It may be difficult or prohibitive to test for all possible failures, or all chain of event combinations.	**Limitations** • In complex systems, it is difficult to determine all hazards, failure modes and failure effect propagation paths. • Safety measurement is subject to the 'zero-infinity' problem; numerical estimates become questionable for very rare events that have major consequences. • Probabilistic risk assessment has to be used with engineering judgement; emphasis is usually placed on conservative, dependable indicators rather than accuracy of prediction. • A desirable outcome of a safety assessment is an *absence* of hazards; confidence in a process that identifies few hazards depends on the scope and depth of assessment undertaken.

Related Measurement Categories • Functional Correctness • Supportability - Maintainability • Usability	**Related Measurement Categories** • Functional Correctness • Supportability - Maintainability • Dependability - Reliability • Scope - Safety • Usability
Example Indicator(s) • MTBF Ranges Based on Historical Data (PSM Part 5, Section 2.22) • Reliability Growth Tracked With Mean Time to Failure (PSM Part 5, Section 2.22)	**Example Indicator(s)** • Hazard Log, multiple indicators • Failure Mode Log, multiple indicators

Dependability - Safety	**Assurance - Safety**
Common Issue Area: Product Quality	Common Issue Area: Product Quality
Dependability - Safety measures estimate the safety of an item for a specified period of time under certain conditions. Safety is interpreted as (1) the mitigations associated with a set of identified hazards, and (2) a degree of confidence that all hazards have been identified. Each hazard is associated with (1) a probability of an accident occurring and (2) a severity of the consequences. Mitigations can take a variety of forms, but share the common purpose of reducing hazard risks to acceptable levels. Safety measures are used in the development phases of a product or system in order to control the safety risks presented to users and the environment during operations. Safety measures are used during operations to support maintenance processes and to inform ongoing and future safety assessments. Integrated safety arguments are developed for purposes of assurance and certification.	Assurance - Safety measures estimate the progress of safety work in meeting regulatory certification requirements. This is assumed to be achieved by means of: (1) a top-level safety argument and (2) referenced certification evidence. Measurement is made against a planned safety argument.
Project Application • Applicable to all sizes and types of projects that are safety critical.	**Project Application** • Applicable to all sizes and types of projects that are safety critical and subject to regulatory certification.
Measures Included in this Category • Hazards • Failure Modes • Hazard Scenarios • Safety Assessments and Assumptions • Mitigations • Safety Incidents and Accidents	**Measures Included in this Category** • Safety Argument
Limitations • In complex systems, it is difficult to determine all hazards, failure modes and failure effect propagation paths. • Safety measurement is subject to the 'zero-infinity' problem; numerical estimates become questionable for very rare events that have major consequences. • Probabilistic risk assessment has to be used with engineering judgement; emphasis is usually placed on conservative, dependable indicators rather than accuracy of prediction. • A desirable outcome of a safety assessment is an *absence* of hazards; confidence in a process that identifies few hazards depends on the scope and depth of assessment undertaken.	**Limitations** • Measurement against a planned safety argument has to track changes in the plan arising, for example, from uncovered hazards.
Related Measurement Categories • Functional Correctness • Supportability - Maintainability • Dependability - Reliability • Scope - Safety • Usability	**Related Measurement Categories** • Dependability -Safety • Scope - Safety

Example Indicator(s) • Hazard Log, multiple indicators • Failure Mode Log, multiple indicators	**Example Indicator(s)** • Percentage of safety argument that is supported by evidence.

Requirements Status	**Category: Work Unit Progress** **Issue: Schedule and Progress**
The Requirements Status measure is derived from the Requirements measure in the Functional Size and Stability measurement category. It counts the number of requirements that have been defined and allocated to hardware and software components. It also counts the number of defined requirements that have been allocated to test cases, and the number that have been successfully tested. The measure is an indication of product design and test progress. When used to measure test status, the measure is used to evaluate whether required functionality has been successfully demonstrated against the specified requirements, and the amount of testing that has been performed. The measure provides excellent test coverage and is also known as "Breadth of Testing."	The Requirements Status measure is derived from the Functional Requirements measure in the Functional Size and Stability measurement category and from the Requirements measures in the non-functional scope measurement categories. When used to measure test status, the measure is used to evaluate whether required functionality and non-functional properties have been successfully demonstrated against the specified requirements, and the amount of testing that has been performed…
Selection Guidance	**Selection Guidance**
Project Application • Generally applicable to all sizes and types of projects with a requirements or design activity.	
Process Integration • Requires disciplined requirements traceability and testing processes for successful implementation. Allocated requirements should be testable and mapped to test sequences. If an automated design tool is used, the data is more readily available. • Can be applied for each unique test sequence, such as CI, integration, system, and regression test, including "dry-runs." • One of the more difficult Work Unit Progress measures to collect since requirements may not map directly to components, test cases, and test procedures. It is sometimes difficult to objectively determine if a requirement has been successfully tested. • Early in a project, the requirements baseline is limited to high-level specifications. Later in a project, the requirements baseline expands and measurement data is traceable to components and test cases. • Some requirements may not be testable until late in the testing process. Others are not directly testable. Some may be verified by inspection. • Software requirements are allocated from system requirements and organization imposed requirements.	

• Track which requirements are allocated to hardware and which are allocated to software.	
Usually Applied During • Requirements Analysis (Estimates) • Design (Estimates and Actuals) • Implementation (Estimates and Actuals) • Integration and Test (Estimates and Actuals)	
Specification Guidance	**Specification Guidance**
Typical Data Items • Total number of requirements • Number of requirements traced to detailed specifications • Number of requirements traced to hardware or software components • Number of requirements traced to test specifications • Number of requirements tested successfully	• Number of requirements traced from non-functional analysis
Typical Attributes • Increment • Category of requirement (stated, derived) • Type of requirement (user, system, component, software, etc.) • Specification reference • Test sequence reference	• Type of requirement (user, system, component, software, non-functional property, etc.)
Typical Aggregation Structure • Function	• Depends on non-functional property (e.g. hazard scenario)
Typically Collected for Each • Requirement specification	
Count Actuals Based On • Completion of specification review • Baselining of specifications • Baselining of requirements traceability matrix • Successful completion of all tests in the appropriate test sequence	
This measure answers questions such as: Have all of the requirements been allocated to hardware or software components? Are the requirements being tested as scheduled? Is implementation of the requirements behind or ahead of schedule?	What proportion of the requirements is derived from safety assessment?

Action Item Status	**Category: Work Unit Progress** **Issue: Schedule and Progress**
The Action Item Status measure reports the number and status of action items for technical and management activities. This measure provides information on the total number of open action items, as well as the number opened or closed during the reporting period. Analyzing trends of opened and closed items is effective in evaluating plans.	
Selection Guidance	**Selection Guidance**
Project Application • Useful to any project that identifies specific action items.	
Process Integration • Requires a process for identifying, handling, and tracking action items. • Data is usually available. An automated tracking system or database simplifies data collection and improves timely analysis. Otherwise, data may be collected manually from staff members, meeting minutes, or other management reports.	• Particular processes (e.g. safety) will generate and track action items pertaining to the particular system properties etc. for which they have responsibility.
Usually Applied During • Requirements Analysis (Estimates and Actuals) • Design (Estimates and Actuals) • Implementation (Estimates and Actuals) • Integration and Test (Estimates and Actuals) • Operations and Maintenance (Estimates and Actuals)	
Specification Guidance	**Specification Guidance**
Typical Data Items • Number of action items reported • Number of action items resolved • Average age of action items • Average time to resolve	
Typical Attributes • Priority • Source • Scope • Impact	• Source, including specialty engineering • Responsibility for action
Typical Aggregation Structure • Activity • Component	
Typically Collected for Each • Key activity • Project	• Process (e.g. safety)
Count Actuals Based On • Action items identified • Action items verified • Action items resolved	
Alternatives to Action Items Include • Project issues	

This measure answers questions such as: Are high priority action items being resolved quickly?	What is the status of action items arising from the safety process?

Functional Requirements	**Safety Requirements**
Category: Functional Size and Stability **Issue: Product Size, Stability and Scope**	Category: Scope - Safety **Issue: Product Size, Stability and Scope**
The Requirements measure counts the number of requirements in the system or product specifications. It also counts the number of requirements that are added, modified, or deleted. The measure provides information about the total number of requirements and the development risk due to growth and/or volatility in requirements.	The Safety Requirements measure counts the number of safety requirements in the system or product specifications arising from safety needs of the Customer and from the safety process itself. It also counts the number of safety requirements that are added, modified, or deleted. The measure provides information about the total number of safety requirements and the development risk due to growth and/or volatility in safety requirements.
Selection Guidance	**Selection Guidance**
Project Application • Applicable to all domains. • Useful for any size and type of project that tracks requirements. • Effective for both non-developed (COTS/GOTS/Reuse) and newly developed components.	**Project Application** • Applicable to the safety domain and to domains affected by safety. • Useful for any size and type of project that tracks requirements and is safety-related. • Effective for both non-developed (COTS/GOTS/Reuse) and newly developed components.
Process Integration • It is sometimes difficult to specifically define discrete requirements. A consistently applied definition makes this measure more effective. • Requires a good requirements traceability process. If an automated design tool is used, the data is more readily available. • Count changes against a baseline that is under formal configuration control. Both stated and derived requirements may be included. • To evaluate stability, a good definition of the impacts of each change is required. • Organize requirements hierarchically (e.g. user requirements lead to system requirements which are decomposed into software, hardware, operations, and maintenance requirements.	**Process Integration** • See the Functional Requirements measure for general comments on requirements. • Safety requirements are requirements that are derived from safety concerns and processes. • Meeting safety requirements may involve activity additional to the safety process, for example in the design process. A safety requirement may trace to derived safety requirements.
Usually Applied During • Project Planning (Estimates) • Requirements Analysis (Estimates and Actuals) • Design (Actuals) • Implementation (Actuals) • Integration and Test (Actuals) • Operations and Maintenance (Actuals)	**Usually Applied During** • Project Planning (Estimates), including Safety Planning • Requirements Analysis (Estimates and Actuals) • Design (Actuals) • Implementation (Actuals) • Integration and Test (Actuals) • Operations and Maintenance (Actuals)
Specification Guidance	**Specification Guidance**
Typical Data Items • Number of requirements (user, system, component, etc.)	**Typical Data Items** • Number of requirements (user, system, component, etc.)

• Number of requirements added • Number of requirements deleted • Number of requirements modified	• Number of requirements added • Number of requirements deleted • Number of requirements modified
Typical Attributes • Increment • Change source (supplier, acquirer, user) • System component • Priority (high, medium, low) • Level of requirement (user, system, software)	**Typical Attributes** • Increment • Change source (supplier, acquirer, user) • System component • Priority (high, medium, low) • Level of requirement (user, system, software)
Typical Aggregation Structure • Function	**Typical Aggregation Structures** • Function • Hazard Scenario • Safety Argument
Typically Collected for Each • Requirement specification	**Typically Collected for Each** • Requirement specification
Count Actuals Based On • Passing requirements inspection • Release to configuration management • SCCB Approval	**Count Actuals Based On** • Passing requirements inspection • Release to configuration management • SCCB Approval • Regulatory clearance
This measure answers questions such as: Have the requirements allocated to each incremental delivery or increment changed? Are requirements being deferred to later increments? How much has functionality changed? What components have been affected the most? Is the number of requirements growing? If so, at what rate?	**This measure answers questions such as:** When are safety requirements being addressed? How much has required system/product/ component safety changed? What components have been affected the most? Is the number of safety requirements growing? If so, at what rate?

Components	**Safety-Critical Components**
Category: Product Size, Stability and Scope **Issue: Product Size and Stability**	**Category: Product Size, Stability and Scope** **Issue: Scope - Safety**
The Components measure counts the number of elementary components in a system or product, and the number that are added, modified, or deleted. The total number of components defines the size of the system. Changes in the number of estimated and actual components indicate risk due to product size volatility and additional work that may be required. Reporting the number of components provides size information earlier than other size measures, such as lines of code or system interfaces.	The Safety-Critical Components measure counts the number of elementary components in a system or product, and the number that are added, modified, or deleted, that carry safety-critical functions. The total number of safety-critical components defines an aspect of the size of the safety-critical part of the total system. The measure can be applied at different safety integrity levels. Changes in the number of estimated and actual components indicate risk due to product size volatility and additional work that may be required.
Selection Guidance	**Selection Guidance**
Project Application • Applicable to all sizes and types of projects. • Applicable to all application domains, generally with different component definitions.	**Project Application** • Applicable to all sizes and types of projects that are safety critical. • Applicable to all safety domains, generally with different component definitions.
Process Integration • Requires a well-defined and consistent component allocation structure. • Required data is generally easy to obtain from design tools, configuration management tools, or documentation. • Counts of deleted and added components are relatively easy to collect. Modified components are sometimes not tracked. • Volatility in the planned number of components may represent instability in the requirements or in the design of the system or product.	**Process Integration** • See the Components measure in the Product Size and Stability category for general guidance on component measures. • The safety process will generate initial estimates of component scope as part of the planning activity. Subsequent safety assessment will often call for revisions of initial assessments.
Usually Applied During • Requirements Analysis (Estimates) • Design (Estimates and Actuals) • Implementation (Estimates and Actuals) • Integration and Test (Actuals) • Operations and Maintenance (Actuals)	**Usually Applied During** • Requirements Analysis (Estimates) • Design (Estimates and Actuals) • Implementation (Estimates and Actuals) • Integration and Test (Actuals) • Operations and Maintenance (Actuals)
Specification Guidance	**Specification Guidance**
Typical Data Items • Number of units • Number of units added • Number of units deleted • Number of units modified	**Typical Data Items** • Number of units • Number of units added • Number of units deleted • Number of units modified
Typical Attributes • Increment • Source (new, reused, NDI, GOTS, or COTS)	**Typical Attributes** • Increment • Source (new, reused, NDI, GOTS, or COTS)

• Language (if software) • Delivery status (deliverable, non-deliverable) • End-use environment (operational, support)	• Delivery status (deliverable, non-deliverable) • End-use environment (operational, support)
Typical Aggregation Structure • Component	**Typical Aggregation Structure** • Component
Typically Collected for Each • CI or equivalent	**Typically Collected for Each** • CI or equivalent
Count Actuals Based On • Release to configuration management • Passing unit test • Passing inspection	**Count Actuals Based On** • Release to configuration management • Passing unit test • Passing inspection
This measure answers questions such as: How many components need to be implemented and tested? How much has the approved system baseline changed? Have the components allocated to each increment changed? Is functionality slipping to later increments?	**This measure answers questions such as:** How many components need to be subjected to the safety process? At what level of integrity? Which components are affected by *this* change in safety requirements? Are changes in safety requirements being responded to by the design process?

Failures	**Hazards**
Category: Dependability-Reliability **Issue: Product Quality**	**Category: Dependability-Safety** **Issue: Product Quality**
The Failures measure is based on the number, criticality, and time interval between failures. A failure is the inability of a system component to perform a required function under certain conditions within a specified time. This measure is used to support indicators of reliability such as historical achievement of system mean time between failures (MTBF) and reliability growth.	The Hazards measure is based on the number, criticality, and status of identified system hazards. A hazard is a particular safety - related risk that a system presents to its operational environment. It is usually expressed as the product of the likelihood of an accident and the severity of the consequences. This measure is used to support assessment of acceptability of safety risks. Hazard consequences are usually categorized into severity levels by regulatory authorities within an industrial sector; acceptable risk levels are usually indicated with associated required levels of safety assurance (e.g. required process tasks, provided evidence) .
Selection Guidance	**Selection Guidance**
Project Application • Applicable to all sizes and types of projects.	**Project Application** • Applicable to all sizes and types of projects that are safety-critical.
Process Integration • Requires a disciplined failure tracking process, including training of users, operators, and testers. Easier to collect if an automated system is used. Data comes from test logs or incident reports. • It is useful to categorize failure causes, including failures caused by requirements specification problems, component design, operator error, or documentation errors. • It is beneficial to categorize failures by the type of corrective and preventive actions necessary, including repair or replacement of the item, or training of test personnel or operators. • Some projects specify reliability threshold limits, such as an acceptable number of failures over time. • Operating time to failure may be based on either component operating time or clock time. • The test environment must be representative of the operational environment. The test environment and input data must thoroughly exercise the system for resulting indicators to be representative of operations.	**Process Integration** • Requires a disciplined hazard tracking process, including training of users, operators, and testers. Easier to collect if an automated system is used. Data comes from historical data, standards, safety assessments, test logs and incident/ accident reports. • Likelihoods may be expressed as probabilities per unit time or per exposure time or per mission event. • It is useful (and often required) to categorize hazards by the severity of their consequences. Categories are usually specified by applicable regulatory standards • Hazards with initially unacceptable risks, once identified, have to be 'mitigated'; the tracking of hazards should include records of their status and references to the mitigations selected. • The hazards and their mitigations form the basis of the safety argument used for safety assurance and certification. • Top-level system hazards typically arise from combinations of component failures, system modes, operational actions and environmental factors; the aggregation structure 'hazard scenario' aggregates those entities involved causally in a hazard.
Usually Applied During • Design (Estimates) • Implementation (Estimates and Actuals) • Integration and Test (Estimates and	**Usually Applied During** • Requirements (Estimates) • Design (Estimates) • Implementation (Estimates and Actuals)

Actuals) • Operations and Maintenance (Estimates and Actuals)	• Integration and Test (Estimates and Actuals) • Operations and Maintenance (Estimates and Actuals)
Specification Guidance	**Specification Guidance**
Typical Data Items • Date and time that failure occurred • Date and time that failure was resolved • Operating time since the last failure	**Typical Data Items** • Hazard Log fields, e.g. date identified, name, assessment that triggered identification etc.
Typical Attributes • Failure identifier • Type of failure • Severity of failure effect • Root cause of failure • Phase of occurrence • Corrective and preventive actions required • Test sequence	**Typical Attributes** • Hazard identifier • Probability • Severity • Status • Phase of occurrence • Mitigation actions required • Test sequence
Typical Aggregation Structure • Function • Component	**Typical Aggregation Structure** • Hazard Scenario
Typically Collected for Each • Function • CI or equivalent	**Typically Collected for Each** • Safety-critical Function
Count Actuals Based On • Failure documented • Failure validated • Failure resolved	**Count Actuals Based On** • Accident documented • Accident validated • Accident resolved
This measure answers questions such as: What is the system's operational reliability? Is the system ready for operation? How often (and how severely) will the system/component fail during operation of the system? Will the system, component, or function be available for use when it is needed?	**This measure answers questions such as:** What is the system's operational safety? Is the system ready for operation? How often (and how severely) will the system/component fail safety-critically during operation? Is the part of the safety argument relating to *this* hazard acceptable?

Hazards	**Hazard Scenarios**
Category: Dependability - Safety **Issue: Product Quality**	**Category: Dependability - Safety** **Issue: Product Quality**
The Hazards measure is based on the number, criticality, and status of identified system hazards. A hazard is a particular safety - related risk that a system presents to its operational environment. It is usually expressed as the product of the likelihood of an accident and the severity of the consequences. This measure is used to support assessment of acceptability of safety risks. Hazard consequences are usually categorized into severity levels by regulatory authorities within an industrial sector; acceptable risk levels are usually indicated with associated required levels of safety assurance (e.g. required process tasks, provided evidence).	The Hazard Scenarios measure is based on counting the number of sets of causes of a potential accident. A particular hazard may be associated with different sets of failure modes, operational events and other factors; this measure indicates the 'size' of a hazard in terms of its causes.
Selection Guidance	**Selection Guidance**
Project Application • Applicable to all sizes and types of projects that are safety-critical.	**Project Application** • Applicable to all sizes and types of projects that are safety-critical.
Process Integration • Requires a disciplined hazard tracking process, including training of users, operators, and testers. Easier to collect if an automated system is used. Data comes from historical data, standards, safety assessments, test logs and incident/ accident reports. • Likelihoods may be expressed as probabilities per unit time or per exposure time or per mission event. • It is useful (and often required) to categorize hazards by the severity of their consequences. Categories are usually specified by applicable regulatory standards • Hazards with initially unacceptable risks, once identified, have to be 'mitigated'; the tracking of hazards should include records of their status and references to the mitigations selected. • The hazards and their mitigations form the basis of the safety argument used for safety assurance and certification. • Top-level system hazards typically arise from combinations of component failures, system modes, operational actions and environmental factors; the aggregation structure 'hazard scenario' aggregates those entities involved causally in a hazard.	**Process Integration** • Requires a disciplined hazard tracking process, including training of users, operators, and testers. • Requires records of the contributory failure modes and related factors that give rise to hazards. • An example measure is the counting of cut sets in a Fault Tree Analysis.
Usually Applied During • Requirements (Estimates) • Design (Estimates) • Implementation (Estimates and Actuals)	**Usually Applied During** • Requirements (Estimates) • Design (Estimates) • Implementation (Estimates and Actuals)

• Integration and Test (Estimates and Actuals) • Operations and Maintenance (Estimates and Actuals)	• Integration and Test (Estimates and Actuals) • Operations and Maintenance (Estimates and Actuals)
Specification Guidance	**Specification Guidance**
Typical Data Items • Hazard Log fields, e.g. date identified, name, assessment that triggered identification etc.	**Typical Data Items** • Fields in the Hazard Log • Fields in the Safety Assessments
Typical Attributes • Hazard identifier • Probability • Severity • Status • Phase of occurrence • Mitigation actions required • Test sequence	**Typical Attributes** • Hazard identifier • Probability • Severity • Number of Failure Mode sets • Number of phases/ modes involved • Number of operational actions involved
Typical Aggregation Structure • Hazard Scenario	**Typical Aggregation Structure** • Safety Argument
Typically Collected for Each • Safety-critical Function	**Typically Collected for Each** • Hazard
Count Actuals Based On • Accident documented • Accident validated • Accident resolved	**Count Actuals Based On** • Accident documented • Accident validated • Accident resolved
This measure answers questions such as: What is the system's operational safety? Is the system ready for operation? How often (and how severely) will the system/component fail safety-critically during operation? Is the part of the safety argument relating to *this* hazard acceptable?	**This measure answers questions such as:** In what different ways can this hazard occur? What is the 'causal reach' of this hazard within the system? What is the 'causal reach' of this hazard within operations?