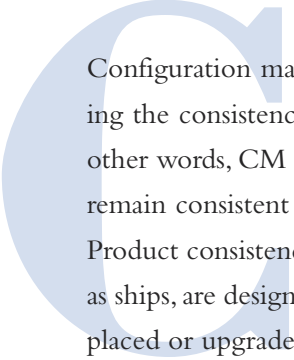


Configuration Management Best Practices

By Denise Duncan and Al Lager



Configuration management (CM) is a systematic process for establishing and maintaining the consistency of a product—such as a part or component—throughout its life. In other words, CM ensures that a product’s functional performance and physical attributes remain consistent with its design and operational requirements throughout its life cycle. Product consistency is particularly important for DoD, because many of its systems, such as ships, are designed to be used for decades. Parts and components, however, must be replaced or upgraded periodically.

Possibly the first user of CM in the production of U.S. military equipment was Eli Whitney (the inventor of the cotton gin). In 1798, he started a business to manufacture muskets for the Army. He used an innovative technique to revolutionize the manufacturing process. Specifically, he fabricated interchangeable parts rather than fabricating one complete musket at a time. This approach would not have worked without employing this rudimentary form of configuration control, a major function of what we now know as configuration management.

Over time, CM practices have evolved, and DoD’s guidance has evolved along with them. The current version of DoD 5000.02¹ requires program managers (PMs) to

use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle. This approach will identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; be integrated with the Systems Engineering Plan and technical planning; and be consistent with the Intellectual Property Strategy.

A wide variety of guidance is available to help PMs implement a successful CM program. That guidance is contained in standards, handbooks, and tools, such as the following:

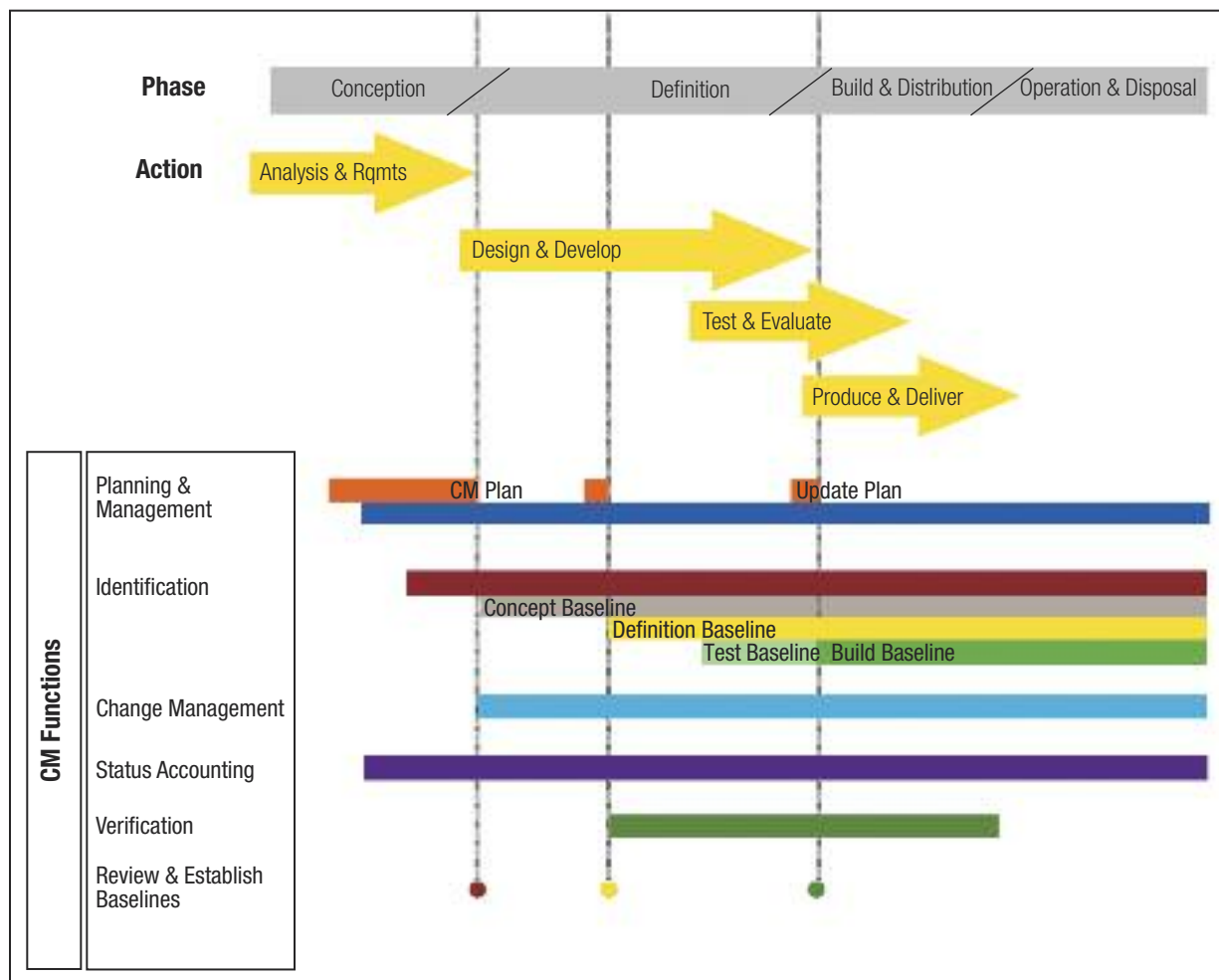
- EIA-649-B, “National Consensus Standard for Configuration Management”
- GEIA-HB-649A, *Implementation Guide for Configuration Management*
- EIA-649-1, “Configuration Management Requirements for Defense Contracts”
- MIL-HDBK-61A, *Configuration Management Guidance*
- EIA-836, “Configuration Management—Data Exchange and Interoperability”
- MIL-STD-961, “Defense and Program-Unique Specifications Format and Content”
- MIL-STD-31000A, “Technical Data Packages”
- *Configuration Management Advisor*, an online resource maintained by the Naval Air Warfare Center, Training Systems Division
- *Acquisition Community Connection*, an online resource, including a Configuration Management Plan Template, maintained by the Defense Acquisition University.

This article summarizes best practices from successful, experienced configuration managers, organized by five functions inherent in CM:

- CM planning and management
- Configuration identification
- Configuration change management
- Configuration status accounting
- Configuration verification and audit.

All five CM functions are necessary to some degree for all products. A robust CM approach is required for a complex product, such as an electronic system, a military weapon, or other product that must be supported over the product's complete life cycle. Figure 1 shows how CM works across the product life cycle. Simpler CM techniques may be used for a noncomplex product as long as they maintain the needed consistency between essential requirements, product configuration information, and the product.

Figure 1. CM across the Product Life Cycle



CM Planning and Management

From the early phases of the product life cycle, the PM and the configuration manager must determine the appropriate application of CM functions throughout the product life cycle. By identifying the context and environment of the product, they can appropriately tailor the application of CM based on things like the product requirements, complexity, and life-cycle environment.

A best practice for this CM function is to prepare a CM plan that reflects the efficient application of CM principles and practices over the product's life cycle. The CM plan should cover the following topics:

- General product definition and scope
- Description of CM activities and procedures for each major CM function
- Organization, roles, responsibilities, and resources
- Definitions of terms
- Programmatic and organizational interfaces
- Deliverables, milestones, and schedules
- Subcontract flow-down requirements.

Configuration Identification

Configuration identification is the process of identifying and documenting the attributes (functional and physical characteristics) of items that are to be placed under configuration control. Configuration identification includes the selection (identification) of configuration items (CIs), including computer software configuration items (CSCIs); determining the types of configuration documentation required for each CI/CSCI; assigning unique identifiers to each CI/CSCI and the technical documentation describing its configuration; and the establishment of configuration baselines. A hierarchical structure should be established that identifies and summarizes the CIs/CSCIs constituting a given project, product, or automated system.

To perform this function, the configuration manager must establish the product structure, determine and document the configuration items, and define the item identification scheme, that is, what characters or markings will be used and how they will be assigned to configuration items, their subordinate parts, and their associated documents.

One of the best practices in this CM function is to ensure that the identification scheme covers both developmental and final versions of configuration items, including hardware, software, documents, and procedures. The scheme must relate items at lower levels in the hierarchy to the items at which requests for change will be addressed (i.e., configuration items), and it must address the effect on associated CIs, support, training,

and maintenance equipment, as well as on associated electronic media, computer files, documents, and software components. In addition, the scheme should include version, revision, and other important status information about each item.

An important best practice in software CM is to ensure that products delivered to the customer are all placed under CM. This includes software requirements, software design, code, build scripts, software test procedures and documents, and any items that are identified with or required to create, test, operate, and maintain the software products, such as the compiler, vendor-supplied/government-furnished information, and so on.

Configuration Change Management

Change management (also called configuration control) consists of the evaluation, coordination, approval or disapproval, and implementation of changes to CIs/CSCIs after they are formally baselined. Effective change management depends on placing products under control by employing mechanisms that ensure proposed changes are properly identified, prioritized, documented, coordinated, evaluated, and adjudicated.

Once a change is approved, it must be fully documented, implemented, verified, and monitored to ensure its incorporation in all applicable systems and products. Changes identified during ongoing maintenance of products or systems in operation or production cycle forward into new requirements for appropriate analysis and entry into the change management process. In other words, they become new requests for change.

A change (or configuration) control board (CCB) is the preferred forum both for establishing CM baselines and for approving/disapproving subsequent changes to those baselines. A CCB may exist at the enterprise (customer and contractor) level, project level, or both, as defined in its charter and operating procedures.

One of the best practices in this CM function is to design the change evaluation and coordination process to be repeatable and to cover a wide variety of proposed changes. For example, the process should consider things such as the following:

- Cost or savings to both the supplier and customer
- Current work scope and schedules affected
- Design, development, and test effort involved
- Product documentation revision or replacement required
- Effects on warranty and other contractual considerations, delivered product (e.g., whether it requires recall, retrofit, replacement), spare/replacement parts, and environmental considerations
- Modifications required in manufacturing, assembly, installation, test, and operating or maintenance instructions

- Modifications required to training devices and training materials
- Effects on the performance or on the functional and physical interfaces with other products.

Another best practice is to institute a process to ensure that changes to a CI are complete and that the changes have not introduced any unanticipated issues. This is often part of a change verification process that includes verifying the consistency of the product, documentation, operation/maintenance information, interfaces, and training after change completion.

Configuration Status Accounting

Configuration status accounting is the function of reporting the current state of a system (or any configuration) efficiently, accurately, and quickly. The data for status accounting are a product of many systems—those used for project management, engineering, manufacturing, quality assurance, release, change control, logistic support organizations, and the customers. In an optimal CM system, these data are easily extracted, correlated, and maintained for status accounting in a database. Ideally, configuration status accounting data are a byproduct of these other systems. For example, in software configuration management, status accounting data are the result of baselining software versions, providing library control, and executing change management for software and its documentation.

For this CM function, configuration managers should implement two key best practices:

- Design configuration data and the CM database for integration with other systems in the enterprise, from finance to engineering, manufacturing, release management, and maintenance.
- Design CM data capture to provide visibility and traceability of the product configuration and the status of release of new product configuration information.

Configuration Verification and Audit

This CM function ensures, through formal functional and physical configuration audits, that a product's specified verification requirements—including tests, demonstrations, inspections, and analyses—have been met. The functional configuration audit (FCA) systematically compares requirements with the results of specified verifications. The physical configuration audit (PCA) determines whether the product is consistent with its design documentation.

This CM function also ensures that the content of the CM database is accurate. Operational systems must be validated periodically to ensure consistency between the in-use

product and its current baseline documentation. A critical function of this activity is verification of the incorporation of modifications.

The audit process has three phases: planning and preaudit preparation, execution of the configuration audit, and postaudit follow-up and closeout. Planning is as important as the audit itself. Planning is considered effective if

- audit requirements are consistent with the acquisition strategy and
- the audit schedule, or agenda, is keyed to program events and the availability of items, information, and personnel, resulting in
 - ❖ approved functional/allocated configuration documentation;
 - ❖ FCA prior to or concurrent with PCA, following CI/CSCI verification testing;
 - ❖ PCA conducted on an article in production (operational) configuration;
 - ❖ incremental hardware PCAs shadowing the assembly or test sequence; and
 - ❖ software PCA after integration testing.

The audit plan and agenda should address the following:

- Location and dates for each audit
- Composition of the audit team—government, contractor, subcontractor—and the team members' functions in the audit
- Identification of government, contractor, and subgroup chairpersons
- Documentation to be available for review
- Chronological schedule for conduct of the audit
- CIs/CSCIs to be audited and specific units to be audited
- Documentation to be audited and reference material
- Detailed information pertinent to the audit, for example, team requirements, facility requirements, administrative information, and security requirements.

Overall CM Best Practices

To summarize, PMs and configuration managers can ensure a successful CM program by applying the following best practices:

- Understand and use a comprehensive guide to CM, such as the DoD-adopted standard (EIA-649-B) and its handbook (GEIA-HB-649A) or MIL-HDBK-61A to implement CM. Both contain examples and tools for robust CM methods; for example, MIL-HDBK-61A has activity guides showing who does what for each CM function.
- Design metrics for the CM processes and build them into the CM system, including the supply chain.

- Plan for the business context and plan CM activities based on program milestones. This CM planning should begin with the request for proposals for the product.
- Train the CM staff and cross-train personnel in functions that integrate with CM; better understanding and integration from other functions are the secret to passing any audit. Trained personnel become resources for backup and for succession planning.
- Use a CM standard (for example, the principles in EIA-649-B) as an assessment tool for evaluation and troubleshooting.
- During incremental supplier configuration verification and audits, ensure that CM requirements flow down the supply chain.

¹Interim DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” November 25, 2013.

About the Authors

Denise Duncan is a senior fellow at LMI with 30 years of information systems management experience. She has managed a wide variety of projects, from assisting senior leaders with portfolio management to strategic planning for chief information officers. For the last 10 years, Ms. Duncan has worked extensively on the application of data management (DM) principles to engineering and scientific data. She has authored standards, handbooks, and training materials in enterprise-level DM and information management. Ms. Duncan has been honored as a technical fellow of TechAmerica and is the vice president for programs in the local chapter of Data Management Association—International.

Al Lager has been an industry spokesperson on military standards concerning CM, DM, and related topics since the early 1970s and has chaired working groups responsible for ANSI/EIA industry consensus standards for CM, DM, data interoperability, and exchange. Among other things, he served as the team leader and principal author of EIA-649, “National Consensus Standard for Configuration Management,” and principal editor of EIA-649-B; represented industry on DoD’s Configuration Management Advisory Group; authored MIL-HDBK-61 and 61A, *Configuration Management Guidance*; and served as industry team leader for EIA-836, “Configuration Management—Data Exchange and Interoperability.” ❀