

Automating Compliance for Software Certification

Leveraging Change and Configuration Management to Automate Compliance with FAA DO-178B and Other Federal Compliance Standards

Executive Summary

Many IT professionals who rely on manual methods for configuration and change management are faced with great difficulty when creating and maintaining comprehensive records and detailed documentation trees with complex relationships. These manual processes can be very timeconsuming, error-prone, costly and frustrating for all involved.

This white paper will explore the challenges of change and configuration management by focusing on one industry that has a very strong need to leverage powerful configuration management tools and technologies –commercial and military aerospace manufacturers and their suppliers who are subject to stringent FAA regulations and intricate software certification processes.

This white paper will show how Integrity, a PTC product, can be used to streamline these processes by automating workflow to make the change process enforceable and repeatable across the entire application lifecycle.

Introduction

To help ensure the safety of aircraft developed for both military and commercial use, the U.S. Department of Transportation's Federal Aviation Administration (FAA) has developed detailed procedures for software certification of all new and modified avionics systems. These procedures were designed to help government, civilian, aerospace, and defense firms, as well as their suppliers, measure and document the airworthiness of their airborne systems and equipment, as well as the software processes that support these requirements.

The Radio Technical Commission of Aeronautics (RTCA) DO-178B "Software Considerations in Airborne Systems and Equipment Certification", provides an acceptable means of compliance to the FAA regulations for all of the software aspects of certification. THE RTCA published the first version of the DO-178 specification in 1982. It was updated in 1985, called DO-178A. In 1992, various industry groups published the current working version of the specification, named DO-178B. Today, all new and retrofit commercial, military and space systems have to comply with the FAA regulations for avionics, and all require DO-178B certification.

As the DO-178B specification states, "The testing of airborne software has two complementary objectives. One objective is to demonstrate that the software satisfies its requirements. The second objective is to demonstrate with a high degree of confidence that errors which could lead to unacceptable failure conditions, as determined by the system safety process, have been removed."

All phases of the systems development lifecycle (SDLC)—from defining the business requirement in the systems engineering domain, to engineering/research and development, quality assurance/test and the production/manufacturing assembly line—are affected by the specifications. But adhering to these guidelines for software certification can be very time consuming when using complex, manual processes.

As a result, the avionics industry and other regulated entities have long been in need of a robust, end-to-end set of integrated processes and tools capable of supporting and automating these tedious processes across the entire software development lifecycle.

Configuration Management

Configuration Management is an industry-accepted discipline designed to ensure that the configuration and dependencies of business services and the software assets by which they are comprised are identified, documented, controlled, and tracked. At the core of any configuration management implementation is the Software Configuration Management (SCM) data base, which stores the information about the individual configuration items, as well as the relationship between them. Think of the SCM data base as the "Bill of Materials", or BOM, of your application as it traverses its lifecycle.

Until recently, configuration management has typically been a stand-alone, non-integrated portion of the application lifecycle process, particularly between R&D, the test beds, and the production lines. Configuration management tools formerly were separate, standalone programs that were executed by an assigned configuration management agent whose primary role was to track and maintain version control (VC) and configuration management libraries for application assets and products, which typically consisted of only released code developed by the embedded software engineers in R&D. The integration of the R&D process into a formal production-level configuration management process was typically manual and required disparate tool sets.

It is quite challenging to keep an up-to-date SCM record of all application assets. Manually creating and maintaining these records and their relationships can be very time-consuming, expensive, and error-prone. In addition, creating a BOM without SCM is nearly impossible with all the configuration files, source code, documentation, test data, requirements and project information that must be tracked as the application heads down the "conveyor belt" towards production.

Integrity provides what the industry needs today to solve this issue: A powerful solution that tightly integrates the configuration management processes with the entire SDLC, making configuration management more of a workflow control mechanism rather than a strictly static, stand-alone configuration management process.

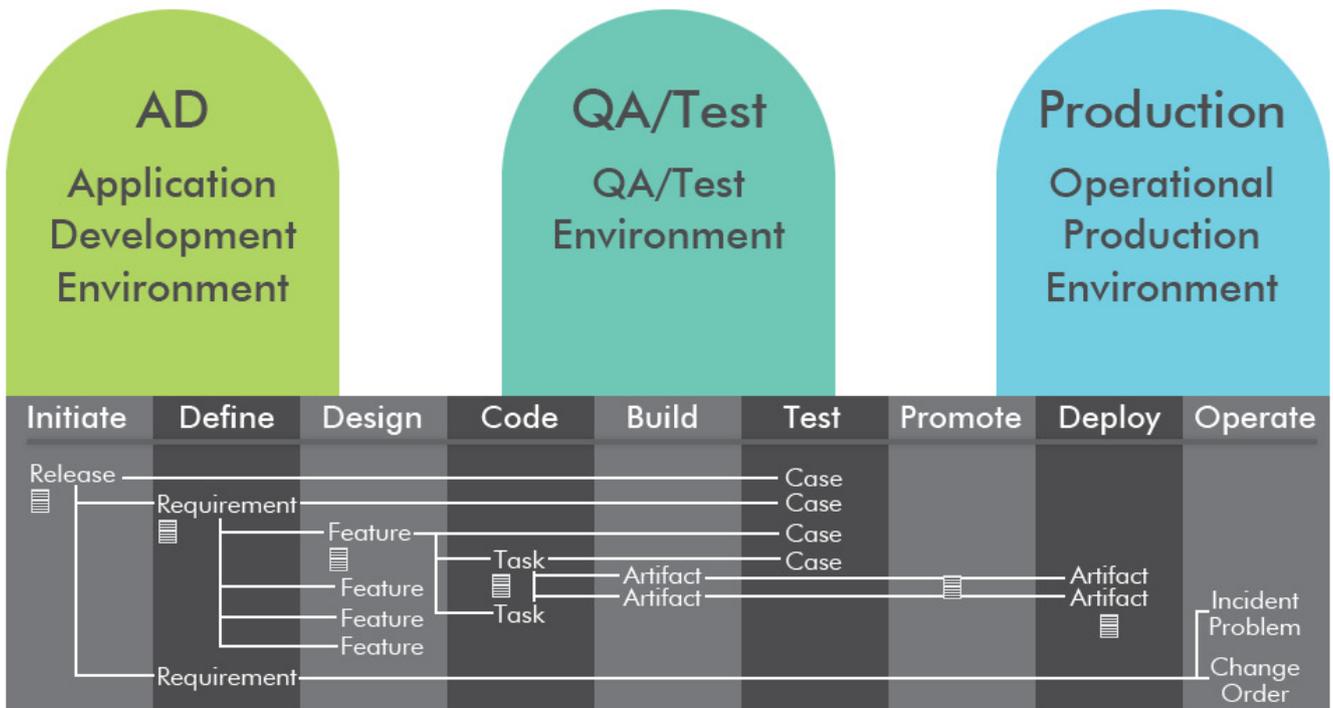
Integrity: Addressing Change and Configuration Management Challenges

Integrity offers a unique approach to solving the end-to-end BOM change and configuration management challenges with Integrity. It provides visibility and traceability into the relationships between the applications and their related assets (e.g. configuration files and settings, O/S level test at, test data, requirements, source code, etc.)

Integrity provides the ability to utilize the change and configuration management process to define and control the entire application lifecycle—from inception of requirement, across development, into test, and finally, upon promotion into production. The ability to control every software configuration item developed for the lifecycle, and not just the code, is

the single most important capability to ensure that production applications consist of what the business, development, test and operations all had in mind when promoting it to production.

Integrity includes a workflow to make the change process enforceable and repeatable—from end-to-end. It simplifies the complexity of understanding and controlling IT elements, including application inter-dependencies, and how they support the intended business processes.



With Integrity change management workflow control mechanisms, these configuration items can also be defined in an IT Infrastructure Library (ITIL)-compliant Configuration Management Data Base (CMDB), all orchestrated using the Integrity process and change management capabilities. With a tightly integrated configuration management process, Integrity workflow can define:

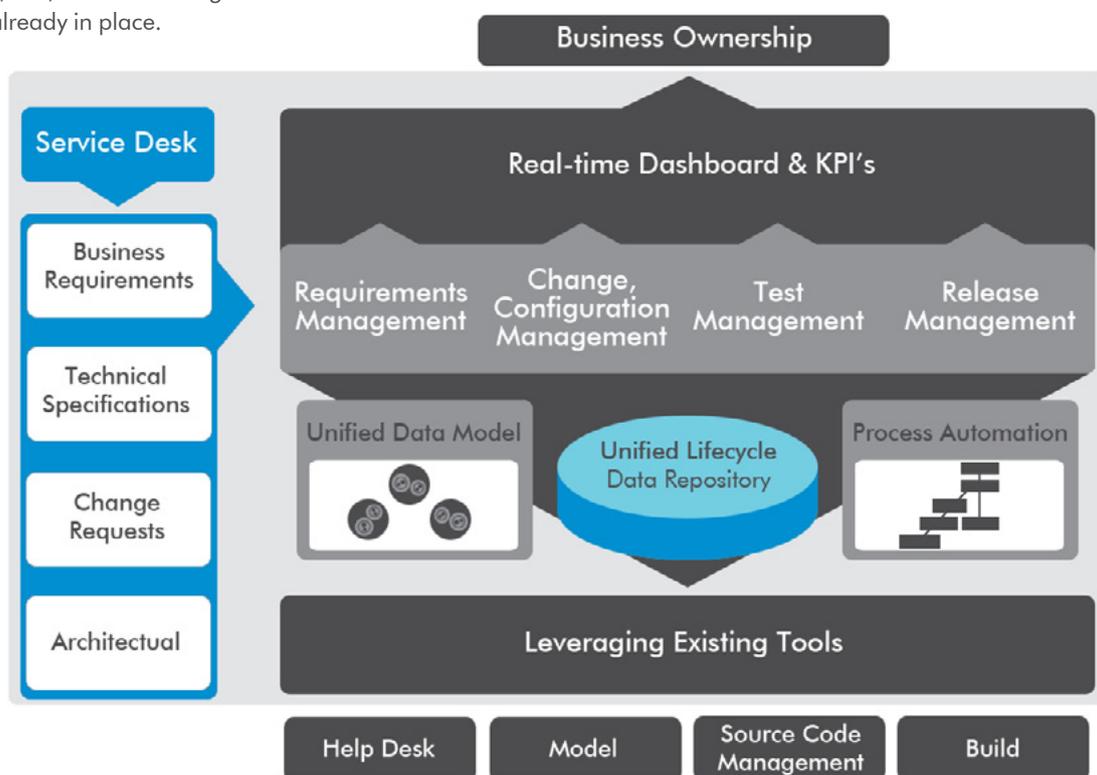
- The roles of all participants in the application lifecycle (e.g. developer, manager, tester, coder, QA, production, change manager, operations, etc.)
- All of the products and components that can be developed over the course of the project (e.g. requirements, source code, test data, scripts, documents, etc). These become part of the BOM.
- The state of each product item within the current application lifecycle (e.g. design, source code, test, maintenance, retirement, etc.), such as approved, rejected, pending release, under revision/change, etc., and can be aligned with Service Desk capabilities already in place.

Utilizing these defined roles, states, and products, Integrity can then provide visibility into project and portfolio management and metrics collection to report on the current state of the project automatically, or show the current state of an incident ticket from a service desk currently being worked on via the defect management process in the application development group.

Application Configuration Management Integration

Integrity’s change management process supports software engineering by ensuring the integrity of software products. A significant difference between the current software standards and previous standards is the emphasis on integrating configuration management into the software engineering process—without “slowing down”the development activities. Another difference is the type and variety of products that are to be controlled.

In the context of Service Oriented Architecture (SOA), all products that results from applying the process-methods-tools approach are to be controlled. These include models, analysis products, architectures, services, the output from other design products, test cases, test scripts, builds, data bases, source code, configuration files/settings, and any other work product produced or used by the project.



Configuration Management is essential to ensure that a product's integrity is not compromised or changed in an ad hoc manner once it has been evaluated and satisfied its completion criteria. Software Engineers must have full confidence and assurance that the products they need as an input are in their "as-evaluated" configuration. This confidence must also flow down the BOM conveyor belt > through test and into production.

With Integrity, configuration management is integrated into the software process through the instantiation of process models that define the steps to be followed to produce the products, the methods used, and the tools that implement the method. At any point in time, there is a record of the product in work, in the repository, and under change control. Change records are maintained for all products, along with the change history associated with each product. The environment tracks the products through their complete lifecycle and interfaces directly with the release system and the Service Desk.

Integrity Support for DO-178B and other Federal Compliance Standards

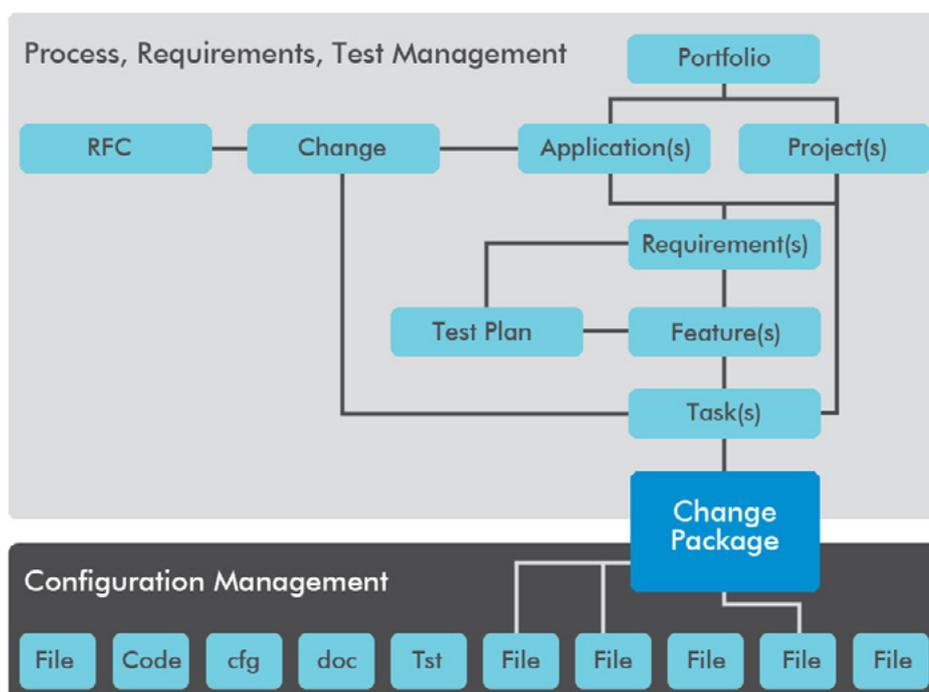
DO-178B defines a set of processes that are integral to the software development process. It specifies that every line of code be directly traceable to a requirement and a test routine, and that no extraneous code outside of this process be included in the build. As part of this process, extensive documents, and records must be created and maintained, including detailed software configuration and change management records, for each step along the conveyor belt for the BOM.

Integrity provides a best-in-class solution for software certification, since it automates workflow to make the change process enforceable and repeatable.

Another key benefit of Integrity is that it can be leveraged across the entire software development lifecycle. DO-178B key requirements that relate to and can benefit from Integrity include:

- Software Planning Process
- Software Verification & Validation
- Software Configuration Management
- Software Release Management
- Software Change Management
- Software Quality Assurance
- Certification Liaison (Compliance Process)
- Software Lifecycle Data (Environments)

Integrity addresses all of these functional areas, across the entire application lifecycle, facilitating the creation and maintenance of the documents and records required for obtaining software certifications.



Summary

Using Integrity, organizations can instantiate their change management best practices and methodologies to uniformly plan, deploy, and manage changes, hiding the complexity of version control and testing tools while leveraging their functionality. Integrity's integrated approach also enables analysts, developers, testers, database administrators, and operators to collaborate effectively through automated best-practice processes, improving quality and speed while lowering costs. This feature, using the BOM conveyor belt illustration, can augment existing Service desk's change management capability by providing visibility across the lifecycle and maintain that visibility live, rather than with a static incident ticket.

Integrity Business Unit Locations

North America
1 800 613 7535

United Kingdom
+44 (0) 1252 453 400

Germany
+49 (0) 711 3517 75 0

Asia Pacific
+65 6830 8338

Japan
+81 3 5422 9503

integrityinfo@ptc.com

For more information visit: [PTC.com/products/integrity](https://www.ptc.com/products/integrity)

© 2011, Parametric Technology Corporation (PTC). All rights reserved. Information described herein is furnished for informational use only and is subject to change without notice. The only warranties for PTC products and services are set forth in the express warranty statements accompanying such products and services and nothing herein should be construed as constituting an additional warranty. References to customer successes are based upon a single user experience and such customer's testimonial. Analyst or other forward-looking statements about PTC products and services or the markets in which PTC participates are those of the analysts themselves and PTC makes no representations as to the basis or accuracy thereof. PTC, the PTC Logo, Mathcad, Creo, Elements/Pro, and all PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States