Proceedings of the International Conference on Aerospace Science and Technology
26-28 June 2008, Bangalore, India

INCAST 2008-013

VALIDATION OF CONTROL PARAMETERS FOR A RE-CONFIGURABLE ALGORITHM IN A FLIGHT CRITICAL AVIONICS APPLICATION

CM Ananda

Aerospace Electronics & Systems Division, National Aerospace Laboratories, Bangalore, India,
ananda_cm@css.nal.res.in

ABSTRACT: Earlier generation avionics, federated architecture (FA) is used where each function has its own independent, dedicated fault-tolerant computing resources. To overcome few disadvantages of federated architecture, NAL had developed and proposed a re-configurable algorithm for avionics flight critical software applications under integrated time and memory partitioned applications. The algorithm uses four control parameters, which define the re-configurable state of the system in real time. It also preserves the advantages of non-Reconfigurable systems over federated architecture. The availability of the avionics applications increases substantially with the use of this new algorithm

The paper presents a detailed validation process, methodology and data dictionary for control parameters namely: re-configurability Information factor, Schedulability Test/TL/UF, Context Adaptability/suitability and Context Flight Safety. The algorithm is data centric and interfaces system health as control input and initiation of the re-configuration is only after successful evaluation of the parameter metrics. The control parameters are validated against the statistical data generated based on the system design analysis like FMEA, FHA, SSA and the basic architecture of the system. Since the control parameters define the re-configuration state, it is very critical to verify and validate the correctness of the control. Parameter characteristic data as it leads to critical action in flight. This enhances the availability and reliability of the system under failed conditions by efficient selection and procedural re-configuration with safe state exit. Invalid failure of control parameter validation brings the system to safe state. The scheme, algorithm and the control parameters validation metrics and their validation approach are described with experimentation using VxWorks environment.

1. INTRODUCTION

The avionics systems and software architecture of federated era was no doubt very good in terms of the fault containment, fault tolerant and a sort of fool proof architecture. However, this has disadvantages like, increased weight, redundant computer resources in each Line Replaceable Unit (LRU), higher looming volume, electrical interfaces complexity and physical maintenance. The advances in computer technology encouraged the avionics industry to utilize the increased processing and communication power and combine multiple federated applications into a single shared platform [1]. The Integrated Modular Avionics (IMA) was developed for integrating multiple software components into a shared computing environment [2]. This is powerful enough to meet the computing demands of multiple applications using common hardware and system resources. The IMA integration has the advantage of lower hardware costs and reduced level of spares inventory.

1.1 Motivation and related work

Current system behavior in the event of a task failure is to declare system failure resulting in non-availability of either part or full partition functionality. Here the failure recovery, by removing the faulty task or replacing by a new task is not exercised. However, all the failures cannot be re-configured due to the safety and criticality of the avionics applications. Re-configurable algorithm [3] has the desirable feature of reconfiguring the critical tasks or removal from the schedule to enable continued functionality of the non-faulty partition. The novelty of the proposed algorithm is of reconfiguring the critical tasks or removal is by using control metrics [4]. This re-configuration algorithm is based on rule based decision-making approach and control metrics coupled with state and condition matrix. The algorithm is described for a typical multi partitioned multiple process task based architecture [3][4]. Control metrics parameters plays crucial role in re-configuration and hence the validation of these parameters are critical in realizing the efficient re-configuration.

2. ORGANIZATION OF TASK OR PROCESS SCHEDULER IN A TYPICAL AEROSPACE AVIONICS APPLICATION

Typical aerospace IMA applications employ multiple functionalities with the same hardware and system software resources.

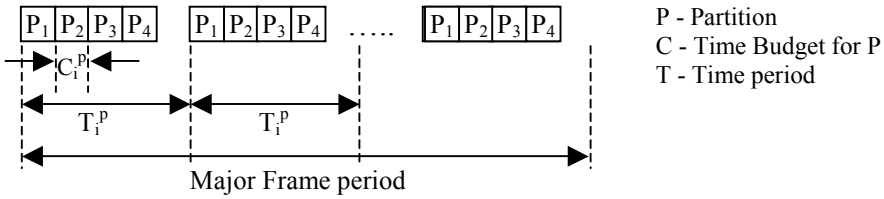

Fig. 1. Static table schedule diagram with partition period and process execution duration

This uses the concept of major frames, multiple partitions and each partition having multiple processes to schedule the tasks. Fig. 1 shows the set of partitions [5], which are scheduled across a major frame M consisting set of partitions and each partition having set of tasks/process (typical integrated avionics ARINC 653 based application). Major frame consists of number of partitions with each partition having set of process and each process having set of tasks. Consider a major frame M having a set of partitions $Pt_i..Pt_n$ based on functionalities. Each partition Pt_i consists of a set of process $Ps_i..Ps_n$ based on the applications sub functionalities. The number of partitions and number of processes in each partition is a trade-off to get the real time response based on the capabilities of the hardware and software together. The representation of major frames, partition, processes and each process with number of tasks represented as (1)

$$M = \begin{bmatrix} Pt_1 \\ Pt_2 \\ Pt_3 \\ . \\ Pt_n \end{bmatrix} = \begin{bmatrix} Ps_{11} & Ps_{12} & Ps_{13} & . & Ps_{1n} \\ Ps_{21} & Ps_{22} & Ps_{23} & . & Ps_{2n} \\ Ps_{31} & Ps_{32} & Ps_{33} & . & Ps_{3n} \\ . & . & . & . & . \\ Ps_{m1} & Ps_{m2} & Ps_{m3} & . & Ps_{mn} \end{bmatrix} = \begin{bmatrix} \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n \\ \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n \\ \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n \\ & & \\ \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n & \tau_1,\tau_2,...\tau_n \end{bmatrix} \quad (1)$$

Each process P_s consists of set of tasks $\tau_1...\tau_n$ and the sequence of tasks are predefined and priorities are fixed as per static table scheduling mechanism.

3. RE-CONFIGURATION ALGORITHM

3.1 Control parameters for the proposed algorithm

The re-configuration algorithm is implemented based on four major metrics, which are the heart of the algorithm in re-configuration. The Re-configurability Information-Factor, Schedulability Test/TL/UF, Context Adaptability/ Suitability and Context Flight Safety Factor are the efficient decision-making control parameters [3] defined and used in the algorithm. Based on these control metrics, the re-configuration GO/NO-GO is decided.

3.1.1 Re-configurability Information-Factor (RI)

Re-configurability Information Factor (RI) is defined as the ratio of re-scheduled Task or Process Functional Credit Point (FCP) to the original scheduled task or process FCP. Credit point is represented in the range of 0 to 1. For every selected critical task (τ_s) in a major frame consisting of number of scheduled lists, there can be at least one configurable task (τ_r). The selection of replaceable task is based on the RI and is expressed as

$$(\tau_s = \tau_r) \leftrightarrow (RI(\tau_s) \geq RI(\tau_r)) \text{ or } (Ps = P_r) \leftrightarrow (RI(P_s) \geq RI(P_r)) \quad (2)$$

FCP is derived based on the type of task, criticality of the task and phase of application envelope. Every element of task matrix in (1) has corresponding credit point matrix and are derived from the system requirements, design limits and Failure Mode Effect Analysis and Testing guidelines.

3.1.2 Schedulability Test (Time Loading TL or Utilization Factor UF)

Schedulability Test is the standard method of testing the time loading or utilization for a task to be scheduled

$$(\tau_s = \tau_r) \leftrightarrow \left(WCET(\tau_s) \leq WCET(\tau_r) \right) \text{ and } (\tau_s = \tau_r) \leftrightarrow \left((\sum_{i=1}^{s_n} \frac{C_{s_i}}{T_{s_i}} \leq \sum_{i=1}^{r_n} \frac{C_{r_i}}{T_{r_i}}) \right) \quad (3)$$

For all cases of task phasing, a set of n tasks will always meet their deadlines [6] if utilization time ≤ 0.69. Each task is benchmarked with the execution times and the same is used in real time for the algorithm. For selected critical tasks, reference execution time dataset is compiled and generated in accordance with (1). Re-configurable algorithm, which uses (3) as one control parameter input is tested using the data captured from a live flight critical project. The algorithm checks this reference dataset for task selection criteria.

3.1.3 Context Adaptability and Suitability (CAS)

Context Adaptability and Suitability metric decides acceptability of the faulty task replacement in real time. The context of the scenario is verified and validated for the functionality and context suitability of the task. Context Adaptability and Suitability (CAS) is defined as

(CAS=TRUE) ↔ (Re-scheduled Task or Process Context Flag is equal to Original Task or Process Context Flag) (4)

Every task in a process and partition has the CAS flag dictating the function's use at that point of time using task reference dataset condition table. However, each task can have more than one suitable tasks depending on the prevailing scenario (phase of flight) in real time. The CAS condition table used in the algorithm is derived based on the system functionality and inter system re-configuration dependencies based on Failure Mode Effect Analysis (FMEA) and Failure Hazard Analysis (FHA) along with System Safety Assessment (SSA).

3.1.4 Context Flight Safety Factor (CFS)

It is very vital in aerospace flight critical applications to check the safety of the system before and after re-configuration. The system is checked for safe state to initiate re-configuration. For aircraft systems in closed loop control, a wrong function being re-configured can lead to catastrophic failure. Hence any action carried out in real time is verified and validated thoroughly by all the control parameter artifacts along with the system information. Context Flight Safety Factor (CFS) is defined as

(CFS = TRUE) ↔ ((Re-scheduled task or process Safety Factor / Original scheduled task or process Safety Factor) ≥ 1.0) (5)

CFS is derived from both RI and the Safety Units (Su) based on the Failure Hazard Analysis (FHA), Failure Mode Effect Analysis (FMEA) and System Safety Analysis (SSA)[7]. Every element of task matrix in (1) has corresponding Safety Unit matrix, which will be used by (5). Su is a measure of margin of system safety to re-configure a task with the prevailing dynamic context of the flight.

3.2 Condition, status and state information

Input reference dataset for the control parameters used in the algorithm depends on the information of the system and are captured by system design and analysis, sample Implementation on typical platform, aircraft level Failure Hazard Analysis (FHA), system level Failure Mode Effect Analysis (FMEA),

FAA/TSO requirements for aerospace flight critical systems and System Safety Analysis (SSA). The dataset for each of the control parameters are captured from live projects of flight critical in nature during the design and integration phase. Each control parameter will have dataset captured with varying real time scenarios.

3.3 Simulation and experimental data

A sample schedule partition is simulated in Matlab Simulink using the state machines to check the time loading and execution scenarios and the details are covered in [3][9] which uses additional toolsets like Torsche and True Time.

Various datasets used by the control metrics are FCP, TL, CAS Flag and SU matrix. As described the data for all these data sets are derived from tests, analysis, design guidelines and safety studies of critical systems. These datasets are verified, checked and validated for their correctness and validity before its use for the algorithmic implementation. CFS is critical in terms of safety requirements and hence the validation of CFS is addressed in this paper. CFS mainly depends on the Safety Units (SU), which in turn depends on software metrics of design and code [8]. CFS is validated using

a. ***Defect Density Measure*** **(DDM)** is expressed as

θ_{cd} is cumulative defect ration of design
α is total No. of Reviews
N_i is total No. of Unique defects in the ith design review
L is source lines of design reviewed in thousands

$$\theta_{cd} = \sum_{i=1}^{\alpha} N_i / L \qquad (6)$$

b. Code and Unit Test Phase Measure

γ_{cd} is cumulative defect ration of code
α is total No. of Reviews
M_i is total No. of Unique defects in the ith code review
SL is source lines of code reviewed in thousands

$$\gamma_{cd} = \sum_{i=1}^{\alpha} M_i / SL \qquad (7)$$

c. Mills Model

N_l is maximum likelihood of the unseeded faults
N_{sf} is the number seeds faults
m_{fu} is the number unseeded faults uncovered
m_{sf} is the number of seeded faults discovered

$$N_l = \lfloor N_{sf} m_{fu} \rfloor / m_{sf} \qquad (8)$$

Based on the validation metrics, the following data was generated as part of a typical avionics application to implement CFS in the re-configuration algorithm.

Tasks	CFS	Tasks	CFS	Tasks	CFS	Tasks	CFS	Tasks	CFS
InitProc	1.0 1.0 1.0 0.9	InputProc	0.85 0.91 1.0 1.0	LogicProc	0.97 0.92 0.81 0.84	CompProc	0.96 0.9 0.98 -1	FrmtProc	0.86 0.91 1.0 -1
OutpProc	1.0 0.9 0.95 1.0	DispProc	1.0 0.95 0.91 -1	FltMngt	1.0 0.95 0.94 -1				

The multi-partition multi-task schedule is designed using 7447 PPC hosted with VxWorks AE 653 platform. The timing diagram captured using the Wind River system viewer is shown in Fig.2. The algorithm is implemented with four partitions tasks and the fourth partition as a monitor, which implements the algorithm. Fourth partition decides and declares the decision of re-configuration based on the real time scenario of partition 1,2 and 3. The datasets are validated and verified using CRC algorithm implemented in Xilinx FPGA for a typical application of AFDX protocol design and simulation.

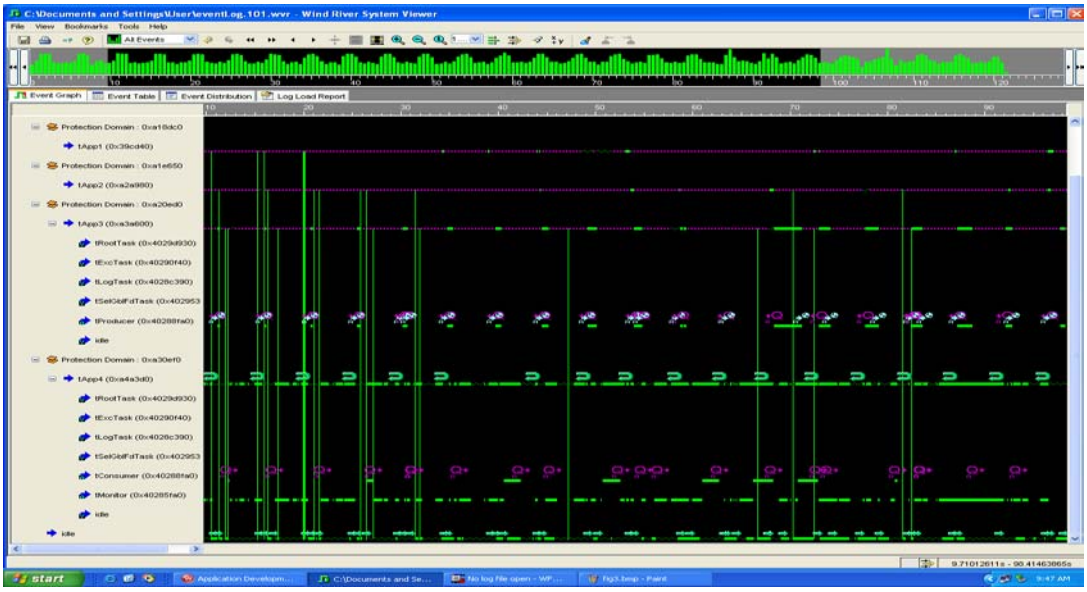

Fig. 2 Partition time capture in VxWorks environment

4. CONCLUSION AND FUTURE WORK

The complete algorithm with control metrics is implemented using VxWorks AE 653 utilizing the time and memory partitioning mechanism to implement the multiple partitions, multiple process and multiple tasks in each process. Work is being done in optimization of the control parameter validation process for task selection and compiling the required reference dataset for the algorithm using flight critical open architecture platform. Also the algorithm fault scenarios are being evolved and studied using VxWorks AE653 platform implementing flight critical application and neural network model using Matlab Simulink.

ACKNOWLEDGMENT

Author thanks Dr. SV Narasimhan, Deputy Director, National Aerospace Laboratories for his guidance and motivation from time to time. Author also thanks Prof. Y Narahari, CSA IISC, Prof. S Govindarajan, SCRC, IISC, Dr. BS Adiga, Dr. MR Nayak, Head ALD and Dr. AR Upadhya, Director NAL.

REFERENCES

[1]. ARINC report 651, Design Guide for Integrated Modular Avionics, Published by Aeronautical Radio Inc., Annapolis, MD, November 1991

[2]. ARINC Specification 653-1, Avionics Application Software Standard Interface, Published by Aeronautical Radio Inc, October 2003

[3]. CM Ananda, Improved availability using re-configuration algorithm in a flight critical system 26th Digital Avionics Systems Conference (DASC), Dallas, Texas, October 21-25, 2007.

[4]. CM Ananda, May 2007, *Avionics for general aviation light transport aircraft: An insight into the avionics architecture and integration*, AIAA Southern California Aerospace Systems and Technology Conference, Santa Anna, California, USA

[5]. Neil Audsley and Andy Wellings, 1996, Analyzing *APEX Applications*, IEEE Real Time Systems Symposium RTSS

[6]. Loic P Briand and Daniel M Roy, *Meeting deadlines in Hard Real-Time Systems The Rate Monotonic Approach,* IEEE Computer Society, 1999

[7]. IEC 60812, 1985, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), IEC 60812 Ed. 1.0 b: 1985

[8]. BS Dhillon, Design Reliability: Fundamentals and Applications, CRC London New York Washington D.C, 1999

[9]. Stibor Miloslav, Kutil Michal, Torsche scheduling toolbox: ListScheduling, 7th International Scientific–Technical Conference–PROCESS CONTROL 2006, Kouty and Desnou, Czech Republic, June 13 – 16, 2006