Abstract

Computer System configuration management (CSCM) is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. For information assurance, CSCM 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. CSCM for information assurance, is 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, system 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.

Keywords: Secure Configuration Management, systematic control, original equipment manufacturers (OEMs), configuration identification, information technology (IT), and preventive maintenance.

1.0 Introduction

1.1 Advent of Configuration management

Configuration management was first developed by the United States Air Force for the Department of Defense in the 1950s as a technical management discipline of hardware. The concepts of this discipline have been widely adopted by numerous technical management functions, including systems engineering (SE), integrated logistics support (ILS), Capability Maturity Model Integration (CMMI), ISO 9000, Prince2 project management methodology, COBIT, Information Technology Infrastructure Library (ITIL), product lifecycle management, and application lifecycle management. Many of these functions and models have redefined configuration management from its traditional holistic approach to technical management. Some treat configuration management as being similar to a librarian activity, and break out change control or change management as a separate or stand alone discipline. However the bottom-line is and always shall be Traceability.
2.0 Software configuration management

The traditional software configuration management (CSCM) 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 CSCM 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 CSCM process is implemented. They are:

1. Configuration identification
2. Configuration control
3. Configuration status accounting
4. Configuration audits

These terms and definitions change from standard to standard, but are essentially the same.

2.1 Configuration identification:

Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baseline. Baseline an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

2.2 Configuration change control:

Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them.

2.3 Configuration status accounting:

Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.

2.4 Configuration audits:

Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.
Configuration management is widely used by many military organizations to manage the technical aspects of any complex systems, such as weapon systems, vehicles, and information systems. The discipline combines the capability aspects that these systems provide an organization with the issues of management of change to these systems over time.

National Consensus Standard for Computer System Configuration Management of U.S submitted that, outside of the military, CSCM is appropriate to a wide range of fields and industry and commercial sectors.

3.0 Computer hardware configuration management

Computer hardware configuration management is the process of creating and maintaining an up-to-date record of all the components of the infrastructure, including related documentation. Its purpose is to show what makes up the infrastructure and illustrate the physical locations and links between each item, which are known as configuration items.

Computer hardware configuration goes beyond the recording of computer hardware for the purpose of asset management, although it can be used to maintain asset information. The extra value provided is the rich source of support information that it provides to all interested parties. This information is typically stored together in a configuration management database (CMDB). This concept was introduced by ITIL.

The scope of configuration management is assumed to include, at a minimum, all configuration items used in the provision of live, operational services.

Computer hardware configuration management provides direct control over information technology (IT) assets and improves the ability of the service provider to deliver quality IT services in an economical and effective manner. Configuration management should work closely with change management.

3.1 components

All components of the IT infrastructure should be registered in the configuration management database. The responsibilities of configuration management with regard to the configuration management database are:

- identification
- control
- status accounting
- verification

3.2 The scope

The scope of system configuration management is assumed to include:

- physical client and server hardware products and versions
- operating system software products and versions
- application development software products and versions
- technical architecture product sets and versions as they are defined and introduced
- live documentation
- networking products and versions
- live application products and versions
- definitions of packages of software releases
- definitions of hardware base configurations
- configuration item standards and definitions
3.3 The benefits

The benefits of computer hardware configuration management are:

- helps to minimize the impact of changes
- provides accurate information on CIs
- improves security by controlling the versions of CIs in use
- facilitates adherence to legal obligations
- helps in financial and expenditure planning

4.0 Maintenance systems

System 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.

A theory of system configuration maintenance on immunity for human-computer systems was worked out by Mark Burgess, with a practical implementation on present day computer systems in the software configured to perform real time repair as well as preventive maintenance.

4.1 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.

4.2 Predictive maintenance

Many types of component use electronic sensors to capture data which provides live condition monitoring. This data is analyzed on board or at a remote location by computer to evaluate its current serviceability and increasingly its likely future state using algorithms which predict potential future failures based on previous examples of failure through field experience and modeling. This is the basis for "predictive maintenance".

Availability of accurate and timely data is essential in order for CM to provide operational value and a lack of this can often be a limiting factor. Capturing and disseminating the operating data to the various support organizations is becoming an industry in itself.

The consumers of this data have grown more numerous and complex with the growth of programs offered by original equipment manufacturers (OEMs). These are designed to offer operators guaranteed availability and make the picture more complex with the operator managing the asset but the OEM taking on the liability to ensure its serviceability. In such a situation, individual
components within an asset may communicate directly to an analysis center provided by the OEM or an independent analyst.

4.3 Standards

- ISO 10007:2003 Quality management systems - Guidelines for configuration management
- Federal Standard 1037C
- GEIA Standard 836-2002 Configuration Management Data Exchange and Interoperability
- MIL-STD-973 Configuration Management (cancelled on September 20, 2000)
- STANAG 4159 NATO Material Configuration Management Policy and Procedures for Multinational Joint Projects
- STANAG 4427 Introduction of Allied Configuration Management Publications (ACMPs)
- CMMI for Development, Version 1.2

5.0 Case study: Construction Industry

More recently configuration management has been applied to large construction projects which can often be very complex and have a huge amount of details and changes that need to be documented. Construction agencies such as the Federal Highway Administration have used system configuration management for their infrastructure projects in the U.S. There have been several construction based configuration management software developed that aims to document change orders and RFIs in order to ensure a project stays on schedule and on budget. These programs can also store information to aid in the maintenance and modification of the infrastructure when it is completed. One such application called ccsNet, was tested in a case study funded by the Federal Transportation Administration (FTA) in which the efficacy of configuration management was measured through comparing the approximately 80% complete construction of the Los Angeles County Metropolitan Transit Agency (LACMTA) 1st and 2nd segments of the Red Line, a $5.3 billion rail construction project. This case study yielded results indicating a benefit to using system configuration management on projects of this nature.

6.0 Summary and Conclusion

While system configuration management may not be the easiest or the first function you implement in controlling your IT environment, it can be a very powerful step in ensuring proper control of your IT resources. System configuration management allows you to understand the IT resources you have and how they relate to one another. This information allows you to make informed decisions on maintaining and upgrading your IT environment. Implementation of a system configuration management program is a critical step to take in optimizing the management of your IT world. More recently system configuration management has been applied to large construction projects which can often be very complex and have a huge amount of details and changes that need to be documented. Construction agencies such as the Federal Highway Administration have used configuration management for their infrastructure projects. There have been several construction based configuration management software developed that aim to document change orders and RFIs in order to ensure a project stays on schedule and on budget. These programs can also store information to aid in
the maintenance and modification of the infrastructure when it is completed.

7.0 Acknowledgements

The authors are greatly grateful and indebted to our research partners and colleagues in the School of Science and Industrial Technology (SSIT), Nigerian Institute of Management (NIM), and Standards Organization of Nigeria (SON), and Manufacturers Association of Nigeria (MAN), who have being research fellows and have supported our research for some years now. We would also like to thank the Management of Abia State Polytechnic, Aba, for providing the platform and the right atmosphere for this work. We received much technical assistance from M. Burgess, and the ANSI/EIA-649-1998 National Consensus Standard for System Configuration Management of U.S.

8.0 References

1. MIL-HDBK-61A CONFIGURATION MANAGEMENT GUIDANCE 7 February 2001