

ISO/IEC JTC 1/SC 7, Software Engineering

Jim Moore

moorej@mitre.org

September 2010

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

Many Standards are Names

A standard is a Name for an otherwise fuzzy concept

In a complex, multidimensional trade space of solutions ...

... a standard gives a name to a bounded region.

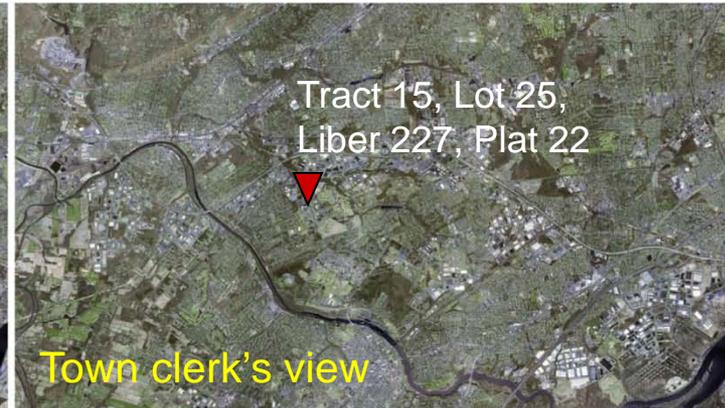


It defines some characteristics that a buyer can count on.

- Many software engineering standards assign names to practices or collections of practices.
- This enables communication between
 - Buyer and seller
 - Government and industry
 - Insurer and insured

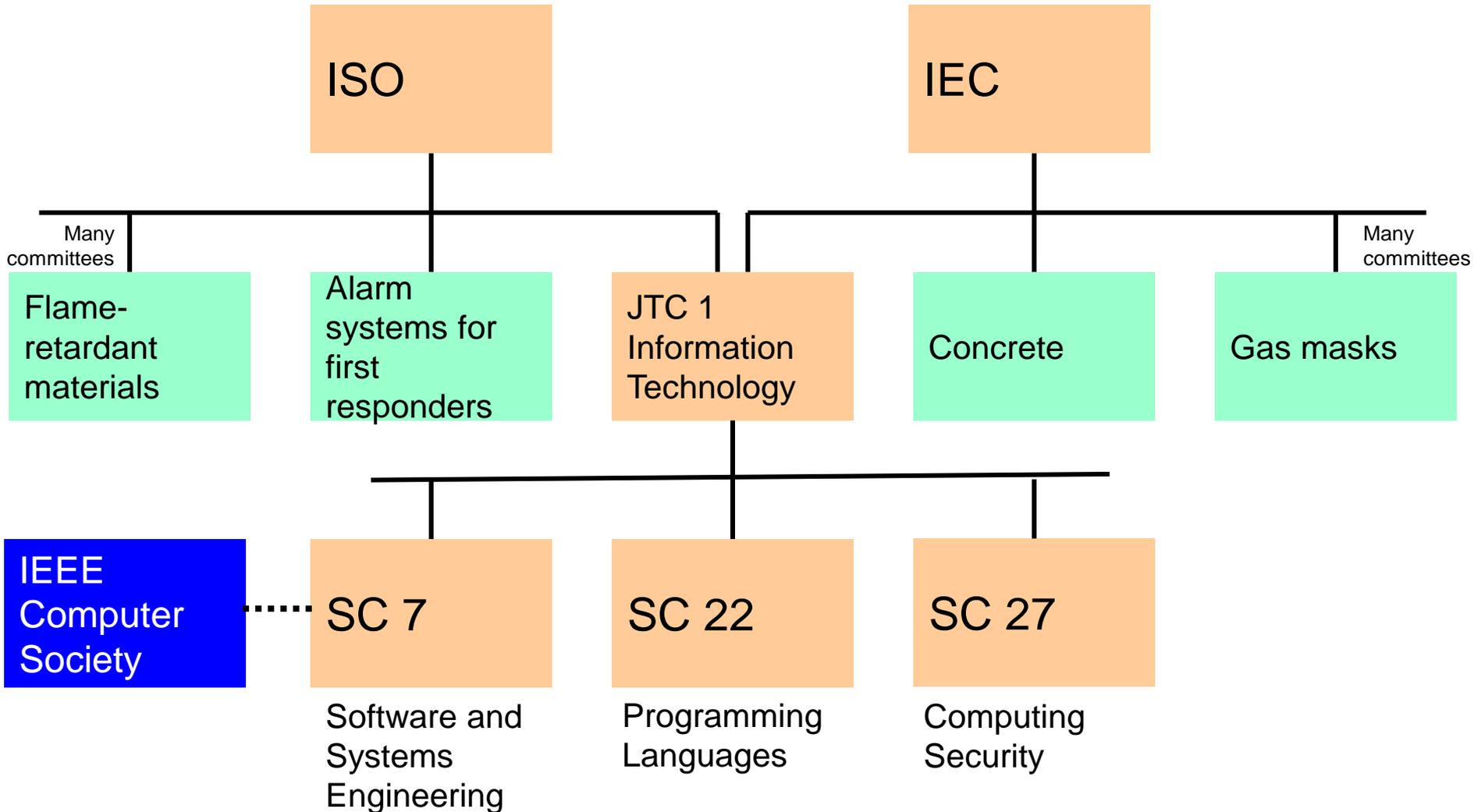
Names are Important

We use names to localize the subject under discussion. But sometimes confusion results because we use different name spaces.



- Would you know that these are different names for the same thing?
- Would you know without the map?
- 12207 and 15288 are “maps” for the life cycle process space.

Security and Assurance Concerns in International Standards

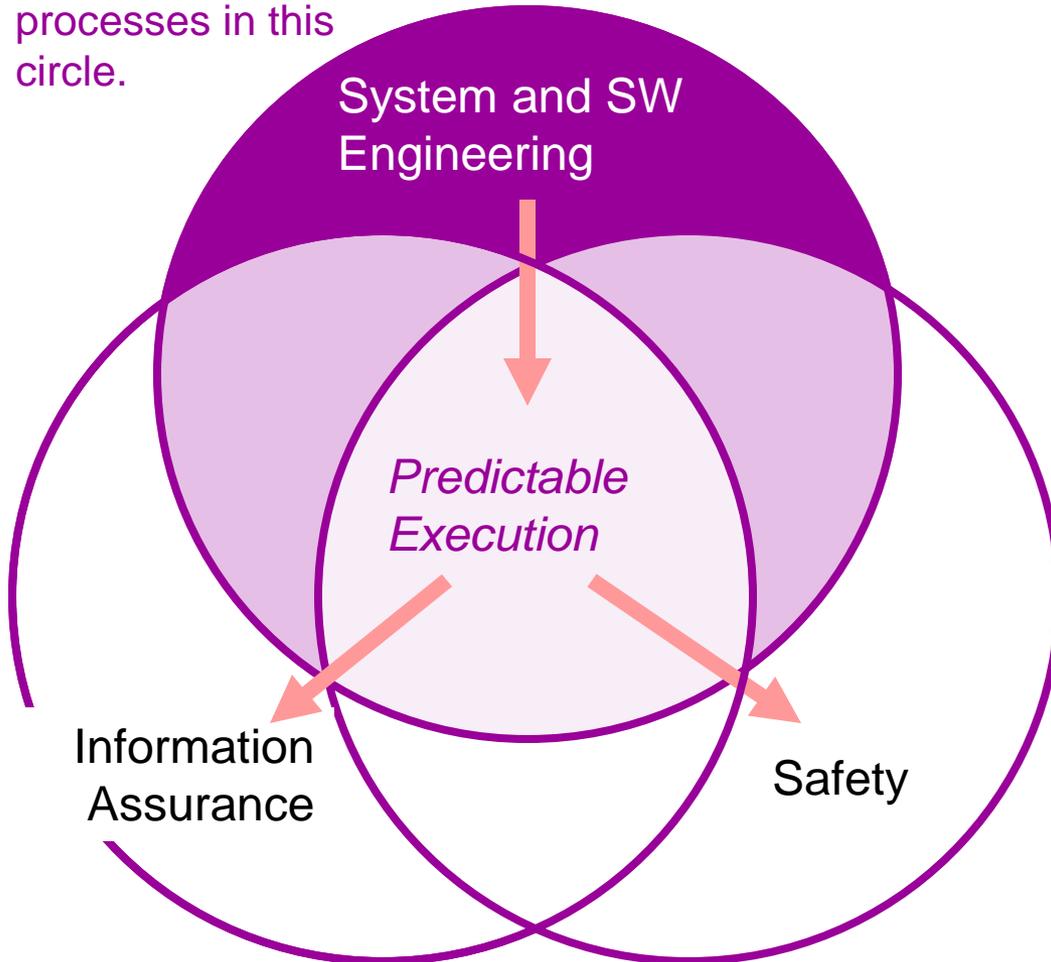


Putting together the pieces

- **ISO/IEC JTC 1/SC 7 (Software and Systems Engineering)**
 - Develop a stable set of software and systems engineering processes that can form the foundation for assurance techniques.
- **ISO/IEC JTC 1/SC 22 (Programming Languages)**
 - Survey vulnerabilities in programming languages and develop comparative guidance on how to avoid or mitigate them.
- **ISO/IEC JTC 1/SC 27 (Computing Security)**
 - Define assurance techniques in a manner that relates to sound software and systems engineering.
- **IEEE Computer Society**
 - **SWEBOK Project**
 - Revise SWEBOK Guide to better address assurance
 - **Professional certification**
 - Revise CSDA and CSDP to better address assurance
 - **Standards Activity**
 - Harmonize IEEE standards with international standards

Relating SW Assurance to SW Engineering

12207 and 15288 address the processes in this circle.



For a safety analysis to be valid ...

For a security analysis to be valid ...

The execution of the system must be *predictable*. This requires

...

- Correct implementation of requirements, expectations and regulations.

Traditional concern of SW Eng

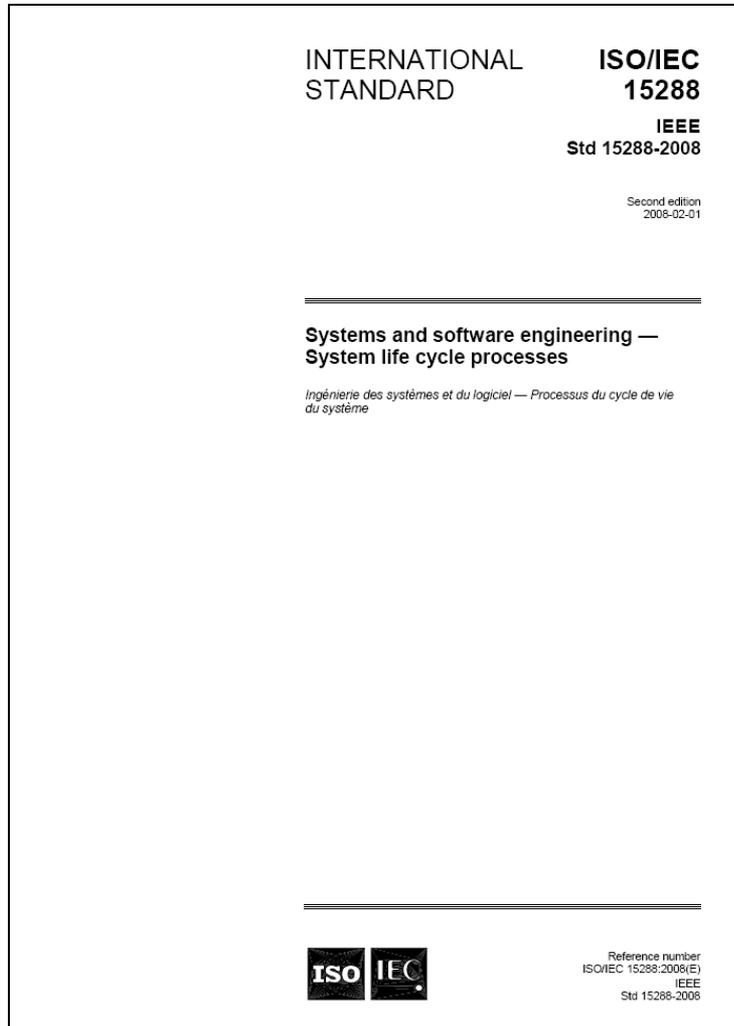
- Exclusion of unwanted function even in the face of attempted exploitation.

New concern

Ongoing work in SC 7

- Documentation of software systems
- Tools and CASE environments
- Software product evaluation and measurement
- ➡ ■ Life cycle processes
- ➡ ■ Software and systems assurance
- Process assessment
- Functional size measurement
- Modeling languages
- Software engineering body of knowledge
- Software asset (license) management
- Vocabulary
- Systems and software quality management
- Software engineering for very small enterprises
- IT service management
- Testing

ISO/IEC/IEEE 15288, System Life Cycle Processes



- Provides 25 processes covering the life-cycle of any human-made system
- 84 pages
- First written by ISO/IEC JTC 1/SC 7 in 2002
- Adopted by IEEE in 2003
- Jointly revised in 2008

ISO/IEC/IEEE 12207, Software Life Cycle Processes

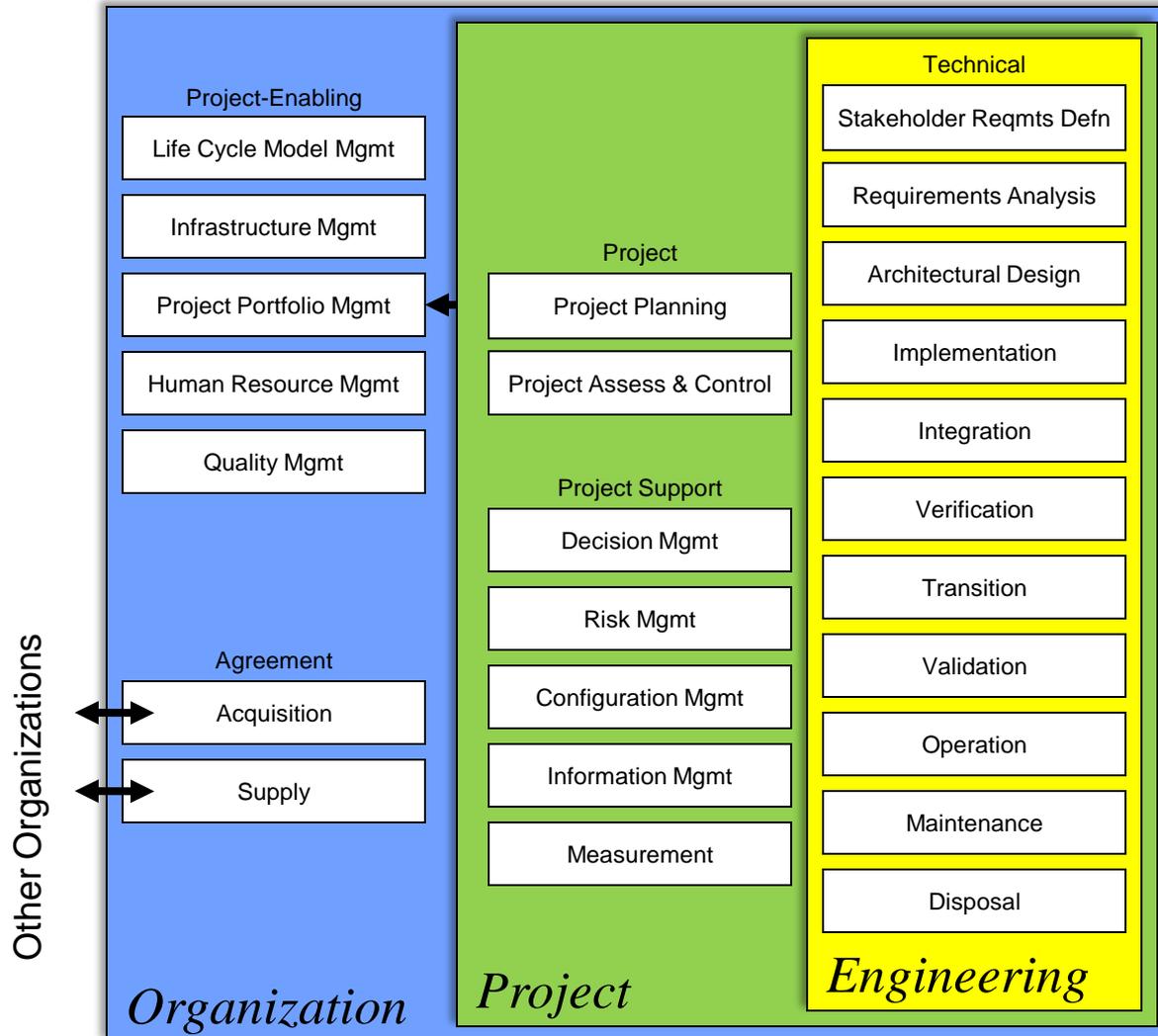


- Provides 43 processes covering the life-cycle of any software product or system element
- 138 pages
- First written by ISO/IEC JTC 1/SC 7 in 1995
- Adopted by IEEE in 1996
- Jointly revised in 2008

15288 and 12207 Give Names to Processes

- ISO/IEC 15288:2008 gives names to processes in the life cycle of a system.
- ISO/IEC 12207:2008 gives names to processes in the life cycle of a software product or service.
- The two standards are designed to be used together for software-intensive systems.
- The names are important so that acquirers and suppliers can communicate regarding their practices.
 - “Oh, when you say ‘implementation’, you include ‘testing’? Oh, no, no, no-- in our corporate process, testing is a separate thing; so our contract doesn’t include that! You have to pay us more if you want testing.”
- The names are important as a basis for process evaluation and improvement.
- The names are important to provide a context for implementing *improved practices*. – **Our goal.**

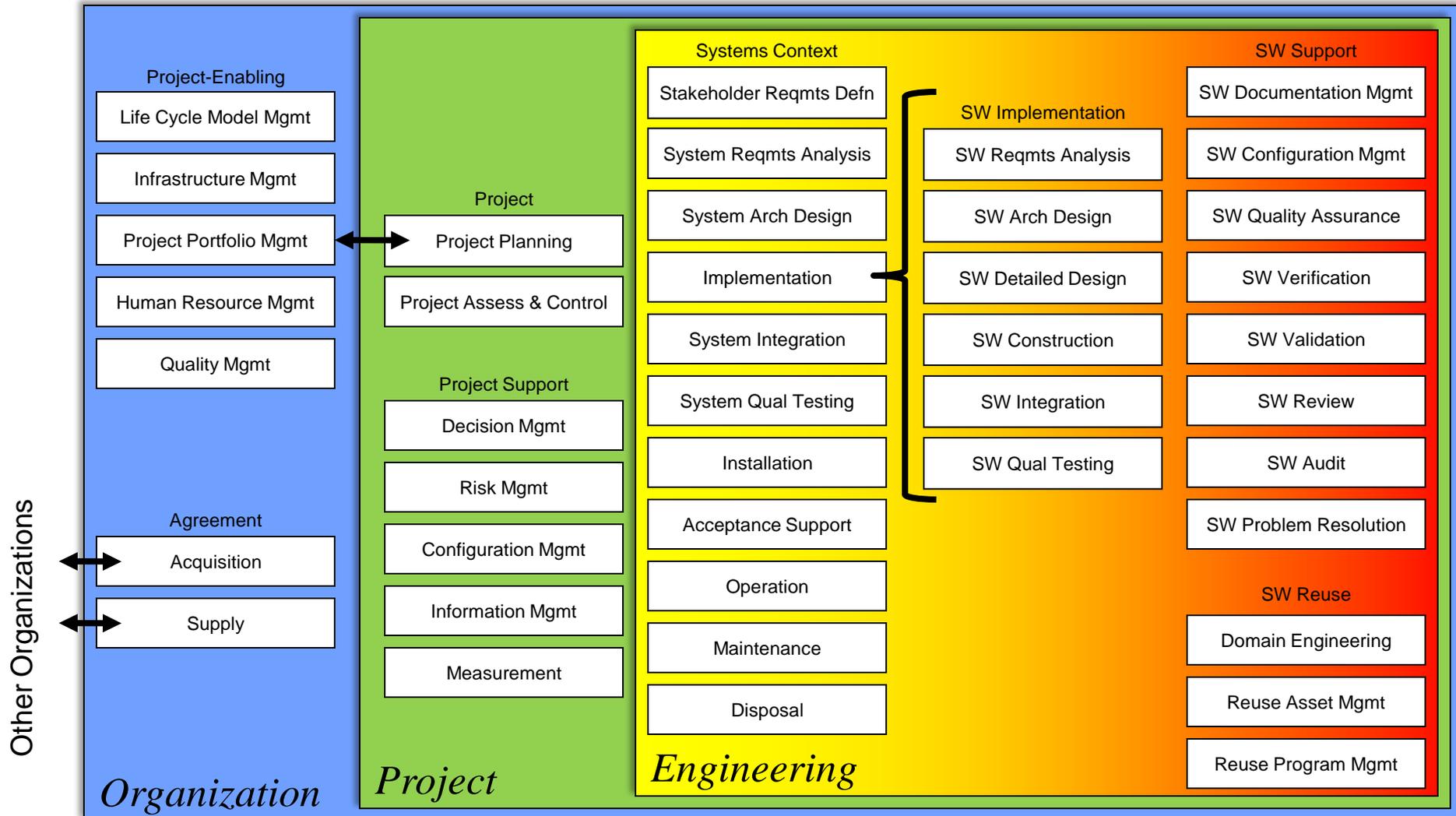
System Life Cycle Processes of 15288



- Provides all of the **Technical** processes for the entire life cycle of the system.
- Provides all of the **Project Management** processes for any stage in a system's life.
 - Provides *just enough* organizational context to enable projects.

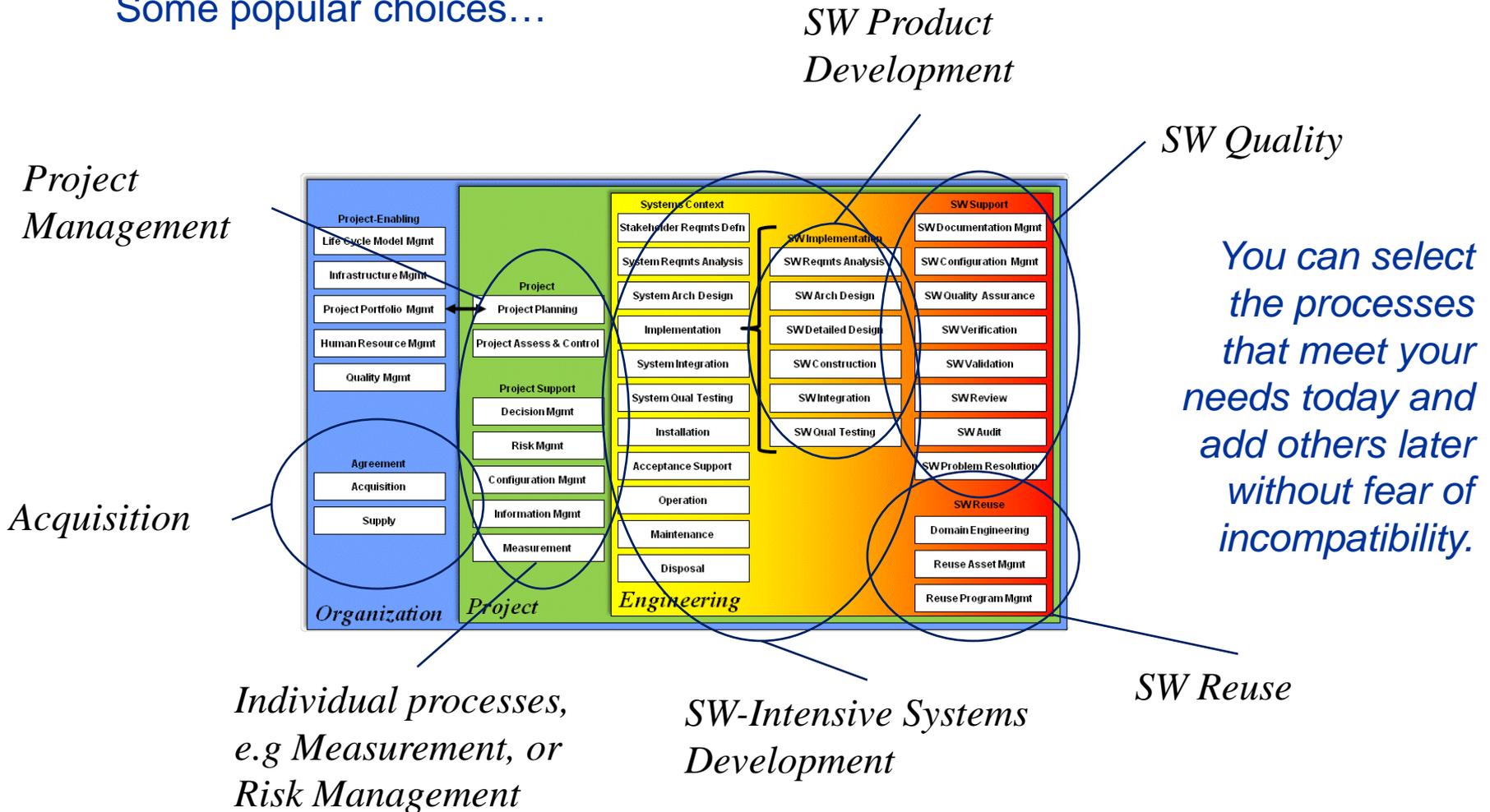
SW Life Cycle Processes of 12207

12207 specializes the processes of 15288 for software and adds software-unique processes.



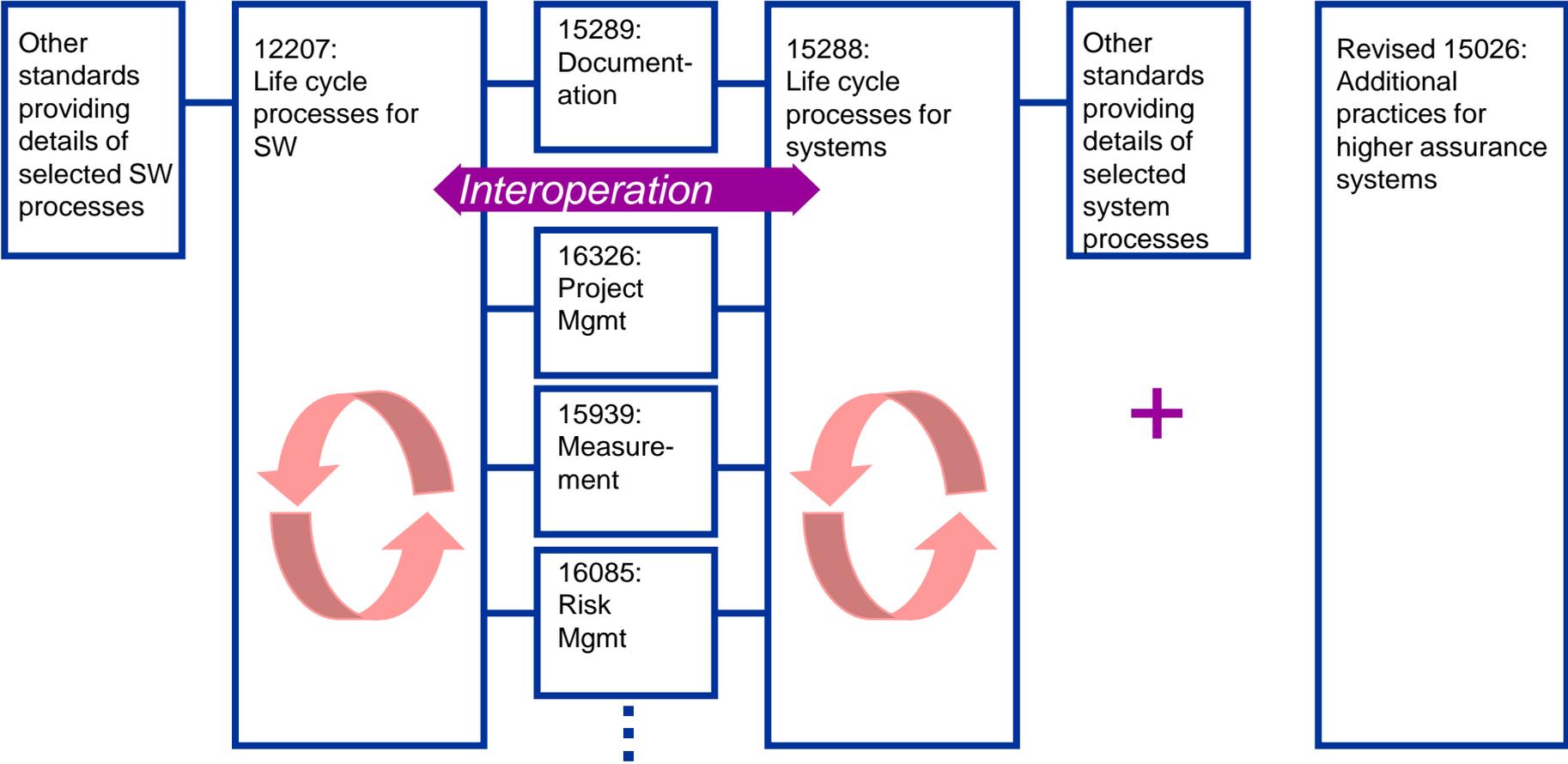
Select the Part(s) of the Standard that Makes Sense for Your Needs

Some popular choices...



Relationship of Key Life Cycle Process Standards

Draft 24748: Guide to Life Cycle Management



Draft 24765: Common vocabulary. 24774: Common process description conventions

A number of additional standards are harmonized with 12207/15228

- These standards provide a uniform context:
 - ISO/IEC/IEEE 24748-1, Guide for life cycle management
 - ISO/IEC/IEEE 24765, Vocabulary
 - Freely available at <http://www.computer.org/sevocab>
- These standards are plug-compatible and provide additional detail for selected processes:
 - ISO/IEC/IEEE 14764, Software maintenance
 - ISO/IEC/IEEE 15026, Software assurance
 - ISO/IEC/IEEE 15289, Information items (documentation)
 - ISO/IEC/IEEE 15939, Measurement
 - ISO/IEC/IEEE 16085, Risk management
 - ISO/IEC/IEEE 16326, Project management
- There are many other process standards that are generally supportive although not yet completely plug-compatible.
 - Annex F of 15288 describes the relationship of each process to 5 IEEE standards.
 - Annex G of 12207 describes the relationship of each process to 30 IEEE standards.
 - For example, IEEE Std 828, SW Configuration Management
- (All of the mentioned standards are either published or very close.)

Life cycle concepts

- Every *system* has a *life cycle* which is viewed as composed of *stages*. (The standards do not require a particular set of stages.)
 - Each stage has a purpose and makes a contribution to the life cycle.
- Stages are separated by *decision gates*.
- Stages may overlap and may be concurrent.
- The purpose of each stage is accomplished by executing *processes*.
- Any process may be useful in any stage.



A typical set of life cycle stages



- It is a common error to talk about life cycle stages when one really means processes or vice-versa.
- Locating practices with respect to processes provides much greater precision.

Life cycle processes versus life cycle phases

- It is more precise to characterize assurance activities in the context of life cycle processes rather than life cycle “phases” or “stages”.
- Some examples (from famous documents):
 - “Reduce risk to an acceptable level.”
 - Applies to all life cycle phases – initiation, development/acquisition, implementation, operation/maintenance, disposal).
 - Applies to a single life cycle process – Risk Management
 - “Clearly delineate the physical and logical security boundaries governed by associated security policies:
 - Applies to four life cycle phases (all but disposal).
 - Applies to a single life cycle process – Architectural Design
 - “Ensure that developers are trained in how to develop secure software.”
 - Applies to three life cycle phases – initiation, development/acquisition, implementation.
 - Applies to a single life cycle process – Human Resource Mgmt: Training

Assurance practices

- **Revision of ISO/IEC 15026, Systems and software assurance**
 - It provides for the assurance of any system property regarded as important enough for additional attention.
 - It posits an assurance case – an explicit evidence-based argument for a claim that the property has been achieved.
- **15026-1: Vocabulary and concepts**
- **15026-2: Assurance case**
 - It specifies the structure of an assurance case.
 - It provides common nomenclature for practices that are already used in high-assurance industries but have differing names.
- **15026-3: Criticality levels**
- **15026-4: Assurance in the life cycle**

What SC 7 provides

- **The systems engineering and software engineering context for specific practices related to safety, security, or any other important property.**
- **A set of life cycle processes that can be used to localize good practices.**
- **The structure of an assurance case supporting direct argument that a property has been achieved.**