



Safety Critical Software Configuration Management Practices

Linda Westfall
Westfall Team, Inc.

International Conference on
Software Quality – ICSQ 2011

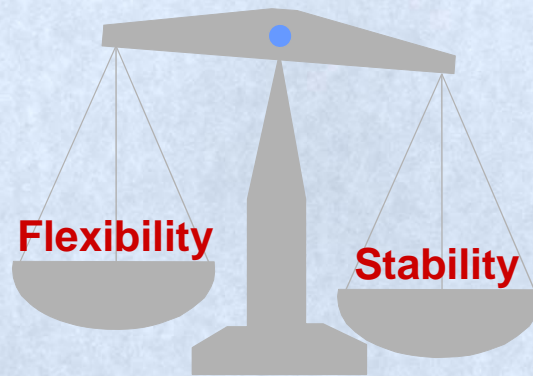
Configuration Management Defined

**A discipline applying technical & administrative
direction & surveillance to:**

- Identify & document the functional & physical characteristics of a configuration item
- Control changes to those characteristics
- Record & report change processing & implementation status
- Verify compliance with specified requirements

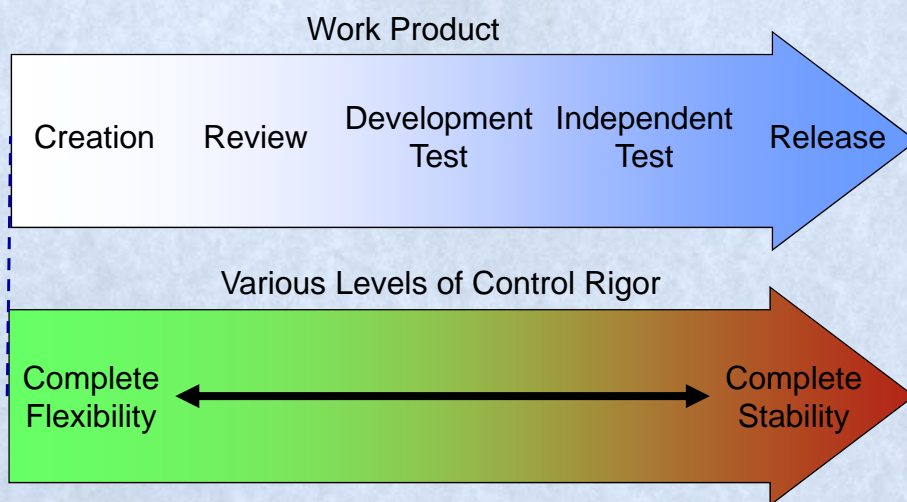
[ISO/IEC 24765]

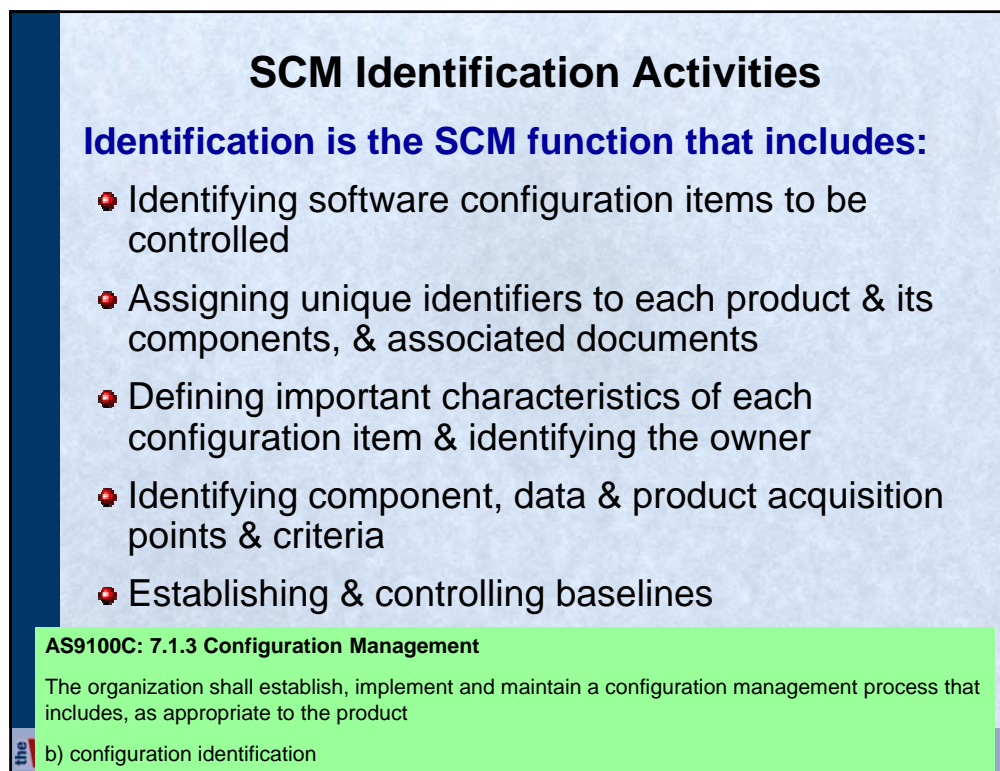
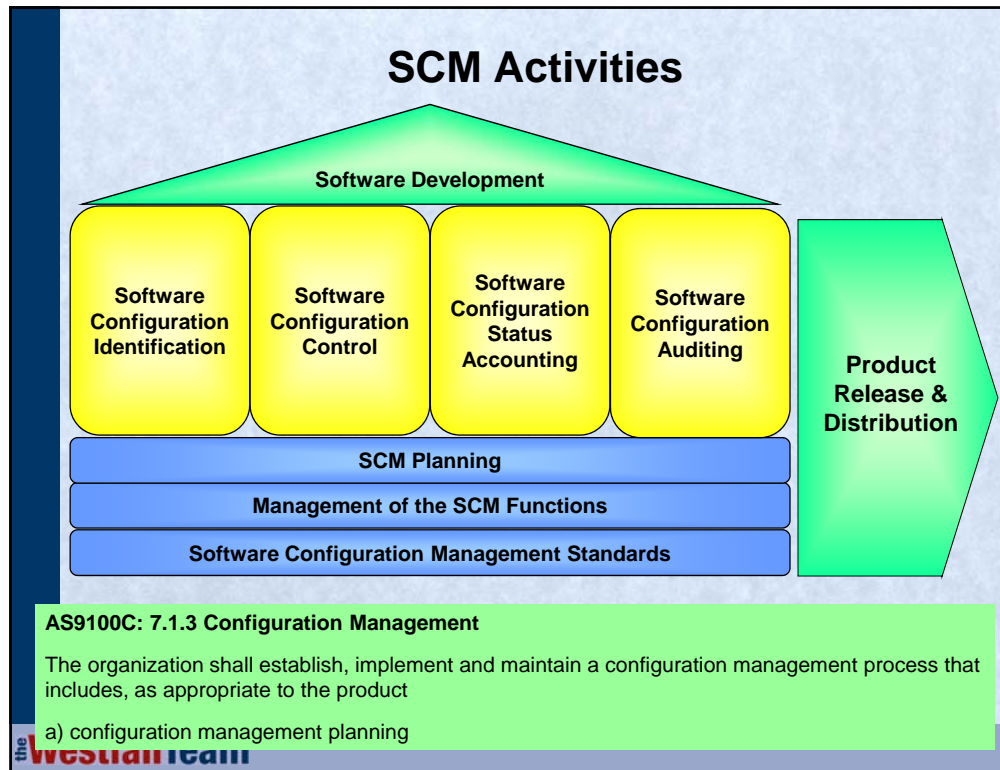
SCM Maintains a Balance



“Software configuration management is necessary to enable large teams to work together in a stable environment, yet still have the flexibility that’s needed to do creative work.”

The Good News – It’s Not All or Nothing





What Are Configuration Items?

Configuration item:

- A work product placed under configuration management & treated as a single entity
- “A collection of hardware or software elements treated as a unit for the purpose of configuration control” [NQA-1a]

the WestfallTeam

Selecting Configuration Items

The following items should be placed under configuration management:

- Externally delivered software products & data
- Designated internal software work products & data
- Designated support tools used to create or support the software product
- Supplier/vendor supplied software
- Customer supplied equipment/software

NQA-1a: Subpart 2.7 Quality Assurance Requirements for Computer Software for Nuclear Facility Applications

203 Software Configuration Management: “Configuration items to be controlled shall include, as appropriate:

1. documentation (e.g., software design requirements, instructions for computer program use, test plans, and results);
2. computer programs (e.g., source, object, back-up files); and
3. support software.

the W

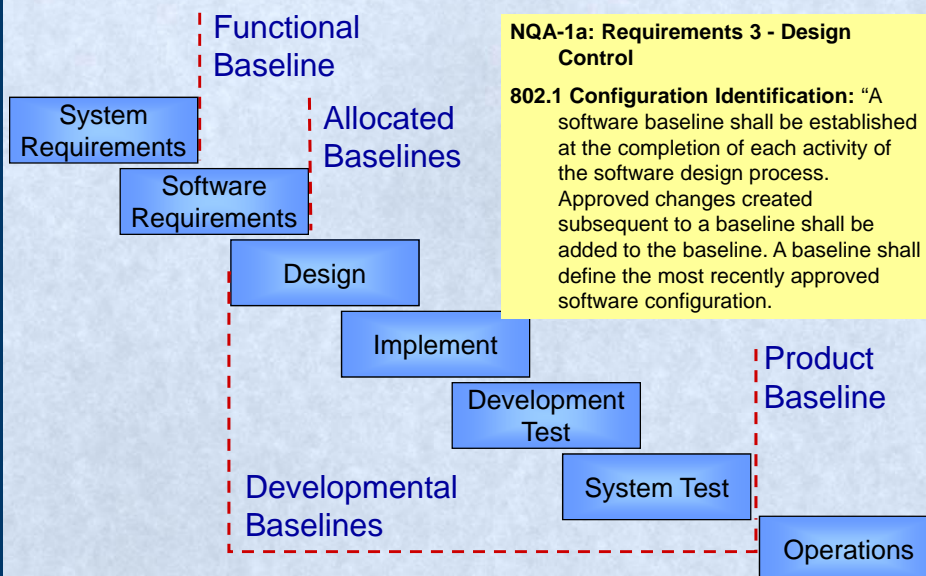
Baseline Defined

1. “A specification or product that has been formally reviewed & agreed upon, that thereafter serves as the basis for further development, & that can be changed only through formal change control processes” [NQA-1a]
2. A document or set of such documents formally designated & fixed at a specific time during the life cycle of a configuration item

Baselines identify how software entities:

- Are related to each other
- Are related to software life cycle milestones

Types of Baselines



Baselines

Baselines should be defined for specific control points in the life cycle.

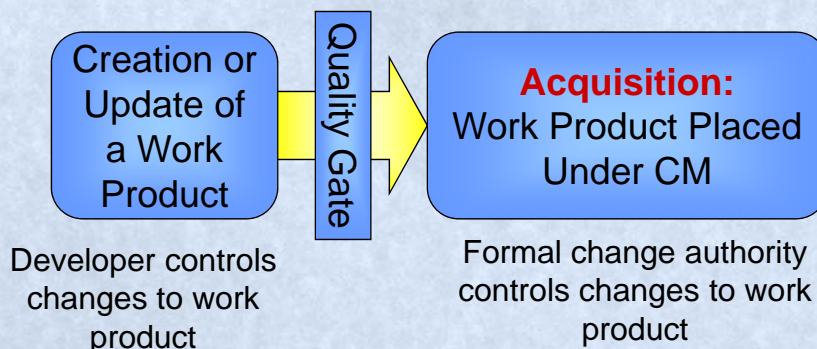
For each baseline, this definition includes:

- Event that creates the baseline
- Items controlled
- Procedures for establishing & changing the baseline
- Authority required to approve changes to the baseline

the **WestfallTeam**

Acquisition

“One critical aspect for control of work products is the proper timing for when they enter into configuration management.” [SPMN-98]



the **WestfallTeam**

Assigning Unique Identifiers

SCM provides a way to uniquely identify each:

- Revision, version & release
- Document
- Software component (source code module, data)
- Baseline

NQA-1a: Requirements 3 - Design Control

802.1 Configuration Identification (cont.): "A labeling system for configuration items shall be implemented that:

- a) uniquely identifies each configuration item;
- b) identifies changes to configuration items by revision; and
- c) provides the ability to uniquely identify each configuration of the revised software available for use."

ISO 13485-2003: 7.5.3.1 Identification

The organization shall identify the product by suitable means throughout product realization and shall establish documented procedures for such product identification.

the Westfall Team

Configuration Control Requirements

NQA-1a: Requirements 3 - Design Control

802.2 Configuration Control: "Changes to software shall be formally documented. The documentation shall include:

- a) a description of the change;
- b) the rationale for the change; and
- c) the identification of affected software baselines.

The change shall be formally evaluated and approved by the organization responsible for the original design, unless an alternate organization has been given the authority to approve the changes. Only authorized changes shall be made to software baselines. Appropriate verification activities shall be performed for the change. The change shall be appropriately reflected in documentation and traceability of the change to the software design requirement shall be maintained. Appropriate acceptance testing shall be performed for the change."

NQA-1a: Subpart 2.7 Quality Assurance Requirements for Computer Software for Nuclear Facility Applications

203 Software Configuration Management (cont.): "The software configuration change control process shall include:

1. initiation, evaluation, and disposition of a change request
2. control and approval of changes prior to implementation; and
3. requirements for retesting and acceptance of the test results

the Westfall Team

Configuration Control Requirements

ISO 13485-2003: 7.3.7 Control of design and development changes

Design and development changes shall be identified and records maintained. The changes shall be reviewed, verified, and validated, as appropriate, and approved before implementation. The review of design and development changes shall include evaluation of the effect of the changes on constituent parts and product already delivered.

AS9100C: 7.1.3 Configuration Management

The organization shall establish, implement and maintain a configuration management process that includes, as appropriate to the product

c) change control

AS9100C: 7.3.7 Control of Design and Development Changes

Design and development changes shall be controlled in accordance with the configuration management process.

AS9100C: 7.6 Control of Monitoring and Measuring Equipment

NOTE: Confirmation of the ability of computer software to satisfy the intended application would typically include its verification and configuration management to maintain its suitability for use.

the **WestfallTeam**

What is Configuration Control?

The systematic process that ensures that changes to a baseline are:

- Properly identified
- Documented
- Evaluated for impact
- Approved by an appropriate level of authority
- Incorporated
- Verified

the **WestfallTeam**

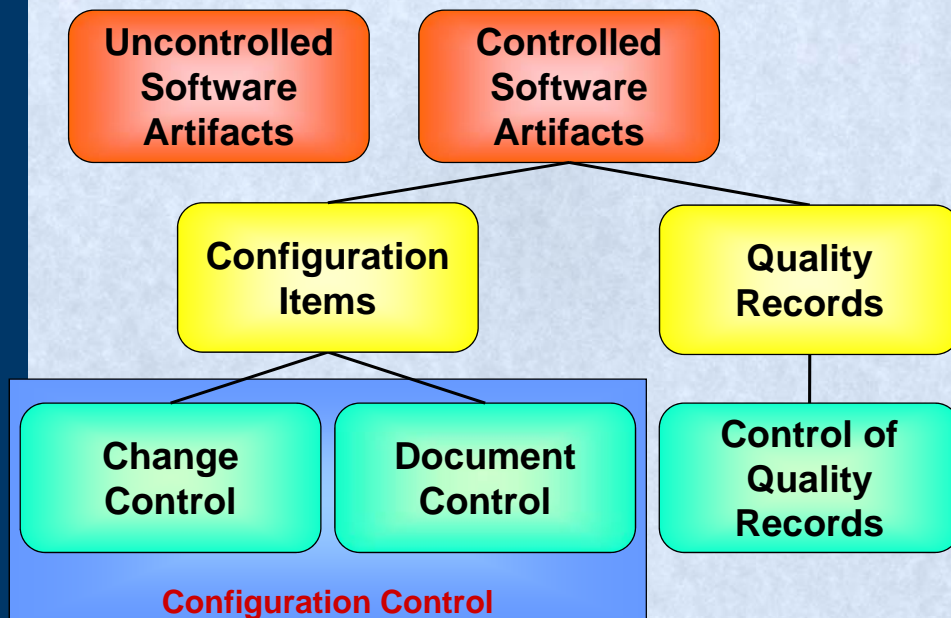
Configuration Control

The configuration control process must answer these questions:

- When is control initiated?
- By what means is an entity placed under control?
- What is the control process?
 - Levels of control each work product passes through
 - Change authority at each level
 - Procedure for obtaining authorization for changes
 - Procedure for implementing & verifying change

the WestfallTeam

Controlled Software Artifacts



the WestfallTeam

Configuration Control Procedures

Configuration control procedures include:

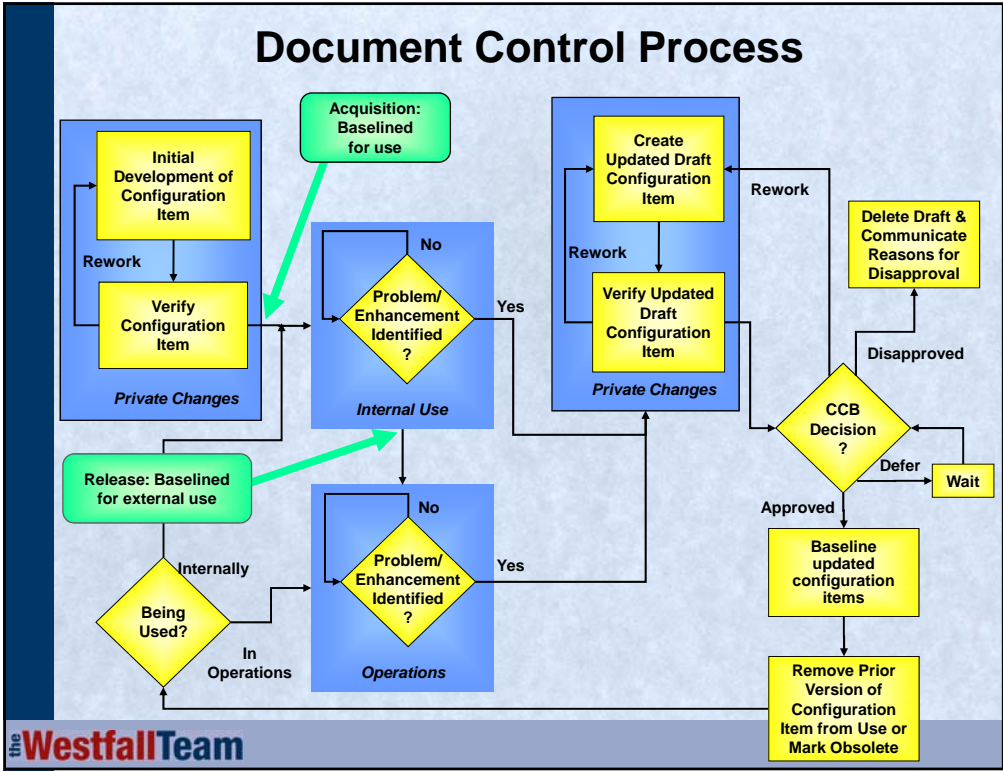
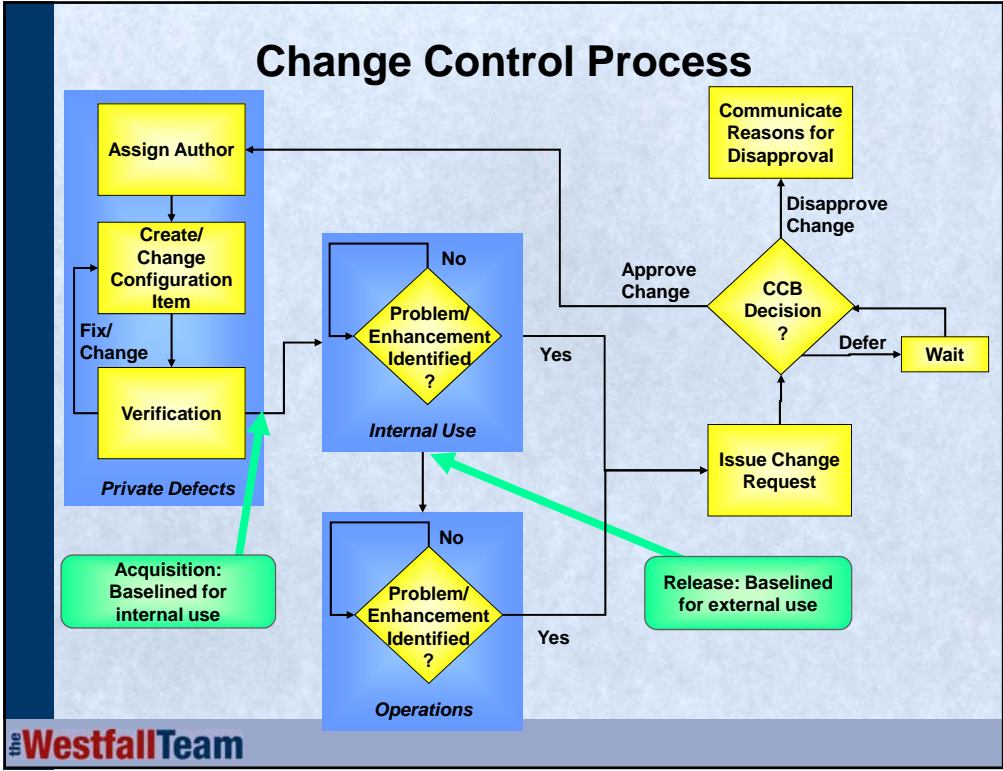
- ◆ Mechanisms for requesting & documenting changes to controlled work products
- ◆ Requirements for performing impact analysis for each requested change
- ◆ Mechanisms for informing affected stakeholders of the change request & soliciting their input to impact analysis
- ◆ An authority exists for making decisions on accepting or rejecting change request

the WestfallTeam

Configuration Control Procedures (cont.)

- ◆ Mechanisms for informing affected stakeholders of the decision to accept or reject the change & for obtaining their commitment to the change if it is accepted
- ◆ Mechanisms for tracking requested changes from submission through final disposition (rejection or completion of the change)
- ◆ Mechanism for verifying the change

the WestfallTeam



Configuration Control Board (CCB)

A Configuration Control Board (CCB) is beneficial because it:

- Provides authority
- Ensures change authorization before implementation
- Provides visibility in change control process
- Provides a vehicle for impact analysis
- Facilitates resource allocation
- Plays an integral role in keeping the software development process under control

the **WestfallTeam**

Multiple Levels of CCBs - Examples

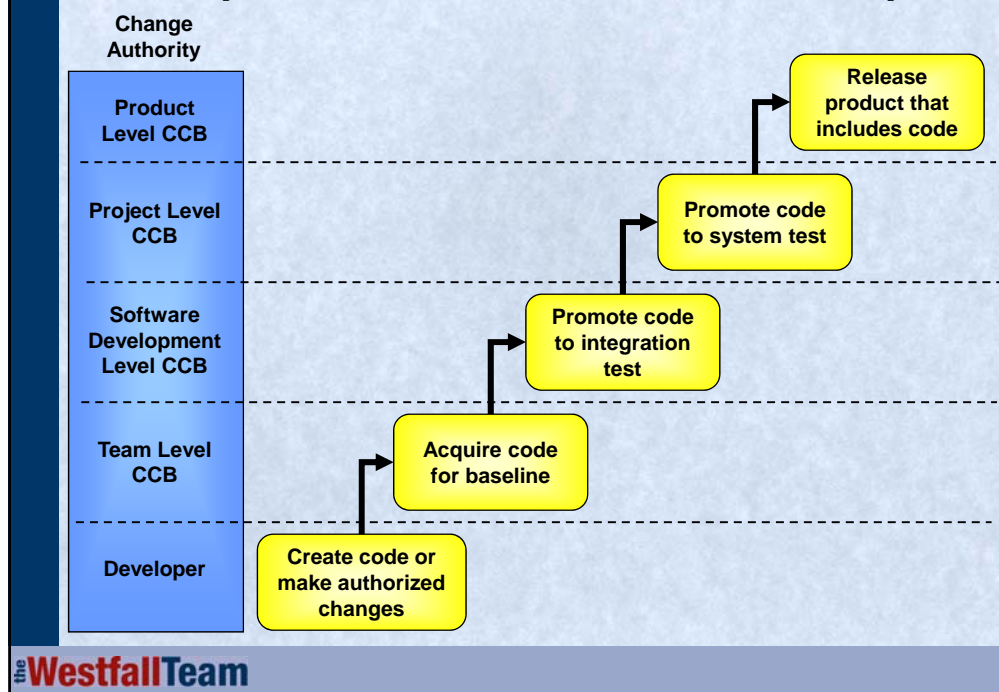
Different levels of CCBs can be used to balance between the need for control & the need to streamline the change process.

Examples include:

- System/product level CCB controls changes to the functional baseline & product baseline
- Subsystem level CCBs control changes to the allocated baselines
- Software development level CCBs control changes to the developmental baselines

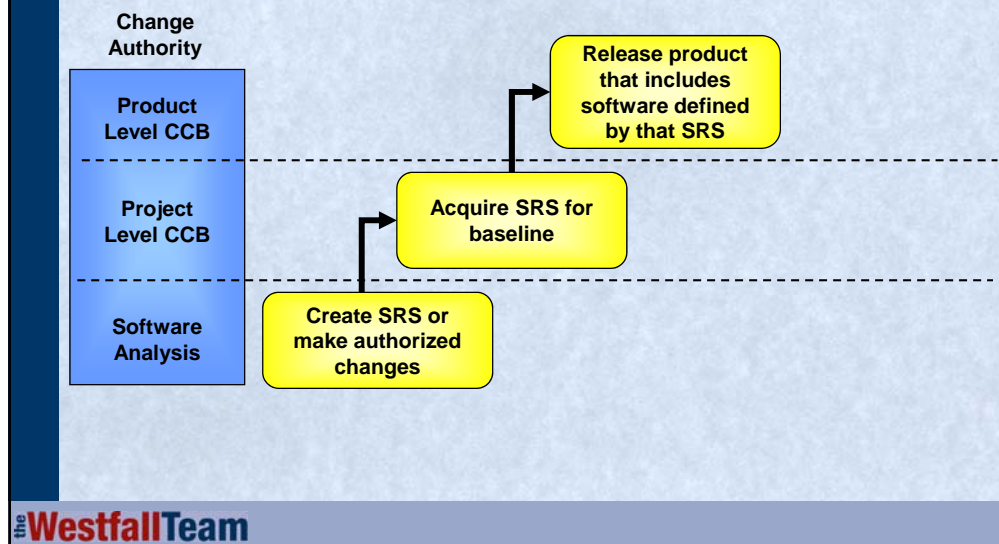
the **WestfallTeam**

Multiple Levels of CCBs – Code Example

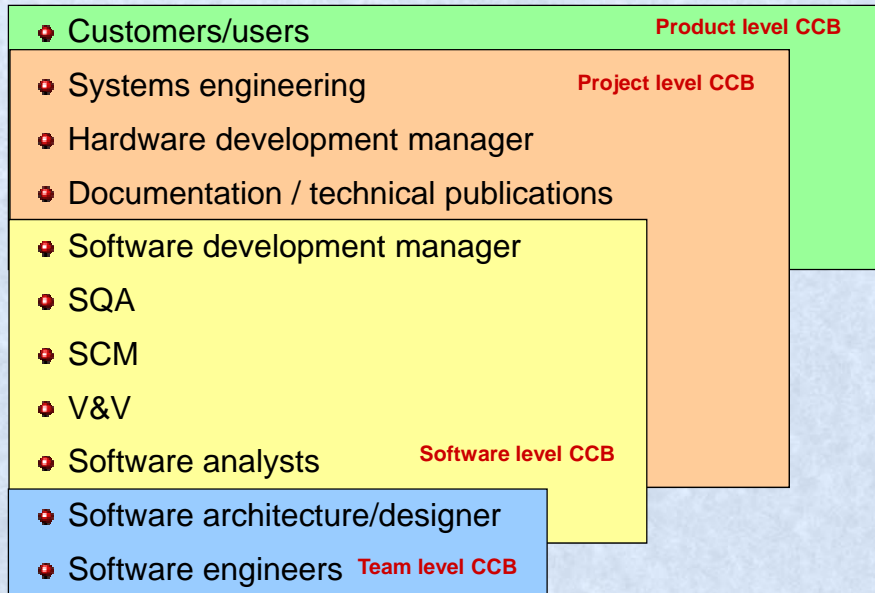


Multiple Levels of CCBs – SRS Example

Software Requirements Specification (SRS) example:



CCB Membership - Examples



the WestfallTeam

Impact Analysis Checklist

Items to consider include:

- Size & complexity of the change
- Severity of the change
- Schedule impacts
- Cost impacts
- Effort impacts
- Technical impacts
- Relationships to other changes
- Testing requirements
- Benefits of the change

the WestfallTeam

Backward Traceability & Impact Analysis



ISO 13485-2003: 7.5.3.2 Traceability (7.5.3.2.1 General)

The organization shall establish documented procedures for traceability. Such procedures shall define the extent of product traceability and the records required.

Where traceability is a requirement, the organization shall control and record the unique identification of the product.

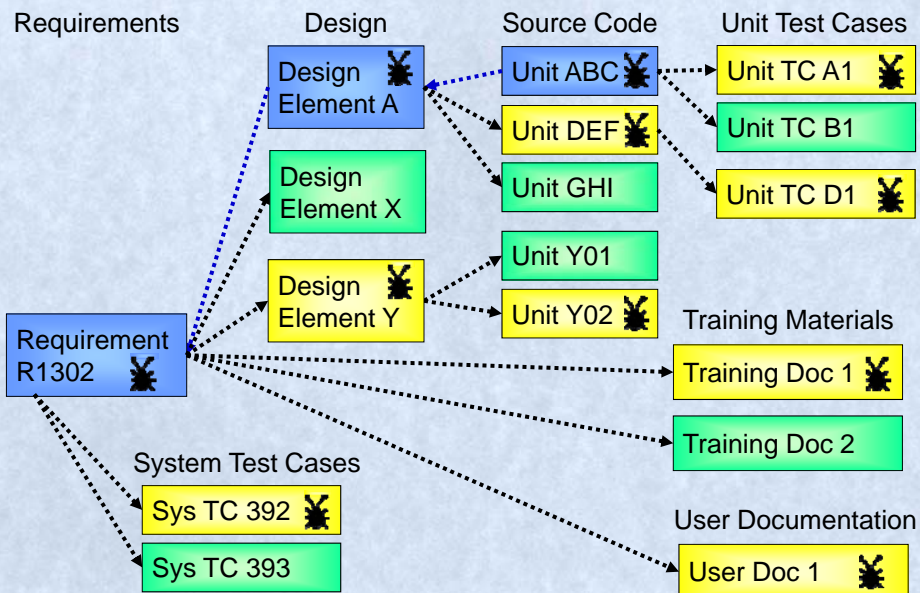
NOTE—Configuration management is a means by which identification and traceability can be maintained.

AS9100C: 7.5.3 Identification and Traceability

NOTE In some industry sectors, configuration management is a means by which identification and traceability are maintained

the WestfallTeam

Forward Traceability & Impact Analysis



the WestfallTeam

Status Accounting Requirements

NQA-1a: Requirements 3 - Design Control

802.3 Configuration Status Control: "The status of configuration items resulting from software design shall be maintained current. Configuration item changes shall be controlled until they are incorporated into the approved product baseline. The controls shall include a process for maintaining the status of changes that are proposed and approved, but not implemented. The controls shall also provide for notification of this information to affected organizations."

ISO 13485-2003: 7.3.7 Control of design and development changes

Records of the results of the review of changes and any necessary actions shall be maintained.

AS9100C: 7.1.3 Configuration Management

The organization shall establish, implement and maintain a configuration management process that includes, as appropriate to the product

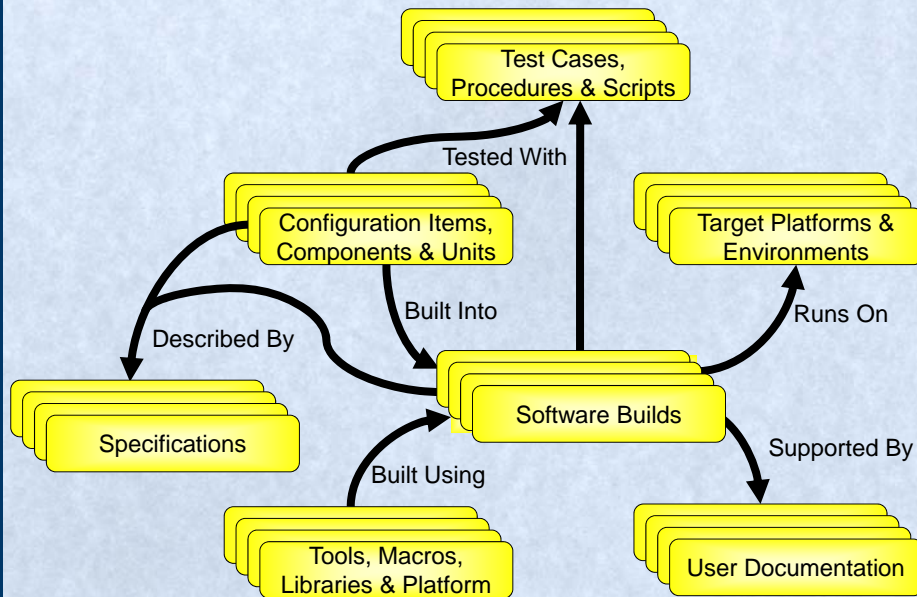
d) configuration status accounting

Status Accounting

The configuration status tracking system should keep track of:

- Product description records
- Status of each controlled software component
- Contents & status of each build/release
- Contents of each baseline
- Configuration verification records
- Change status records (defects & enhancements)
- Installation status of all configuration items at all locations

Configuration Item Dependencies



the WestfallTeam

Functional Configuration Audits

Audits conducted to verify that:

- The development of a configuration item has been completed satisfactorily
- The item has achieved the performance & functional characteristics specified
- Its operational & support documents are complete & satisfactory

AS9100C: 7.1.3 Configuration Management

The organization shall establish, implement and maintain a configuration management process that includes, as appropriate to the product

e) configuration audit

the WestfallTeam

[ISO/IEC 24765]

Conducting a Functional Configuration Audit

The functional configuration audit includes:

- An audit of the formal test documentation against test data
- An audit of the verification & validation reports
- A review of all approved changes
- A review of updates to previously delivered documents
- A sampling of design review outputs
- A comparison of code with documented requirements
- A review to ensure all testing was accomplished

The FCA may include additional sample testing.

Physical Configuration Audits

Audits conducted to verify that:

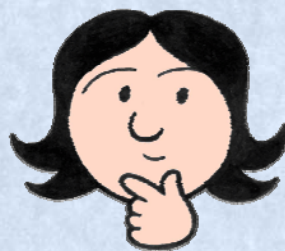
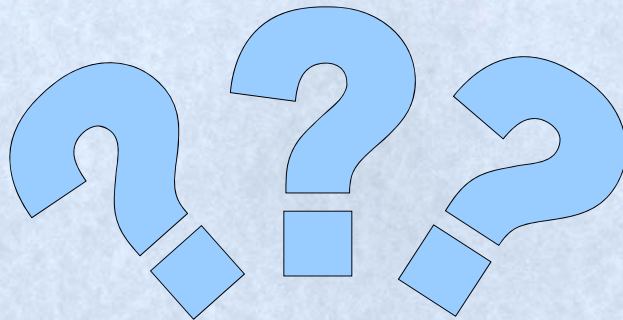
- A configuration item, as built, conforms to the technical documentation that defines it
 - All items identified as being part of the configuration are present in the product baseline
 - The correct version & revision of each part are included in the product baseline
 - They correspond to information contained in the baseline's configuration status report

Conducting a Physical Configuration Audit

The physical configuration audit includes:

- An audit of the system specification for completeness
- An audit of the FCA report for discrepancies & actions taken
- A comparison of the architectural design with the detailed design components for consistency
- A review of the module listing for compliance with approved coding standards
- An audit of the manuals for format completeness & conformance to systems & functional descriptions

Questions?



Contact Information



Linda Westfall
3000 Custer Road
Suite 270, PMB 101
Plano, TX 75075-4499

phone: (972) 867-1172

fax: (972) 943-1484

email: lwestfall@westfallteam.com

www.westfallteam.com

the WestfallTeam