Configuration Management: A Critical Analysis of Applications Using the 8-Step Problem Solving Method

L.L. Fletcher, PhD, SIDC, Advanced Space Operations School, Colorado Springs, CO, USA.

J.M. Kaiser, 50th Space Wing, Air Force Space Command, Schriever AFB, CO, USA.

C.W. Johnson, Ph.D.; Department of Computing Science, University of Glasgow, Scotland.

C. Shea, M.Ed., Ph.D., Principal Consultant, ESR Technology Ltd, Warrington, Cheshire, UK.

Keywords: Configuration Management, Operational Design, 8-Step Method.

Abstract

Configuration management endeavors to verify a system's physical form and mission function are not only initially known but also remain knowable throughout the system life cycle. Operational design is a campaign planning corollary to configuration management which keeps military operations knowable. Any organic or inorganic collection of parts or phases which synchronously forms a unitary whole requires configuration management to avoid mission failure. The parallels between configuration management and operational design provide a framework to reveal mutual overlaps between the knowledge and understanding of systems engineers and of other configuration management stakeholders. There are countless examples cited in history where the interaction of an unknown configuration, which was not managed using an orderly methodology, led to a mishap[1]. The following pages use the insights gained from previous studies to apply an 8 Step Problem Solving Model. This is a standard process based on Boyd's OODA (Observe, Orient, Decide, Act), which we have applied to a configuration management scenario to demonstrate its risk reduction's value for mission success.

Introduction

Configuration management ensures the system's physical form and mission function are not only known initially but also remain knowable throughout the system life cycle. It has long been the 'hallowed' domain of systems engineers and the unintentional nemesis of system operators. The latter stakeholders should be allies in the battle against mission failure and the potential resultant mishaps; however, they are often unlikely rivals in the configuration management process. System Safety Engineers are taught to become stewards of the system's safe operating configuration throughout the indoctrination to their system safety engineering discipline. Operators are likewise trained to become the stewards of mission assurance throughout the indoctrination to their system operating discipline. Despite the convenient conclusions that could be gained through anecdotal observations of interactions between System Safety Engineers and System Operators; where the configuration management and control Venn diagram could be interpreted to be mutually exclusive, there could alternatively be a considerable amount of mutually beneficial overlap (Figure 1). A survey of the British Aerospace Industry reported that, "to some extent CM is a Cinderella Discipline; this lack of recognition is evident in aspects such as the lack of senior management responsibility for the discipline, and deficiencies in education and career path for involved staff" (Burgess, McKee, & Kidd, 2005, p. 299). Perception shapes values and could preclude a sense of common purpose.

[1] Several of these are discussed in a companion paper C.W. Johnson, L.L. Fletcher, C.M. Holloway and C. Shea, Configuration Management as a Common Factor in Space Related Mishaps, Submitted to the 27th International Conference on Systems Safety, Huntsville, Alabama, USA 2009, International Systems Safety Society, 2009.

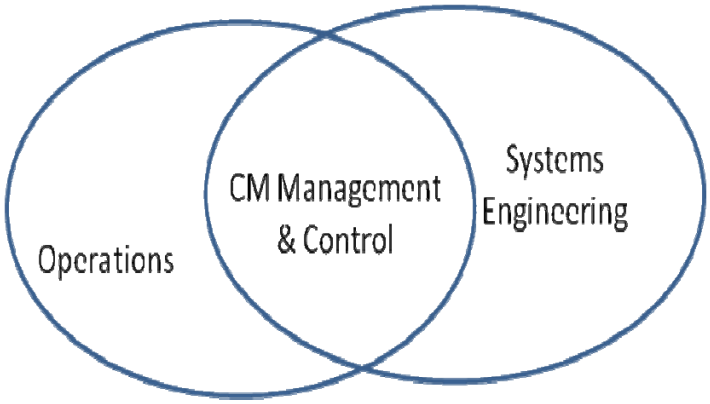

Figure 1. Venn Diagram of the hypothetical CM Overlap between on Operations and Systems Engineering

Both operators and systems engineers are concerned about safety issues that would cause immediate catastrophic mission/system failures or loss of life. These concerns can be seen in the "notes", "cautions", and "warnings" which are usually incorporated into the operator's technical data. The following pages focus less on those potential mishaps that are identified during the development of safety-critical system and more on the hazards that can arise from the changes and updates that occur during operational deployment. After a system is fielded, it can leave the constant scrutiny of program management or other high level oversight. In some cases, the focus can change from ensuring safety constraints, such as accurately documenting configuration changes, to ensuring the system's operational capability. Operators have the specified task of mission accomplishment, and thus the implied task for operators is to keep the system operational to accomplish the mission. Sustaining operational capability is the operator's de facto raison d'être. Operators do not immediately recognize the mission assurance value of accurate configuration control.

Statement of the Problem

Periodic maintenance is scheduled and performed by operational support engineers. However, there is pressure from operators and operational customers to keep the system operating. In consequence, systems engineers are often forced to implement ad hoc fixes to keep the system mission capable. These fixes may be both necessary and effective but they could also significantly alter the known configuration of the system. Once ad hoc changes have been accepted within engineering teams, they tend to proliferate over time (Johnson and Shea, 2007). In consequence, the system migrates farther and farther from the known or baseline configuration. Often operational test requirements are also bypassed by support engineers through the assertion that ad hoc changes are merely "form, fit, and function". The configuration control dilemma can be further compounded when some operators almost routinely accept the risks associated with installing incremental or "spiral development" upgrades directly from the developer. This also circumvents the configuration management process. Unless carefully controlled, the installation of these modifications can undermine the operational test process using the aforementioned "form, fit, and function" paradigm. System operating waivers are another short cut strategy which does not adequately aid the configuration management process. Obviously some risk accepting behavior is necessary for continued operations; however, if it is not documented, it also contributes to loss of the system's known configuration.

The operators, support engineers, and developers are certainly not intended to be villains in this study; however, the latter's acceptance of undocumented and/or unverified upgrades has contribute to unrecoverable mission system failures and other unforeseen mishaps (Johnson, Fletcher, Holloway and Shea, 2009). System Safety Engineers and Operational Testers are chartered to be mitigation agents that would respectively monitor configuration changes or require the configuration to be "baselined" before testing. However, if the latter stakeholders are excluded from the operational change management process due to a perceived adversarial relationship, where the latter agents are perceived as "whistle blowers" or "risk adverse operational obstacles", then configuration management becomes an untenable process. Clearly, a unifying methodology is required to both illuminate and, furthermore, bridge the gaps in understanding and cooperation between operators and the other configuration management stakeholders.

Background of the Problem

The stakeholder dilemma, addressed in this paper, arises because of the different priorities and perspectives that arise between various stakeholders. Understanding configuration management principles could be perceived as an esoteric discipline, especially for mission focused system operators, when couched in systems engineering vernacular. This is not an indictment of the systems engineering process; however, it highlights a potential root cause for the gap in configuration management priorities between operators and the other configuration management stakeholders. This gap could be a contributory factor to the casually observed adversarial interactions between system operators and other stakeholders. In the present study, an assessment of the impediments posed by operational lapses and restrictive policies provides insights into the requirements that are necessary to maintain congruency and collaboration within configuration management stakeholders. The desired collaborative relationship can only be built through the facilitation of a common culture or perspective on the importance of the configuration management process. Unquestionably, to impart the criticality of configuration management beyond the cohort of systems engineers, valid strategies must be offered to build a transformational curriculum to bridge the gap between operators and the other configuration management stakeholders.

The 8 Step Problem Solving Model is a standard process based on Boyd's OODA (Observe, Orient, Decide and Act) Loop which could be applied to the configuration management stakeholder dilemma. The eight steps are:

1. Clarify and Validate the Problem
2. Break Down the Problem and Identify Performance Gaps; "Observe"
3. Set Improvement Target
4. Determine Causes and Contributory Factors; "Orient"
5. Develop Countermeasures; "Decide"
6. See Countermeasures Through
7. Confirm Results and Process
8. Standardize Successful Processes; "Act"

The 8 Step Problem Solving Method could be presented as a feasible candidate framework, for application to a configuration management scenario, to create the transformational curriculum required to highlight areas of mutual overlap for configuration management stakeholders. Clearly the 8 step model, if applied, cannot simply be a restatement of systems engineering dogma. The Zones of Proximal Development; Lev Vygotsky's theoretical limit of what an individual can learn on their own, must be socially constructed and mediated utilizing a collaborative process for all configuration management stakeholders. Hence, the scope of what is characterized as a configuration management issue must be more inclusive of examples which could have relevance for all stakeholders. Configuration management is the progenitor of other technical management disciplines like Systems Engineering, Integrated Logistics Support, and ISO 9000; however, the technical focus must evolve to encompass any organic or inorganic collection of parts which combine to function synchronously as a unitary whole.

Case Studies

The following case studies are samples of incidents where configuration management was a contributory factor. Several of the discussions concern the interaction between management and operational design for military operations (both past and present); and the effect of policy and configuration management. Additionally, there is also a short discussion on how software and lack of configuration management affected NASA's Demonstration of Autonomous Rendezvous Technology (DART) vehicle.

Operations. Campaign planning for military operations is not customarily considered to be under the purview of configuration management. Systems engineers may be consulted on the survivability or sustainability of fielded systems; however, it would be a rare occasion for them to provide input for the overall conduct of the operational art. "Operational art integrates ends, ways, and means and considers risk across the levels of war" (Joint Publication 3-0, 2008, p. xix). Configuration management is "a management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design and operational information throughout its life" (MIL-HDBK-61A, 2001, p. 3-4). The de facto configuration management process of the operational art is "operational design" because "during execution, commanders and their staffs continue to consider design elements and adjust both current operations and future plans as the joint operation

unfolds" (Joint Publication 3-0, 2008, p. xix). The present analogy could characterize the theoretical overlap between the operational and engineering disciplines. A commander would endeavor to become keenly aware of the second and third order impacts to mission accomplishment associated with each change necessitated by military operations. For example, if a commander committed all of their combat power to an operation, without ensuring their flank was protected, they could become surrounded by the enemy. In the latter case their first order actions lead to their second order defeat. Both the operational and the engineering discipline examines organisms which were designed to accomplish specified tasks based on mission needs and require active management to achieve the desired mission objective.

The Battle of Ulm in 1805 is a minor footnote which could have ultimately led to Napoleon's victory at Austerlitz. The Austrians and Russians planned to rendezvous and combine their forces to defeat the French at Ulm; however, the Russians used the Julian calendar while the Austrians used the Gregorian calendar. Unfortunately for the ill-fated coalition, each was unaware of the other's calendar preference; therefore, they were mutually blind to a relative temporal disparity for the chosen campaign window. Consequently the Russians arrived 12 days late for the campaign; according to the Gregorian calendar, because of the hidden incongruity. The Austrians had already surrendered a significant portion of their combat forces at Ulm prior to the arrival of their Russian partners. The Austro-Russian war machine failed in part because their internal standards for tracking time were not synchronized externally using a common standard. The lack of continuity between the operational arts of the two coalition partners was not apparent to either because they did not share a common operational designer. Thus the Austro-Russian coalition could not deduce their status as two temporally discordant organisms destined for mission failure. Unquestionably, the harmony of an operational configuration management process like operational design could have yielded an alternate history for the Battle of Ulm and ultimately changed the Austro-Russian prosecution of the Battle of Austerlitz. Analogously it is the job of the system safety engineer, along with the configuration manager, to ensure that unforeseen mishaps do not happen through the active management of configuration.

Discrepancies in the management of operational design are by no means relegated to early nineteenth century warfare. On 30 August 2007 there was an unauthorized transfer of nuclear warheads between Minot Air Force Base, North Dakota, and Barksdale Air Force Base, Louisiana. A B-52 aircraft left Minot with nuclear-capable cruise missiles loaded on one of its pylons, after several levels of verification were abrogated by the Minot munitions maintenance squadron, facilitated by local changes in nuclear handling processes and the underlying procedures. The Deputy Assistant to the Secretary of Defense for Nuclear Matters (DATSD-NM) defines Nuclear Weapons Surety as, "…the materiel, personnel, and procedures that contribute to the safety, security, reliability, and control of nuclear weapons, thus assuring no nuclear accidents, incidents, unauthorized use, or degradation in performance" (Office of the Deputy Assistant to the Secretary of Defense for Nuclear Matters, 2009). Nuclear Weapons Surety is an operational design for the configuration management process applied to handling nuclear weapons. According to the Defense Science Board Permanent Task Force on Nuclear Weapons Surety "…there is a requirement to identify pylons of nuclear-inert missiles with readily visible markings. Past practice involved placement of placards on multiple sides of the pylon and orange cones around the pylon. However, the Task Force could find no written directive that specifically described the required identifying means. Over time, the practice at Minot was reduced to an 8 x 10 piece of paper placed somewhere on the pylon" (The Defense Science Board Permanent Task Force on Nuclear Weapons Surety, 2008, p. 5). The latter practices were allowed to migrate away from those formerly identical to Intercontinental Ballistic Missile (ICBM) warhead handling procedures; which remained stringent, and are still practiced in parallel at Minot to handle ICBM warheads. The procedural configuration changed, unchecked by oversight during a period of more than a decade following the Cold War, under the auspices of ideas such as the "value added" savings gained by decreasing processing time. Unquestionably the need for active configuration management of operational design is not a requirement relegated to nineteenth century warfare.

Policy: Failure to apply Operational Design to the Operational Art is a possible source of operational configuration management error; however, the policies which dictate the rules of engagement could be just as detrimental. In operational planning, rules of engagement are constraints and "…a constraint is a requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action" (Joint Publication 5-0, 2006, III-26). The direction to behave in a certain manner to honor policy or politics could ultimately alter what would otherwise be considered best practices. Thus, an environment is created that may push a counterintuitive agenda which increases the probability of mishaps due to lack of freedom of action at the tactical level. The configuration management of systems is not immune to mishaps due to implied rules of engagement based on the specified constraints imposed by policy. Configuration Status Accounting (CSA) is; "the configuration management

activity concerning capture and storage of, and access to, configuration information needed to manage products and product information effectively" (MIL-HDBK-61A, 2001, p. 3-5). If policy is enacted to curtail access to configuration information, then CSA will be less efficient. If the CSA process is governed by guidelines that make it less efficient, then the policy masks potential mishaps that are not evaluated for mitigation.

DART: On April 15, 2005 the Demonstration of Autonomous Rendezvous Technology (DART) launched for a rendezvous with the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite. The rendezvous was designed to occur without remote assistance from ground control. The mission proceeded routinely until navigation system anomalies began to manifest. These anomalies caused the spacecraft to fire thrusters excessively and deplete the propellant at a vastly increased rate. Due the position and navigation anomaly DART collided with MUBLCOM 3 minutes and 49 seconds before initiating maneuvers that would have taken DART away from MUBLCOM, due to the depleted propellant, and retired the DART mission.

> "at the time of collision, DART was flying toward MUBLCOM at 1.5 meters per second while its navigational system thought it was 130 meters away from MUBLCOM and retreating at 0.3 meters per second. The collision avoidance design approach never anticipated the possibility that the navigational data would be this inaccurate" (Overview of the DART Mishap Investigation Results, 2006, p. 6).

Root Cause: DART was a NASA high-risk, low budget technology demonstration selected under a NASA Research Announcement (NRA). By NRA design, the government received data and supplied broad requirements, but the requirements were met at the discretion of the contractor. The latter practice creates a Configuration Management 'blind spot' for the government due to lack of process insight. A policy implication for the mishap was predicated on a policy restriction perceived to be imposed by the International Traffic in Arms Regulation (ITAR). The aforementioned ITAR perception caused inadequate technical communication between NASA managers and the international vendor. Restrictions like ITAR have personal and professional implications which could cause extremely conservative behavior. Unquestionably, if any stakeholder interactions are veiled by the perception of policy sanctions the probability of mishap will also increase. Configuration management policy must be informed by the knowledge of the constraints imposed on the system by internal and external polices.

Mars Climate Orbiter: September 23, 1999 the Mars Climate Orbiter's (MCO) signal was lost during Mars Orbital Insertion (MOI) 49 seconds before the expected occultation loss of signal and the signal was never recovered.

> "On September 29, 1999, it was discovered that the small forces '*Delta'* V's 'velocity changes' reported by the spacecraft engineers for use in orbit determination solutions was low by a factor of 4.45 (1 pound force=4.45 Newtons) because the impulse bit data contained in the AMD file was delivered in lb-sec instead of the specified and expected units of Newton-sec" (Mars Climate Orbiter Mishap Investigation Board, 1999, p. 13).

Root cause: The MCO was lost due to a failure to properly code a software file with metric units as opposed to the English units, which were used. There were multiple contributing causes; however, most were related to lapses in Configuration Management and Operational Design policy enforcement. The operations navigation team was not adequately trained on spacecraft operations because they joined the mission very close to the launch date. Furthermore, the operations navigation team did not participate in any tests of the ground software; therefore, they missed another opportunity to gain familiarity. Poorly trained and unindoctrinated operators violate the conditions required for successful operational control. The system engineering process was weak, and thus, allowed an inadequate transition of the program from development to operations which was also a prominent harbinger of the total mission failure. Finally, the Mars Surveyor Operations Project was simultaneously managing three missions; thus diluting focus on any single mission, and there was no single overarching configuration manager. Clearly, there were opportunities to mitigate the mishap; however, ad hoc operations and program management (which bypasses configuration management policy) fosters haphazard rules of engagement, which decrease the probability of success.

Configuration Management 8-Step Method Scenario

The 8-Step Method (AFSO21 Playbook, October 2007) is a process to solve problems by clearly discerning solutions to foreseeable problems associated with configuration management. This process creates a systematic approach with a common structure for solving problems in a consistent and concise format for presentation of data, problem solving facts and information. The process uses lean tools from Air Force Smart Operations for the 21st Century (AFSO21) program which uses the idea of eliminating waste or non-value added steps in a process. In our example, the goal is to ensure configuration management is value added to everyone concerned and is accomplished in such a manner as to be unobtrusive and cost effective.

Step 1. Clarify and Validate the Problem. Present the problem and its significance; the problem statement should characterize the issue to be resolved, where it happened, and when it happened. Typically, the problem is presented in one paragraph using factual, dispassionate, and descriptive terms. Furthermore, the statement of the problem should represent a consensus of all team members. For the present scenario, a notional problem statement could be: "The Program Manager needs to develop a configuration control process for a widget, which includes updates through engineering change proposals, development, waivers or 'on the fly' contractor upgrades to hardware and or software, this will ensure a known configuration for mission assurance and safety".

Step 2. Break Down the Problem and Identify Performance Gaps (Observe). Problem solving and process improvement begins with the data, therefore the team must 'Gather and Review Key Performance Indicators and Metrics'. Understanding what the data means is critical to true "root cause" problem solving. There are different tools for use during this step; for example performance gap analysis or bottleneck analysis characterizes inhibitors to the flow of the process. This gap could be assessed by getting the team to compile a value stream map of the process. A value stream map is where the process is described step-by-step. For our case study, since we don't have a process established, the team could compile an ideal state map, which is a perfect world without resource constraints, configuration management process to guide the team to the desired end state. From the ideal state map a more realistic future state map, which is a map with resource and maybe regulatory constraints, would yield a well thought out configuration management process devoid of much waste. Additionally, the Program Manager should reference MIL-STD-882 to ensure that the configuration control steps are on the contract performance work statement and secure compliance. This step would also be ideal to gather the information is necessary to tailor MIL-STD-882 for contract amendment. For example, the contract could notionally be tailored as follows (SMCI 63-1205):

1. Task 101 - System Safety Program
   1.1. Task 101 (System Safety Program). Comply with all of section 4 of MIL-STD-882C. Acceptable level of risk shall be based on Table 1. The resolution of residual risk shall be accomplished per the requirements of Table 2. System safety shall be included in the work breakdown structure.

Table 1. **Example Mishap Risk Assessment Matrix (MRAM).**

Probability	Severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20
Designed Out	21	22	23	24

Table 2. **Example Mishap Risk Acceptance Levels (MRALs).**

Mishap Risk Index	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive

6 – 9	Serious	Program Executive Officer
10 – 15	Medium	Program Manager
16 – 24	Low	As directed

1.1.1 The status of the following activities shall be reported to the SPO:

- Safety critical characteristics and features shall be tracked separately to ensure that risks are reduced to acceptable levels. Safety critical software (critical software configuration items) CSCIs shall be designated and labeled as such. Where multiple inhibits are employed in a safety critical system at least one inhibit shall be implemented in hardware that is independent of the computer and software controlling the hazardous function.

1.2. Task 102 System Safety Program Plan (SSPP). The SSPP shall be contractually binding when approved by the SPO. Apply Task 102 as written.

1.2.1. The preliminary SSPP shall be submitted no later than TBD days after contract award and the final version due TBD days after review by the Government. The SSPP shall be contractually binding when approved by the Government. Updates to the SSPP shall be provided upon request by the Government, and shall be approved by the Government.

1.3. Task 103 (Integration of Associate Contractors, Subcontractors and A&E Firms). (Assume prime and sub contractors). Apply entire task except 103.2.1 and 103.2.2.

1.4. Task 104 (System Safety Program Reviews). Contractor shall support all milestone reviews and audits.

1.5. Task 105 (SSG/SSWG Support). The contractor shall be a technical advisor to the SSG. The contract shall support one SSG, a test review meeting and two other safety meetings per contract year. This support shall include briefing assigned topics at these meetings and answering questions related to the system safety effort.

1.6. Task 106 (Hazard Tracking and Risk Resolution). The contractor shall maintain a hazard log of all hazards initially ranked as a Category I, II or III (Catastrophic, Critical or Marginal) severity - this hazard list shall be accessible to the government

1.7. Task 107 (System Safety Progress Summary) Prepare quarterly system safety reports as part of the SPO Quarterly Review.

2. Tasks for the 200 series are concerned with hazard assessments, ie: preliminary hazard assessment (PHA), software hazard assessment (SHA), etc…for our example we should apply all of the tasks in the 200 series.

3. Tasks in the 300 Series begin about after our widget is built and before testing begins

3.1. Task 301 (Safety Assessment). All.

3.2. Task 302 (Test and Evaluation Safety). The contractor shall comply with all range safety test requirements as well as OSHA, State, and Local Safety regulations.

3.3. Task 303 (Safety Review of ECPs, SCNs, SPRs, and Requests for Deviation/Waiver). The contractor SSM shall notify the SPO within one working day of identifying the change in the hazard severity or probability by one level.

4. Task 401 (Safety Verification). Safety critical items shall include command and control elements of a system, subsystem or component; fuses, firing circuits, and safe and arm devices for ordnance; and any hardware, software or procedures that controls risk for catastrophic or critical severity hazards.

Step 3. Set Improvement Target(s). The program manager should identify specifically the different steps for hardware upgrades and software upgrades or changes in the Performance Work Statement (PWS) and the responsible parties for such upgrades. These targets should be balanced to ensure goals are balanced with the operators, developers and managers. The team should identify specific outputs which are based on subject matter expert knowledge and experienced stakeholders such as System Safety Engineers. Targets should be measurable, include time frames, and have data that is obtainable. Furthermore targets should use an action and result orientation which is traceable to the stated mission, vision, and goals which are meaningful to the operator. This step should provide the Program Manager with step-by-step measurable milestones.

Step 4. Determine Causes and Contributory Factors (Orient). This should be a systematic approach to solve the problem of inadequate configuration management. For instance, 'chain of events' techniques including ECF or STEP can identify the ways in which operator errors of omission or commission combine with latent or underlying organizational issues, including lack of review. Alternatively, more recent techniques such as STAMP or the ACCIMAP approach can help to expose the political, managerial and technical constraints that often lead to failures in complex safety-related systems. In either case, this step should be accomplished through a collaborative session between the system engineer, system safety engineer, contractor, operators and program manager to brainstorm ideas on how to best execute the configuration control to support operational processes. This step could be accomplished through a collaborative session between the system engineer, system safety engineer, contractor, operators and program manager to brainstorm ideas on how to best execute the configuration control to support operational processes. Several issues can hinder proper configuration management; the biggest one faced by program managers is balancing cost, schedule and performance. Program managers should ensure to have a cost benefit analysis accomplished and lessons learned ready to answer questions which will arise since configuration management is usually placed in the back burner.

Step 5. Develop Countermeasures (Decide). This step is intended to develop an action plan for configuration control. The most important activity at this step is to build a consensus with all stakeholders by facilitating interaction with the appropriate subject matter experts during the process. Including stakeholders in the solution creation step will develop a sense of ownership in the configuration control solution. Therefore, the stakeholder will have a vested interest in the success of the configuration management process.

Step 6. See Countermeasures Through. This step involves ensuring the countermeasures are acted upon through Process Improvement Tools such as:

- 6-S & Visual Management – Pertains to having a clearly labeled place for everything
- Standard Work – The foundation for process improvement – documents the change for the workplace
- Cell Design – Arrangement of work centers for optimum workflow
- Variation Reduction – A six sigma tool used more in production environments
- Error Proofing – Attempting to remove the chances for making mistakes, ie: templates
- Total Productive Maintenance (TPM) – Planning for upcoming due work during office downtime
- Rapid Improvement Events (RIE) – The right group assembling to solve a problem quickly

Step 7. Confirm Results and Process: Evaluation of data relative to effects and implementation of the action plan. The key is to review metrics, manage action plan, and ensure standard work has been established. This is where the team reviews performance relative to steps and readdress steps if necessary to ensure configuration management is working.

Step 8. Standardize Successful Processes (Act). This is the step where the team communicates best practices to other teams and creates a storyboard of success. If the process is not successful or not working as desired, this is the step where the team would loop back to step 1 and restart the 8-step process. One of the key concerns in each of these steps is to ensure the benefits do not outweigh the costs of adoption. Hence, it is critical to communicate success stories that can both streamline the process and also focus investments to configuration management activities that potentially offer the greatest returns.

Discussion and Conclusion

The approach described in this paper is work in progress and much remains to be done. Revealing the Venn diagram overlap between operators and other configuration management stakeholders, illustrated in Figure 1, will not be an easy task because it requires an evolution in the respective cultures. Accepting Operational Design as a campaign planning analogy for Configuration Management would be a good embarkation point for Operators and Systems Engineers. The operational examples provided during this study could be critiqued as to whether they are truly configuration challenges or personal lapses in discipline; however, they do serve to address the need for interdisciplinary understanding in the CM stakeholder community. History reveals copious examples of operations and systems which, when inconsistently managed, fail (Johnson, Fletcher, Holloway and Shea, 2009). Policy is a common denominator in every enterprise which dictates the rules of engagement which could either help or hinder the progress of a mission or program.

Misunderstanding policy is as bad as a weak or nonexistent policy because mitigation becomes untenable and the probability of success is decreased. The 8-step Method is a framework which could readily be applied to facilitate orderly configuration management and control. Traceability to Boyd's OODA (Observe, Orient, Decide and Act) Loop gives the 8-step Method an operational lineage which also aptly supports the configuration management process. Unquestionably, the path to mutual understanding must weave the foundations of multiple disciples together to create a new common dialogue and CM stakeholder culture. Further work intends to build on the approach described in this paper by applying it to both identify configuration management problems within a number of existing projects and then to use these insights proactively to develop more details support for the management of future projects in complex, dynamic environments.

References

Air Force Smart Operations for the 21st Century (AFSO21) Playbook, *Volume B, Introduction to the Eight Step OODA Loop AFSO Problem Solving Model*, Version 2.0, October 2007

Burgess, T. F., McKee, D., Kidd, C. Configuration management in the aerospace industry: a review of industry practice, *International Journal of Operations & Production Management;* 2005; 25, 3/4; 290-301.

C.W. Johnson and C. Shea, The Contribution of Degraded Modes to Accidents in the US, UK and Australian Rail Industries. In A.G. Boyer and N.J. Gauthier (eds.), Proceedings of the 25th International Systems Safety Conference, Baltimore, USA, International Systems Safety Society, Unionville, VA, USA, 626-636, 0-9721385-7-9, 2007.

C.W. Johnson, L.L. Fletcher, C.M. Holloway and C. Shea, Configuration Management as a Common Factor in Space Related Mishaps, 27th International Conference on Systems Safety, Huntsville, Alabama, USA 2009, International Systems Safety Society, 2009 (this volume).

Joint Publication 3-0, Joint Operations, Joint Chiefs of Staff, Washington, DC, 2008.

Joint Publication 5-0, Joint Operation Planning, Joint Chiefs of Staff, Washington, DC, 2006.

Mars Climate Orbiter Mishap Investigation Board, Phase I Report, NASA, 1999.

Office of the Deputy Assistant to the Secretary of Defense for Nuclear Matters, Nuclear Weapons Surety, Retrieved February 22, 2009; http://www.acq.osd.mil/ncbdp/nm/nuclearweaponssurety.html.

Overview of the DART Mishap Investigation Results, report for public release, NASA, 2006.

Space and Missile Systems Center Instruction, SMCI 63-1205. *United States Air Force - Space System Safety Policy, Process, and Technique,* Air Force Space Command 20 August 2007.

The Defense Science Board Permanent Task Force on Nuclear Weapons Surety, Report on the Unauthorized Movement of Nuclear weapons, 2008.

US Department of Defense, Military Handbook: Configuration Management Guidance, MIL-HDBK-61A (SE), Washington DC, 2001.

Biography

Louis L. Fletcher, PhD, Dean, SIDC, Advanced Space Operations School, Colorado Springs, CO, USA.
Telephone +1(719)593-8794 x320, Fax +1 (719) 637-9007, louis.fletcher@afspc.af.mil

Dr. Fletcher is currently the Dean of Air Force Space Command's Advanced Space Operations School. He was the first Chief of Safety for the Space Innovation & Development Center where he was responsible for verifying the safe operation and testing of ground-based radars, flight test launched Intercontinental Ballistic Missiles, on-orbit space systems and terrestrial command and control equipment.

Jacqueline M. Kaiser, Wing System Safety Engineer, 50th Space Wing, Air Force Space Command, 210 Falcon Pkwy Suite 148b, Schriever AFB, CO 80910, USA.
Telephone +1(719)567-7496, Fax +1(719)-567-5026, jacqueline.kaiser@schriever.af.mil

Ms. Kaiser is currently serving as the 50th Space Wing system safety expert for satellite systems. She is responsible for the wing continuous improvement program (AFSO21) and is Level II certified. Prior to transitioning to the Air Force, she served as the Senior Aerospace Engineer for the Navy J85 engine supporting acquisition, upgrades, maintenance and aircraft mishap support. Ms. Kaiser also, worked as human factors engineer for the In-Flight Escape Systems Branch for the Navy. She provided comprehensive engineering support for Crew Systems supporting acquisition, engineering, Research, Development, Test and Evaluation (RDT&E) efforts for all Navy aircraft equipped with ejection seats.

Chris.W. Johnson, DPhil, MA, MSc, FBCS, Ceng, CITP, Dept of Computing Science, Univ. of Glasgow, Glasgow, G12 8RZ, Scotland, UK.
Telephone +44(141)3306053, Fax +44(141)3304913, Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.

Christine Shea, M.Ed., Ph.D., Principal Consultant, ESR Technology Ltd, Whittle House, 410 The Quadrant, Birchwood Park, Warrington, Cheshire, UK.
Telephone: +44(1925)843 472, Fax: +44(1925)843500, christine.shea@esrtechnology.com

Christine is a principal consultant in safety and risk management with ESR Technology. Her work involves the management of risk in complex, safety-critical domains including aviation, rail, the petroleum industry and health care. Her research interests include the management and organization of work in safety critical domains, safety culture, the development and implementation of incident reporting systems and human error.