HOW CONFIGURATION MANAGEMENT WORKS WITH QUALITY TO ENSURE MISSION SUCCESS

Presented by Jeffrey Parnes

to ASQ 0511

Northern Virginia Section

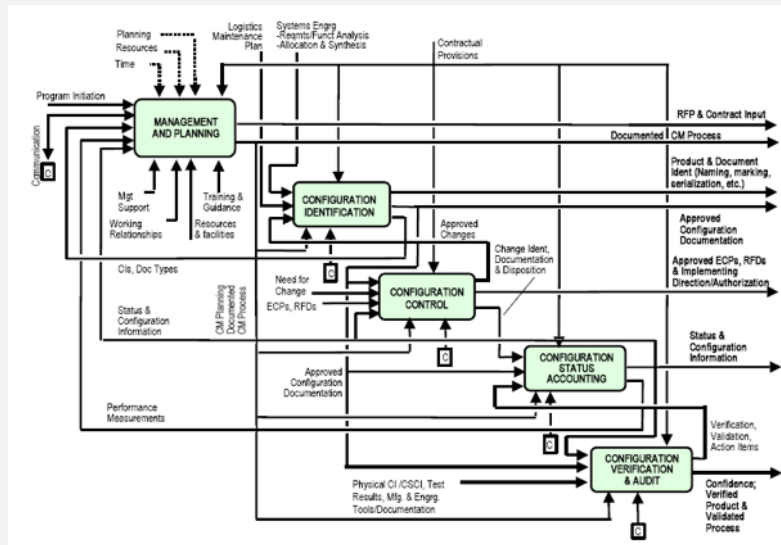8 July 2020

WHAT IS CONFIGURATION MANAGEMENT (CM)?

- CM is the practice of handling changes systematically so that a system maintains its integrity over time.

- CM implements the policies, procedures, techniques, and tools that manage, evaluate proposed changes, track the status of changes, and maintain an inventory of system and support documents as the system changes.

- CM programs and plans provide technical and administrative direction to the development and implementation of the procedures, functions, services, tools, processes, and resources required to successfully develop and support a complex system.

- During system development, CM allows program management to track requirements throughout the life-cycle through acceptance and operations and maintenance. As changes inevitably occur in the requirements and design, they must be approved and documented, creating an accurate record of the system status. Ideally the CM process is applied throughout the system lifecycle

CONFIGURATION MANAGEMENT HISTORY

- Configuration Management originated in the US DoD in the 1950s as a technical management discipline for hardware material items—and it is now a standard practice in virtually every industry.

- The CM process became its own technical discipline sometime in the late 1960s when the DoD developed a series of military standards called the "480 series" (i.e., MIL-STD-480, MIL-STD-481 and MIL-STD-483) that were subsequently issued in the 1970s. In 1991, the "480 series" was consolidated into a single standard known as the MIL–STD–973 that was then replaced by MIL–HDBK–61 pursuant to a general DoD goal that reduced the number of military standards in favor of industry technical standards supported by standards developing organizations.

- This marked the beginning of what has now evolved into the most widely distributed and accepted standard on CM, ANSI–EIA–649–1998. Now widely adopted by numerous organizations and agencies, the CM discipline's concepts include systems engineering (SE), Integrated Logistics Support (ILS), Capability Maturity Model Integration (CMMI), ISO 9000, Prince2 project management method, COBIT, Information Technology Infrastructure Library (ITIL), product lifecycle management, and Application Lifecycle Management.

- Many of these functions and models have redefined CM from its traditional holistic approach to technical management. Some treat CM as being similar to a librarian activity, and break out change control or change management as a separate or stand alone discipline.

ELEMENTS OF CONFIGURATION MANAGEMENT

- Configuration Management Planning and Management A configuration management plan (CMP) describes any project specific procedures and the extent of their application

- Configuration Identification (CI): Involves breaking down the project and creating a referencing system for each item.

- Configuration Control: Ensures that all changes to configuration items are controlled. Configuration control of specifications and test plans is vital for quality control to be effective.

- Configuration Status Accounting (CSA): Provides records and reports that relate to a deliverable and its configuration information.

- Configuration Verification Audit (CA): Determines whether a deliverable conforms to its requirements and configuration information

CM PLANNING AND MANAGEMENT

- CM Planning and Management is a formal document and plan to guide the CM program that includes items such as:
  - Personnel
  - Responsibilities and resources
  - Training requirements
  - Administrative meeting guidelines, including a definition of procedures and tools
  - Baselining processes
  - Configuration control and configuration-status accounting
  - Naming conventions
  - Audits and reviews
  - Subcontractor/vendor CM requirements
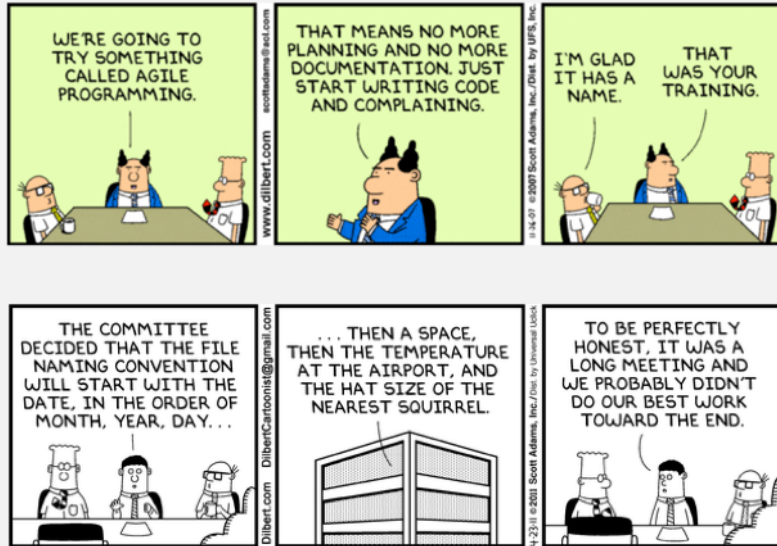
CONFIGURATION IDENTIFICATION (CI):

- Configuration Identification (CI):
  - Consists of setting and maintaining baselines, which define the system or subsystem architecture, components, and any developments at any point in time.
  - The basis by which changes to any part of a system are identified, documented, and later tracked through design, development, testing, and final delivery.
  - Incrementally establishes and maintains the definitive current basis for Configuration Status Accounting (CSA) of a system and its configuration items (CIs) throughout their lifecycle (development, production, deployment, and operational support) until disposal.

CONFIGURATION CONTROL

- Configuration Control includes the evaluation of all change-requests and change-proposals, and their subsequent approval or disapproval.

- It covers the process of controlling modifications to the system's design, hardware, firmware, software, and documentation.

CONFIGURATION STATUS ACCOUNTING

- Configuration Status Accounting includes the process of recording and reporting configuration item descriptions (e.g., hardware, software, firmware, etc.) and all departures from the baseline during design and production.

  - Deviations: A deviation from the contractual performance requirements or approved drawings, a specific written authorization to depart from a particular requirement of an item's approved configuration documentation for a specific number of units or period of time. (Defined as "planned departure")

  - Waivers: a request for authorization to accept an item which, during manufacture or after inspection, is found to depart from specified requirements, but nevertheless is considered suitable for use as is or after repair by an approved method. (Defined as "unplanned departure")

- In the event of suspected problems, the verification of baseline configuration and approved modifications can be quickly determined.

CONFIGURATION VERIFICATION AND AUDIT

- Configuration Verification and Audit: an independent review of hardware and software for the purpose of assessing compliance with established performance requirements, commercial and appropriate military standards, and functional, allocated, and product baselines.

- Configuration audits verify that the system and subsystem configuration documentation complies with the functional and physical performance characteristics before acceptance into an architectural baseline.

CONFIGURATION BASELINES (FORMAL)

- Formal Baselines:

  - Functional: The approved configuration documentation describing a system's or top level configuration item's performance (functional, inter-operability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics

  - Allocated: The current approved performance oriented documentation, for a CI to be developed, which describes the functional and interface characteristics that are allocated from those of the higher level CI and the verification required to demonstrate achievement of those specified characteristics

  - Product: The approved technical documentation which describes the configuration of a CI during the production, fielding/deployment and operational support phases of its life cycle.

PRODUCT BASELINE

- The product baseline prescribes:

    - All necessary physical or form, fit, and function characteristics of a CI,

    - The selected functional characteristics designated for production acceptance testing, and

    - The production acceptance test requirements

Image removed by the request of the license owner

CONFIGURATION BASELINES
(INFORMAL)

- Informal Baselines
    - Test: Version and documentation used for testing – changes as testing proceeds
    - Release: Multiple baselines as features are incorporated
    - Documentation: Baseline used for creating documentation

Saturday January 16, 2016 *Unexpected Things Happen*

CONFIGURATION AUDITS

- **Functional Configuration Audit (FCA)**
- The FCA is a configuration management examination of the product to verify, via testing, inspection, demonstration, or analysis results, that the product has met the requirements specified in the functional baseline documentation. The examination verifies that all authorized change proposals were incorporated into the product and documentation set prior to acceptance testing.

- **Physical Configuration Audit (PCA)**
- The PCA is a configuration management examination of the as-built (implemented) product configuration against its technical documentation. The PCA includes a detailed examination of the engineering drawings, design documentation, and specifications to ensure that the documentation set is ready to support the post-development processes.

The New York Times

BP Shortcuts Led to Gulf Oil Spill, Report Says

The Deepwater Horizon oil drilling rig burning at a well in the Gulf of Mexico in April 2010. Gerald Herbert/Associated Press

By John M. Broder

Sept. 14, 2011

WASHINGTON — BP, running weeks behind schedule and tens of millions of dollars over budget in trying to complete its troubled Macondo well in the Gulf of Mexico, took many shortcuts that

The Deepwater Horizon Disaster was made worse because the actual configuration of the well on the sea floor had not undergone a Physical Configuration Audit – they didn't know what its configuration was, making their recovery planning that much more difficult

Most computer software products are updated regularly, with features or bug fixes added with each release
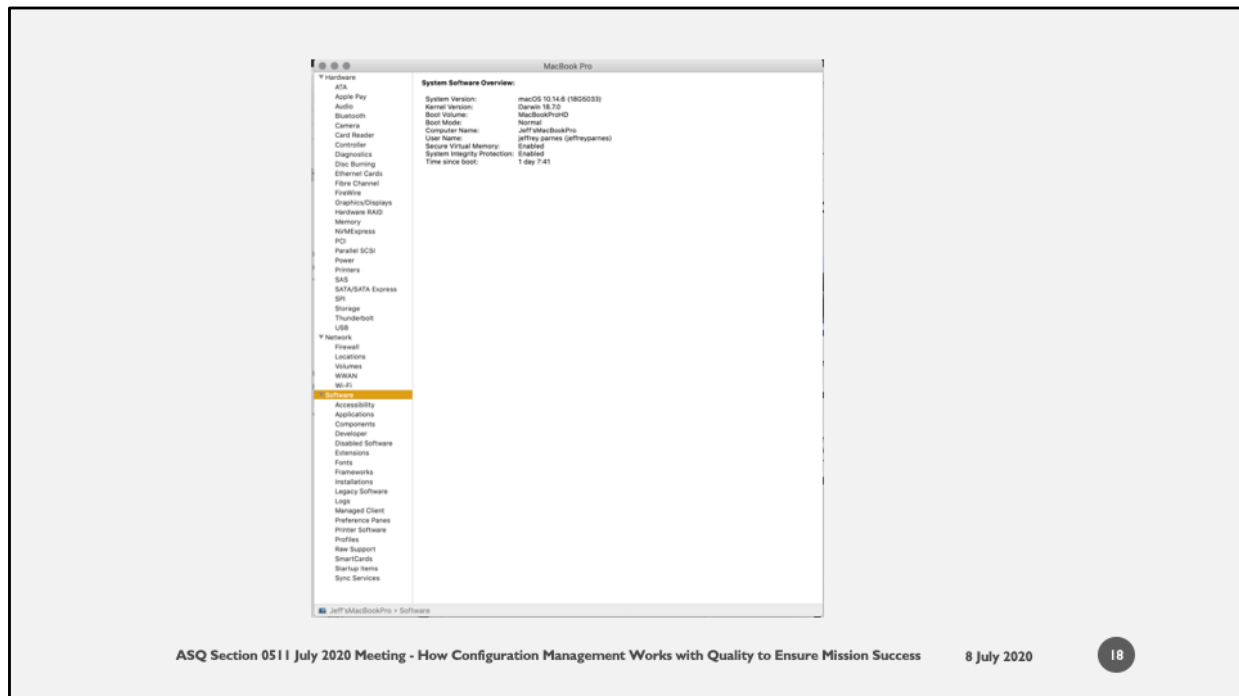
The first step in trouble shooting a problem is determining what it is you currently have.

SOFTWARE CONFIGURATION MANAGEMENT

- The software configuration management (SCM) process is looked upon by practitioners as the best solution to handling changes in software projects. It identifies the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

- The SCM process further defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented.

If you look at the definition of CM and compare SCM, you'll notice slight variations, most of which are the insertion of the word "software".

CONFIGURATION MANAGEMENT DATABASE

- The Information Technology Infrastructure Library (ITIL) specifies the use of a Configuration management system (CMS) or Configuration management database (CMDB) as a means of achieving industry best practices for Configuration Management. CMDBs are used to track Configuration Items (CIs) and the dependencies between them, where CIs represent the things in an enterprise that are worth tracking and managing, such as but not limited to computers, software, software licenses, racks, network devices, storage, and even the components within such items.

- The benefits of a CMS/CMDB includes being able to perform functions like root cause analysis, impact analysis, change management, and current state assessment for future state strategy development. Many vendors commonly identifiy themselves as IT Service Management (ITSM) systems

INFORMATION ASSURANCE

- For information assurance, CM can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

- CM for information assurance, sometimes referred to as Secure Configuration Management, relies upon performance, functional, and physical attributes of IT platforms and products and their environments to determine the appropriate security features and assurances that are used to measure a system configuration state.

  - For example, configuration requirements may be different for a network firewall that functions as part of an organization's Internet boundary versus one that functions as an internal local network firewall.

MAINTENANCE SYSTEMS

- Configuration management is used to maintain an understanding of the status of complex assets with a view to maintaining the highest level of serviceability for the lowest cost. Specifically, it aims to ensure that operations are not disrupted due to the asset (or parts of the asset) overrunning limits of planned lifespan or below quality levels.

- In the military, this type of activity is often classed as "mission readiness", and seeks to define which assets are available and for which type of mission; a classic example is whether aircraft on board an aircraft carrier are equipped with bombs for ground support or missiles for defense

  - Remember last year's movie "Midway" – the Japanese had to reconfigure their aircraft when they changed their mission from attacking Midway Island to attacking the US carriers, allowing the US planes to catch them still on their carriers

PREVENTIVE MAINTENANCE

- Understanding the "as is" state of an asset and its major components is an essential element in preventive maintenance as used in maintenance, repair, and overhaul and enterprise asset management systems.

- Complex assets such as aircraft, ships, industrial machinery etc. depend on many different components being serviceable. This serviceability is often defined in terms of the amount of usage the component has had since it was new, since fitted, since repaired, the amount of use it has had over its life and several other limiting factors.

- Understanding how near the end of their life each of these components is has been a major undertaking involving labor-intensive record keeping until recent developments in software.

CONFIGURATION MANAGEMENT (CM) (CMMI-DEV)

- Summary
    - The purpose of Configuration Management (CM) (CMMI-DEV) is to establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.
- Introductory Notes
    - The Configuration Management process area involves the following activities: Identifying the configuration of selected work products that compose baselines at given points in time
    - Controlling changes to configuration items
    - Building or providing specifications to build work products from the configuration management system
    - Maintaining the integrity of baselines
    - Providing accurate status and current configuration data to developers, end users, and customers
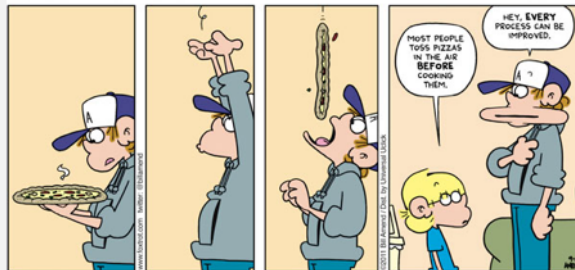
CONFIGURATION MANAGEMENT IS QUALITY MANAGEMENT

- The lack of a robust configuration management implementation is a quality management issue. An example is a company that sabotaged itself by creating information silos which did not operate under a common Configuration Management Plan as an integral part of the overall Quality Management Strategy.

- The Centers of Excellence agreed they can't truly run like separate companies. Information exchange through Configuration Management was just too critical to be ignored or lost in silos. The CEO mandated:

  - Integrating Configuration Management at the enterprise level and flowing throughout the organizational functions.

  - Integrating test with design and systems engineering at the product level.

  - Product level change control boards with representatives from all the centers.

  - Vetting of changes across all stakeholders with wider distribution of released engineering.

  - Capture of As-Built, As-Tested, As-Delivered and As-Maintained configurations by serial number.

  - The entire organization to understand that configuration management, just like quality control, is not a function to be relegated only to the CM group or the QA department but belongs to everyone.

QUALITY ASSURANCE AND CONFIGURATION MANAGEMENT

- Sandia National Laboratories implemented quality assurance and configuration systems essential to the control and traceability of modeling used to demonstrate regulatory compliance

  - The need to efficiently manage and tightly control the information used to demonstrate regulatory compliance and the scientific basis underlying program positions was recognized and addressed by Sandia as a major component in the success of the WIPP Compliance Certification Application process.

  - This requirement involved interactions between those responsible for collecting and interpreting site characterization data and those using the data to perform predictive analyses.

  - A formal program to control and document these interactions and manage the subset of data and parameters selected for use in licensing was developed and implemented by Sandia.

  - It proved essential in maintaining traceability, consistency, and reproducibility of modeling results and conclusions. In addition to the formal control of parameters selected for licensing analyses, this system also maintained full traceability to supporting documentation.

  - This traceability allowed the ready retrieval of associated records, provided a transparent means to evaluate the process by which conclusions were developed, and allowed regulatory judgments to be made about the adequacy of program positions.

27

STANDARDS SUPPORTING OR INCLUDING CONFIGURATION MANAGEMENT

- ANSI/EIA-649-1998 National Consensus Standard for Configuration Management
- EIA-649-A 2004 National Consensus Standard for Configuration Management
- ANSI EIA-649-C 2019 Configuration Management Standard
- ISO 10007:2003 Quality management systems – Guidelines for configuration management
- Federal Standard 1037C
- GEIA Standard 836–2002 Configuration Management Data Exchange and Interoperability
- IEEE 829 Standard for Software Test Documentation
- 828-2012 IEEE Standard for Configuration Management in Systems and Software Engineering. 2012. doi:10.1109/IEEESTD.2012.6170935. ISBN 978-0-7381-7232-3.

- MIL-STD-973 Configuration Management (cancelled on 20 September 2000)
- NATO STANAG 4427 Configuration Management in Systems Life Cycle Management including
- NATO ACMP 2000 Policy on Configuration Management
- NATO ACMP 2009 Guidance on Configuration Management
- NATO ACMP 2100 Configuration Management Contractual Requirements
- CMMI CMMI for Development, Version 1.2 Configuration Management
- CMII-100E CMII Standard for Enterprise Configuration Management
- Extended List of Configuration Management & Related Standards
- ITIL Service Asset and Configuration Management
- ISO 20000:1 2011& 2018 Service Management System.

28

GUIDELINES

- IEEE 828-2012 Standard for Configuration Management in Systems and Software Engineering, published date:2012-03-16

- ISO 10007:2017 Quality management – Guidelines for configuration management

- NATO ACMP-2009 – Guidance on configuration management

- ANSI/EIA-632-1998 Processes for Engineering a System

- ANSI/EIA-649-1998 National Consensus Standard for Configuration Management

- GEIA-HB-649 – Implementation Guide for Configuration Management

- EIA-836 Consensus Standard for Configuration Management Data Exchange and Interoperability

- MIL-HDBK-61B Configuration Management Guidance, 7 April 2020

- MIL-STD-3046 Configuration Management, 6 March 2013 and canceled on June 1st, 2015

- Defense Acquisition Guidebook, elements of CM at 4.3.7 SE Processes, attributes of CM at 5.1.7 Lifecycle support

- Systems Engineering Fundamentals, Chapter 10 Configuration Management

- Configuration Management Plan United States Dept. of Defense Acquisition document

REFERENCES

- **Audit Configuration**: https://www.sciencedirect.com/topics/computer-science/audit-configuration
- **MIL-HDBK-61A: Configuration Identification:** https://www.product-lifecycle-management.com/mil-hdbk-61a-5-5.htm
- **Request for Waiver:** https://en.wikipedia.org/wiki/Request_for_waiver
- **Deepwater Horizon:** https://www.nytimes.com/2011/09/15/science/earth/15spill.html
- **Configuration Management:** https://en.wikipedia.org/wiki/Configuration_management
- **Configuration Management (CM) (CMMI-DEV)** https://www.wibas.com/cmmi/configuration-management-cm-cmmi-dev
- **Quality Assurance and Configuration Management** https://energy.sandia.gov/wp-content/gallery/uploads/QA_CM.pdf

QUESTIONS/CONTACTS

- Jeffrey M. Parnes
- Configuration Management Working Group Webmaster and Board Member
- 703.424.2956 (P)
- 484.307.2552 (F)
- webmaster@cmwg.org or jeff@parnes.net
- http://www.cmwg.org or http://pacm.parnes.net
- @CMWorkingGrp or @jeffparnes