Utilizing lifecycle management system approach, boost airworthiness certification of software-centric avionics systems

Chiranjeevi Aradhya
Sr Software Engineer
Collins Aerospace, United States of America

Abstract

Using a well-established Application Lifecycle Management (ALM) framework will enhance the airworthiness analysis process by presenting all pertinent details and ensuring no particular requirement is ignored. A software industries application lifecycle management (ALM) framework can provide considerable value in auditing software projects as it allows engineers to collect, monitor and trace critical software data. An ALM framework enables the collection of specifications, approval, design and construct data for the creation of a software-centric avionics system. The data that provided has a comprehensive nature, and the traceability of the data enables fast and efficient analysis. This paper will address a data model that allows for collecting cross-discipline data in an ALM system, and provide an example of how to use that collected data to build upon the data collection activities of an organization.

Keywords: *Data and Document handling; Business data processing; Data collection; Data integration; Business process management; Information management; Knowledge management*.

1. Introduction

The software's airworthiness certification requires a comprehensive series of Stage of Involvement (SOI) audits, which concentrate on ensuring that it works as expected on a given device. Audits focus on the operating system but include other disciplines, such as Systems Engineering, Configuration Management and Quality Assurance. This paper describes the implementation of an Application Lifecycle Management (ALM) method to collect and coordinate data from all the disciplines involved in software development.

A successful ALM framework will have an integrated system lifecycle management. A major aspect of an ALM tool's functional functionality is the definition of a Data Object, which allows data to be collected, handled, worked with, and monitored from inception to completion. Typical records in an ALM system can include Phase Change Records (PTR), Quality Assurance Records (QAR) and Formal Peer Review Records (FPR). DI (Data Item) include specifications, concept models, source code, test cases, test procedures and outcomes as well as project-level details such as meeting minutes, action items, risks, assignments and deliverable records. There is no restriction of data collection in any electronic management programme. The strength of an ALM system is not just in collecting data using DIs. Via similar to way of establishing relationships between tables in a relational database, data mining concepts in ALM provide information that was not available in legacy data mining methods such as spreadsheets, records, and unstructured collections of files. DIs organise ties among each other to create business rule and relational characterizations among DIs. For example, ALC may connect a Test Case to the requirement DIs that verify it. In addition, the relationship between DIs may be called in order to increase the contextual awareness of the DIs. A Test Case DI "verifies" one or more of the Requirement DIs. Constraints can be placed in place to ensure that Test Case DIs can only connect to Requirement DIs with the “verifies” link role, and avoiding mistakes that are possible by test users who insert data into the system. This ensures you have greater control over health data and labor measurements.

Another highlight of an ALM framework is that it can do the audit process effectively and expediently. These links allow the associated data to be easily retrieved and displayed; it is faster than searching for the associated data in separate documents, files, spreadsheets, etc. The modular architecture encourages efficiencies because of the shared data.

ALM framework can be modified to allow for many different forms of use. This means an ALM framework is used for configuration management, releases, change control, phase changes and reviews. Some are used in requirements management, test management and construct management. This is achieved by exporting the data from the other systems in preparation for configuration and change management. ALM is able to provide a reasonably limited collection of specific data for audit intent, but does not allow contextual linkage with other specifications, tests, etc. ALM specifically results in the ability to characterize the data well and to clarify what has caused the variance.

Many Aerospace Systems and its expanded procedures provide advanced features called ALM. All of these data elements are captured in the ALM system. The results from applying the advanced ALM methodology are far greater than ones provided by a simple approach to software process improvement. Nonetheless, the advanced approach requires a reliable project data that offers the highest level of data to the world that is collected by an ALM Device.

The “comprehensive” ALM is so full that it includes meeting minutes, action items, correspondence from clients, risk management details, and the project management. This detailed model covers the Asset Management for product line engineering (PLE). The system of real-time capture and control would fully eliminate all previous methods of data entry and backup. Furthermore, this achieves the greatest gain from SOI audits because during an audit all data that the auditor may want to examine is on the same framework and interrelated with the data that is of interest.

2. Methodology Description

Configuration Management

The management of the configuration of embedded avionics systems is important in order to ensure that only the approved software and parameter data files are loaded into the system. Configuration management involves monitoring of specified versions of device data and hardware components.

The "Part" DI is the designator that defines a particular version and the location of a managed data object, document or file. A "Release" DI authorizes a particular version of part for a set reason. It regulates changes to approved sections of the company. The relationships between the three DIs ensures that the data is collected and being properly arranged. A Release DI "authorizes" the use of an owned DP for a particular reason. A Shift DI switches a Component DI from one chunk to another. To create a BOM of system and software components, you can connect one or more Parts with a parent Component and then get the BOM.

Quality audits

Verification and validation procedures are applied in order to ensure that the data generated from the system and software creation is accurate and that the processes followed to create and validate the data complies with the accepted processes and plans of the project. The activities are tracked and monitored on the PTR, Analysis, and Quality Assurance Audit Records.

PTR document guarantees the entry requirements of a phase of growth have been met before conducting any activities in that phase. A "Transition" Report describes and documents a phase transition and provides an overview of the input data required.

A review is undertaken at the end of each phase of production to determine the quality of knowledge generated during that phase. It includes a review process and monitors the review process and related outcomes. DI is a tool by which analysis teams can inform and communicate with each other. If one does a review, then the review will become a conclusion of verifications.

A QA Audit takes place after all phases of the programme to ensure that the data are generated in compliance with approved plans and requirements and that the procedure that follows complies with those agreed. A QA Audit is a required process to close out a construction phase. The Audit DI collects the findings of a QA Audit and recognizes any defects and their corrective measures.

A Transition DI provides a way of moving through the requisite stages of developmental planning A Transformation DI will have to define the need for a particular collection of data. Finally, a Transfer DI provides the proof of effective analysis and acceptance of Part data through a Review DI. The Transition DI consists of restrictions that ensure that the referenced Part DIs is the same Part DIs accepted by the referenced Review DIs. An ALM framework is integral to implementing this restriction as there is a misconception about the rule in manual methods.

A Review of DI defines the location and the basic revision of data which is under review. A Review di also references the shift in a section DI to be reviewed. After the review is completed, the revised draught will be approved. QA audit comes to verify if the checked process has been correctly performed. Besides the QA Audit, the second role of QA Audit is to perform the same task of Transformation DI.

Requirements and Testing

ALM is a repository of specifications, design details, source code and tests for software-centric avionics systems.

A "Requirement" DI captures and monitors the functionality that is required. A text-based DI contains the relevant requirement text if a textual requirement approach is used or a model which represents the functionality or characteristic if model-based approaches are used. Additional characteristics of a DI requirement make the specify allocation and enforcement data.

A "Definition" DI is a specification of the entire framework. Data DIs is used to construct a complete and consistent device data dictionary.

A "Design" DI represents a depiction of the architecture and the flow of data needed to fulfill a function or characteristic of the system. The analytical diagram is usually annotated with text.

A "source" DI defines a "source" DII. Information Resource Management is often used to define Parameter Data Item (PDI) files, which tailor the operation of the device during the operation. All source code can be deployed via source DIs in ALM.

A "Test" DI is used to demonstrate that a particular scenario of activity complies with an accepted norm. These disciples make sure that all practical specifications have been incorporated in the programme correctly and absolutely.

Customer Requirement DI "decomposes" other Requirement DIs reflecting different levels of requirements from high to low. The Level of the requirement is either declared as an attribute of a Generic Requirement or an Attribute category for each degree of requirement. A "Requirement DE" "defines" and "uses" "Definition DIs".

A Concept DI captures the architectural characteristics of a system and applications. And the Source Code DI "implements" one or more Feature DIs and is used to ensure that all Feature DIs have been successfully implemented in the programme.

A Unit Test "verifies" one or more Requirement DIs to demonstrate that the programme performs on target system the intended role. A Test DI also "uses" Concept DIs during the test to test both the device and the programme.

To capture the configuration of the entity (or constituent) Specifications, Description, Design, Source and Test Document, A Part Document states that a particular part (or document, like a Requirements Specification) are a container for a specific collection of these DIs.

It is important to be aware about the effect that changes in the framework has on the Specifications, Concept, Design, Source and Test Disclosures. The Change DI is linked to the DIs through the “Impacts” function. Review DIs is not required, because a Review DI links to a Part DI, which links back to these individual requisites.

Miscellaneous Records and Data

One of the benefits of an ALM system is to collect information in any type. Awareness of this sort is an important part of a creation folder. All of this information can now be stored in an ALM framework and connected to DIs that represent product data such as product specifications, product ratings, product parts and product releases.

Meeting DI captures the minutes of a meeting at which design decisions are made. Minutes stored in an end-to-end lifecycle management system allow information stored in various ways to be handled in way that enables easier access later.

A conference also produces ideas. “Action” lists these ideas. By linking Action DIs to Change DIs, the output of the Action object can be changed. The Meeting DI is also used for development of lifecycle objects of interest with the generic “relates to” connection role.

A recurring issue in group work or interaction is the lack of a permanent record of discussions. Team members are encouraged to log their conversations to promote communication with fellow colleagues. The discussions can be stored indefinitely and then recalled at a later date. Discussions are part of any other subject which has the “relates to” position.

In order to control the risks associated with project, risks are considered. A RISK DI facilitates the monitoring of the status of risks over the lifecycle of the project. Risky objects are connected with the generic "relates to" connection role.

Critical events must be prioritized based on the magnitude of the effect or the likelihood of occurrence. Event (A) is attached with the source (D) with a response “pays attention”. Activity artifacts are correlated with lifecycle artifacts of interest with the generic "relates to" connection function.

3. Findings:

Create document

In order to expediently locate all documents and data upon arrival of an airworthiness certification audit, it is common to create a list of all documents and data available in the project. When you use non-integrated systems to monitor lifecycle, you can spend a substantial amount of time gathering and securing data. Depending on the scale of the project, the catalogue will cover hundreds of items, from various levels of requirements documents, to source code files, software and library, test cases, traceability matrices for each module, programme, test results and test procedure.

In the past, this engineering work was done by junior engineers and it took four engineer-weeks. Using the manual system resulted in incomplete data accumulation resulting in errors in preparation of reported data objects. Inaccurate catalogues typically result in loss of reputation of configuration management activities with the auditor.

The entire data catalogue is largely streamlined with the use of Part DIs, which relates to unique revisions and positions of the records. Reviewing the ALM-generated catalogue should still take place even though the manual audits have been published.

A human-generated catalogue would take much longer to complete. This job takes less than one engineer's work week.

Pre-audit review

A Pre-audit Review is similar to a certification audit and is conducted by the project team to ensure that all information is complete for the audit and ready to be reviewed. This activity reviews lifecycle and project related data to ensure that they are trued, traceable, and eligible according to approved plans and standards.

Legacy data capture mechanisms like spreadsheets and custom databases are time-consuming and cause pain because to locate only one piece of information is hard. Another widely used part of the assessment is the multiple “slices” of inspection of various objects to ensure that the product specifications were properly decomposed and used properly in software. It is important that safety software is scientifically applied and there are no added features that might raise safety concerns. Huge volumes of data must be reviewed to allow the final checked assurance.

In the past, the analysis of a large project has been divided between the production and verification teams and consumed approximately eight engineer-weeks of effort using manual methods and diverse systems.

An "ALM" System is one that is designed to collect and associate this form of data, thus saving on time consuming Traceability is done automatically in the ALM system and there is no need to manually scan through multiple traceability documents. It's as easy as following the ties from DI to DI in the ALM scheme. Many benefits exist from project management simply by capturing all project data in a single framework and in a consistent manner. For example, requirements at the system level are similarly formatted and presented, which makes tasks of evaluating requirements far simpler.

It has been shown that pre-audit analysis can be done in 1.2 engineer-weeks, while the biggest portion of work includes reviewing the specifics of particular DIs (requirements, test cases, etc.) instead of finding and itemizing data. The importance of the pre-audit analysis is enhanced due to its lack of search and retrieval processes and its ability to concentrate on quality lifecycle data.

Traceability

A description of the traceability architecture is compiled to include a map of the data, documents and the sources from which the data can be obtained. Legacy approaches are problematic because they enable a variety of data sources to be collected in various formats. Changes in methodologies to collect and coordinate data must be expressed in the traceability architecture.

I spent more than two weeks working out traceability architecture. This is significantly minimized because of the use of an ALM scheme. This is because the ALM framework needs to establish the traceability architecture before any data can be processed. Together, they constitute the traceability architecture overview. The reducing of the concept of the traceability architecture is the documentation of the DIs and linkages of those DIs, and the depiction of any variations in the DIs depending on their place in the traceability architecture. The discrepancy between Requirement DIs should be reported as the device requirements vary from software requirements.

Locating Documents

During an airworthiness certification audit it is important to obtain the different types of lifecycle data in place. The information assembled for the audit is checked and used to identify records and data for the purpose of the audit. There are errors and omissions in the electronic database at some stage. In a disconnected and disparate setting the manual scans are sent to an un-tasked team member in order to allow for the audit to proceed in another location. The audit turnaround time is long, taking many engineer weeks.

By applying an ALM scheme to the airworthiness audit activities, the companies are able to retrieve relevant data from their risk assessment tool. In order to retrieve the high level requirements that describe the functionality of a particular programme, it is a simple matter of defining the part describing the software requirements that is captured and tracked. If the component issue is found, downloading the document that contains specifications is a simple mouse click away. There is no need to jump from configuration management system to requirements management system, instead the data is already owned and connected to provide for fast retrieval. The act of finding records and data in an ALM system during an audit is reduced significantly compared to legacy systems. Ever since these massive projects were launched, the engineering effort has been calculated in days.

Cross-discipline traceability

An examination similar to the prior audit check is conducted as part of the cross-discipline monitoring. In this activity, we analyze the audit trail from the requirement through all of the definitions to the source code. In addition to research criteria, experiments are performed too.

Pre-audit analysis did not determine a lot of the lifecycle data the cross-discipline traceability evaluation during a formal airworthiness audit. In this method, there was used a manual process of manual searches, web services, marking documents and other items that are searched manually. When auditing is involved, there will be a team of engineers engaged, leading a similar process. Frequent mistakes and omissions in the document/data catalogue, as seen in the report, can take three weeks of engineer time on the larger systems.

An ALM solution would allow traceability to transfer from one division to the next to reduce tracking tables. This action has removed the need to wait for the project team to find and retrieve the data, so the auditor may focus on the cycle objects of concern instead of waiting for the project team to do the proper work.

Finding current status

A project is happening and a couple of data on it could be incomplete. Auditors need to ensure that production and verification activities are being adequately performed and that reports are submitted in time for the final audit.

The project management teams produce progress updates using legacy methods such as spreadsheets to document action items and defect regression logs. The details should be linked to the project to provide a complete image of current project status. Unfortunately this project has consumed about two weeks of time, on average.

Tracking of project status is developed into an ALM framework with the ability to link workflow with each DI. Therefore, it is easy to show that each Change Done Issuer is in a particular state of the workflow. There is an internal monitoring of time given by an ALM device. This knowledge will assist the process management team in assessing and tracking the efficiency of the DI process. Another big benefit of the ALM method is the project dashboard, which displays real-time progress of projects. Using the roll-up features of the ALM system the individual project's status and predictions can be summarized automatically by the ALM system.

4. Conclusion

It has shown that shift from manual data collection and monitoring to a computerized system offers a major improvement in the effort involved in preparing, preparation and execution of the activities associated with airworthiness certification audits. Widespread and standardised documents associated with tests and analyses of an airworthy aircraft enable easy recall of relevant details during airworthiness certification audits. While an ALM system can capture the data, it's the duty of the engineer to ensure that the right and full data is collected and linked. Inaccuracies and omissions waste precious time in audits and contribute to lengthier audit results. Automated confirmation and intervention in the ALM system can be fixed to ensure the traceability mechanisms and the laws and practices of credit. Workflows and associations of pieces of data may be used to implement policies and order procedures to be performed according to approved plans and the requirements for a project. Measuring and monitoring processes are important to the smooth completion of project milestones.

References

[1] M. Gatrell, “The value of a single solution for end-to-end ALM tool support”, IEEE Software, volume 33, issue 5, pp. 103-105, August, 2016.

[2] H. Lin, J. Wu, C. Yuan, Y. Luo, M. van der Brand, and L. Engelen, “A systematic approach for safety evidence collection in the safety-critical domain”, 2015 Annual IEEE International Systems Conference (SysCon) Proceedings, pp. 194-199, April 2015.

[3] A. Sarkis and L. Dias, “A set of rules for production of design models compliant with standards DO-178C and DO-331”, Information Technology: New Generations (ITNG), 2014 11th International Conference on, pp. 27-32, June 2014.

[4] G. Zoughbi, L. Briand, and Y. Labiche, “Modeling safety and airworthiness (RTCA DO-178B) information: conceptual model and UML profile”, Software & Systems Modeling, pp. 337-367, July 2011.

[5] I. Habli and T. Kelly, “A model-driven approach to assuring process reliability”, Software Reliability Engineering, 19 th Annual Symposium on, pp. 7-16, November 2008.

[6] B. Gallina, “A model-driven safety certification method for process compliance”, Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on, pp. 204-209, November 2014.

[7] RTCA, Inc., DO-178C, “Software Considerations in Airborne Systems and Equipment Cerification”, December 2011.