Chapter 17
A Hybrid Intelligent Risk Identification Model for Configuration Management in Aerospace Systems

Jose Nava
Pinnacle Aerospace, Inc., Mexico

Alejandro Osorio
Pinnacle Aerospace, Inc., Mexico

ABSTRACT

This chapter proposes a multi-dimensional patterns recognition model for Configuration Management's Risk Identification in Aerospace Safety Critical Systems. This work has been designed for Aerospace software systems where companies require full compliance with the Aerospace Standard DO-178b. The solution focuses on Risk Identification for the Configuration Management Process Area. An Anomaly Detection Solution has been designed through the modeling of statistics and artificial intelligence algorithms, following CRISP-DM model standard for data mining solutions. A dimensional architecture was designed to model the problem through three dependent and interconnected dimensions. The first dimension, Behavioral Biometrics, which this model has extended to Human Behavioral Patterns. The second dimension is Infrastructure, which represents all physical specialized equipment, environments, networking, and its configurations. The third dimension is space-time, which in this model represents a time dimension against all geographical information project related (code, files, among others).

INTRODUCTION

Software products are deployed across a wide range of global industries, but when it comes to Aerospace safety critical systems; security and criticality are strictly rigorous. In these kinds of systems, a software failure or malfunction could result in loss of life and significant property damage.

Aviation systems development has been evolving for almost a hundred years now. One of the more notorious development evolving areas is the instruments and displays that were electro-mechanical in the past and now are composed by electronic parts, which make them more reliable, secure and lighter. The

DOI: 10.4018/978-1-4666-9779-9.ch017

biggest priority of this evolution has always been to avoid aircraft accidents and providing security in the air. The rapid increase in the use of software in airborne systems and equipment used on aircraft and engines in the early 1980s resulted in a need for industry-accepted guidance for satisfying airworthiness requirements. DO-178, "Software Considerations in Airborne Systems and Equipment Certification", was written to satisfy this need.

Developing reliable software products becomes more and more challenging for Safety Critical Industries due to specific regulations, short production cycles or high complexity design.

One of the more challenging aspects when working with Aerospace Software is maintaining a good Configuration Management control. A well planned strategy for this area can result in the fault tolerant system we have designed since the beginning.

Configuration Management has always been a complex, dynamic and constantly changing area, which not only interacts with the project team members and the IT department of the service provider, but also with those entities from the client side. This configuration makes it more complex because each company has its own Configuration Management practices, tools, and processes. Other important risk factor is that no matter the technical level of the involved teams, each employee works differently when it comes to practices like code design, SVN activities like commits, check in/out, updates, merges, syncs, cleanups, or other activities like estimation, activities tracking culture, among others.

The Federal Aviation Administration and the Joint Aviation Authorities have defined a list of Failures Condition Categories within DO-178b, as well as a list of Software Level Definitions based upon the contribution of software to potential failure conditions.

The Software level implies that the level of effort required showing compliance with certification requirements varies with the failure condition category (Radio Technical Commission for Aeronautics, 1992). These software level definitions are described below:

- **Level A (Catastrophic):** Software whose anomalous behavior would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the aircraft, and multiple deaths. An example of this anomalous behavior can be the Turbine Engine Monitoring Software, which malfunction can cause a fatal accident.
- **Level B (Hazardous/Severe-Major):** Software whose anomalous behavior would cause or contribute to a failure of system function resulting in a hazardous/severe-major failure condition for the aircraft, and some deaths or severe injuries. An example of this anomalous behavior can be the Landing Gear Control Software, which malfunction can cause a big accident.
- **Level C (Major):** Software whose anomalous behavior would cause or contribute to a failure of system function resulting in a major failure condition for the aircraft, and severe injuries. An example of this anomalous behavior can be the FMS/NAV/COM System, which malfunction can cause damages and accidents.
- **Level D (Minor):** Software whose anomalous behavior would cause or contribute to a failure of system function resulting in a minor failure condition for the aircraft, and minor injuries. An example of this anomalous behavior can be the A/C monitoring system software, which malfunction can cause a failure condition.
- **Level E (No Effect):** Software whose anomalous behavior would cause or contribute to a failure of system function with no effect on aircraft operational capability or pilot workload. An example of this anomalous behavior can be the Entertainment audio system software, which malfunction can cause just a minimal failure condition.