

Issues in Design and Development of Reliable Configurable Distributed Checkout and Launch System for Mission Critical Aero-Space Flight Vehicles

Shivpal Singh, Bhogendra Rao PVRR

Abstract: Role of Configurable Distributed Checkout and Launch System (CDCLS) is pivotal in carrying out quick health checks and launching of Aerospace Flight Vehicles. Configurable Distributed Architecture provides flexibility for connecting nodes and scaling Distributed System. Different configurations can be derived from the Master Configuration. Since, Ultra high reliability and infallible performance of the CDCLS is of paramount importance, Safety criticality and Mission criticality analysis needs to be carried out for determination of mission critical parameters. These critical parameters need to be addressed by required fault tolerant architecture, which can be implemented in Hardware and Software for achieving system reliability objective (Say, 0.99).

Keywords: Distributed System, Launch System, Reliability, Fault Tolerance, Automated Testing, System validation.

I. INTRODUCTION

Automated testing of complex technical equipment involves challenges due to multi-disciplinary nature of the system, inadequacy of technical equipment, cost and schedules. However, such test equipment is highly essential to ensure required reliability and quality of the system under test within the stringent time deadlines of delivery, in addition to test time reduction[1].

The Checkout and Launch System is an automated test equipment for aerospace vehicles. It performs comprehensive health checks of Sub-Systems and integrated Missile Systems/space vehicles and Launch operations. In view of mission criticality, technological complexity, high value, enormous efforts put in towards realization of Aerospace Flight Vehicles (Satellite System, Missile System, Aircrafts, etc.), due attention needs to be paid towards optimal design of Configurable Distributed Checkout and Launch System. Distributed Checkout and Launch System is interfaced with Nodes, Digital Controller, Missile Sub-Systems and Launch Systems.

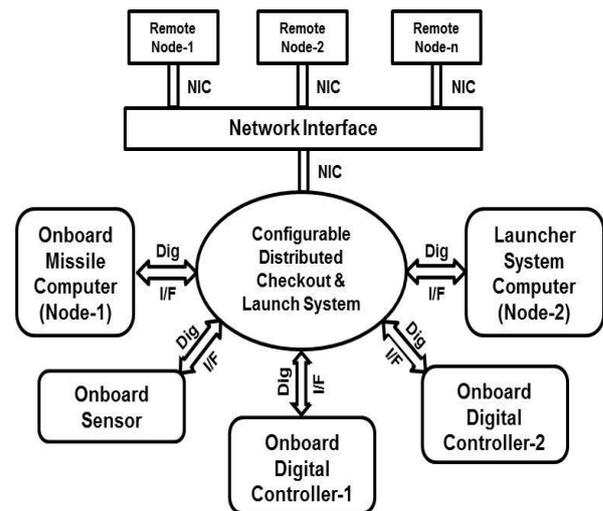


Figure 1. Distributed Architecture of Configurable Checkout and Launch System

Distributed Checkout and Launch Systems for Missile Systems and Flight Vehicles have been designed and realized. The System could be exploited for Checkout and Launch Missions. Issues related to reliability, consistent performance, expandability, configuration, etc. encountered have been addressed.

Organization of this paper is as follows. Section II gives earlier work carried out in this domain. Section III discusses requirement of distributed checkout and launch systems, section IV presents modular and configurable checkout and launch system. Section V discusses how to design such systems for reliability. Section VI presents the software reliability model to achieve the required reliability. Section VII presents testing and evaluation methodology followed to achieve the required reliability and the paper concludes with section VIII.

II. EXISTING SOLUTIONS

The history of Automated Test Equipment was discussed in [2] and technology prediction was presented in [3]. The trends in ATE technology were brought out in [4] in detail. A detailed introduction to the next generation ATE systems is given in [5].

Revised Manuscript Received on March 18, 2020.

Shivpal Singh, M.Tech, Computer Science, IIT, Madras.

Dr PVRR Bhogendra Rao, Ph.D in Computer Science from JNTU, Hyderabad.

Various attempts have been made by researchers and industry in development of such automated systems in past for various complex systems like [6] [9] [7] [8] and they clearly brought out the advantages of using automated test equipment. These systems are mainly meant for electrical and electronic industry. There were attempts made by industry for, development of checkout and launch, systems for aerospace vehicles [10] [11].

These systems are not configurable systems. An architecture of a configurable ATE is presented in [12]. An open architecture for test systems was presented in [13].

The issues and challenges involved in development of Automated Test Equipment for such complex systems were discussed in [14] [15] [16] [17] [15].

However, these papers did not address the issues and challenges involved in developing a distributed configurable automated test equipment. In this paper we are presenting those issues and challenges involved in development of a distributed configurable checkout and launch system in this paper.

III. DISTRIBUTED ARCHITECTURE OF CONFIGURABLE CHECKOUT AND LAUNCH SYSTEM

The requirements of automated test equipment were discussed in depth in [18] [19]. Various architectures available in the literature were evaluated [20]. The following important parameters are motivating factors for design of Distributed Checkout and Launch System.

- System Reliability (Mission Criticality)
- Flexibility in connectivity and integration
- Modularity
- Maintainability
- Interface Management (Interface definition)
- Horizontal Scalability
- Configurable design

Operational requirements necessitate communication channels which work reliably over longer distances with low latency, low propagation delays, tolerable communication errors and low deployment time. The Design of the System caters for aforesaid requirements through connectivity of widely separated heterogeneous and hybrid digital Systems with digital interfaces (RS422, RS485, 1553B, Ethernet). Launch Operations of Flight Vehicles (Missiles) can be carried out remotely.

Each Node/Computer connected through Bus is an autonomous System with adequate internal computational /processing capability and local intelligence. This Architecture facilitates minimizing inter-dependence thereby providing high degree of independence and modularity as shown in fig. 1.

The above critical parameters have been implemented in the design of the CDCLS for Missile System.

IV. MODULAR AND CONFIGURABLE DESIGN

Design approaches for automated test equipment have been discussed in depth in the available literature [21] [22] [23]. Emphasis was given on modular and configurable design of

the CDCLS. Modular design is useful from the point of view of testing and evaluation, expansion of system capabilities and maintenance.

The System design was configurable in nature so as to enable the system for configuring it for different users and for different variants of device under test through test settings and ATE configuration. Hardware and Software dependencies related to a particular type of System are localized within periphery of the System. There is dedicated software controlled configuration definition mechanism defining the Configuration of a particular System. The configurable design provides high level of flexibility to connect different types of systems in different configurations and the same system can be employed for several similar systems.

V. SYSTEM RELIABILITY

High degree of reliability is essential for the Mission critical System such as the system under discussion as they System operation involves man-in-loop. Various system reliability models and design for reliability were discussed in [24] [25]. Analysis of fault coverage to increase the system reliability was presented in [26]. Required System reliability was achieved by implementing fault tolerance at hardware level and software level as discussed in following subsections.

A. Hardware Fault Tolerance by Design

As part of criticality analysis of complete system, identification of hardware critical components is essential during design phase. Critical components may be related to risk, mission or safety. Mission critical system is required to be designed such that it continues functioning as intended even in presence of physical fault (hardware defect) and software design fault.

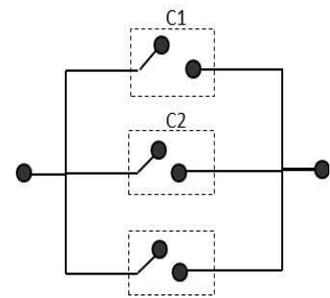


Figure 2. Fault Tolerance through Redundancy

of physical fault (hardware defect) and software design fault.

Therefore, comprehensive approach, to fault management, which includes fault avoidance, fault detection, fault removal and fault tolerance, is necessary to achieve required high system reliability. Based on criticality analysis of the system, critical hardware components should be provided with necessary hardware double or triple fault tolerance as shown in fig. 2.

Based on high criticality of hardware components, fault tolerance is incorporated by employing redundancy in hardware components. Based on criticality analysis of the system, critical hardware components should be provided with necessary hardware reliability. If single component does not meet reliability requirement, necessary fault tolerance needs to be incorporated.

Design Implementation of fault-tolerance for a mission critical hardware component viz. C1 with individual component hardware reliability of 0.80 and reliability objective (0.99) is determined as shown in fig. 2. The Reliability of 3Nos Components connected in parallel is computed as follows:

$$R = 1 - (1 - R_{c1})^3$$

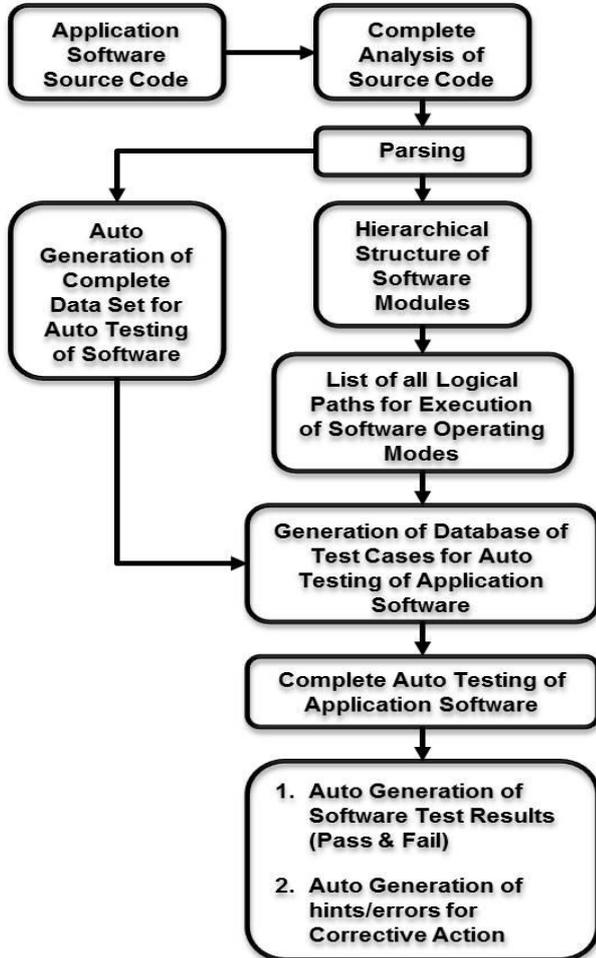


Figure 4. Software Reliability Assessment Model

$$= 1 - (1 - 0.80)^3$$

$$= 0.99$$

Thus over all reliability is increased from 0.80 to 0.99. Mission critical parameters viz. System Flap Open/Closing Sense, Launcher Platform Elevation Angle, Onboard Battery voltages, Onboard Air bottle pressure, etc. were designed to have fault tolerance for achieving high performance.

B. Software Reliability by Design

The complexity of software, in general, is very high for mission critical distributed systems [27]. Various software architectures were studied [28] [29] and middleware were evaluated [30] [31] to arrive at a reliable software architecture for distributed [32] checkout and launch system application. Response time analysis was performed on the real-time task set [33].

High Software reliability is achieved by implementing fault tolerance for highly critical software components (Modules) through N-Version programming (i.e. multi-version software) and not through software redundancy. Software redundancy

could be failure-prone, because, in such case, existing software fault would get propagated in redundant part also and hence this may lead to software failure with serious consequences.

N-Version software is achieved through independent generation of N2 functionally equivalent programs called versions by independent software development Groups.

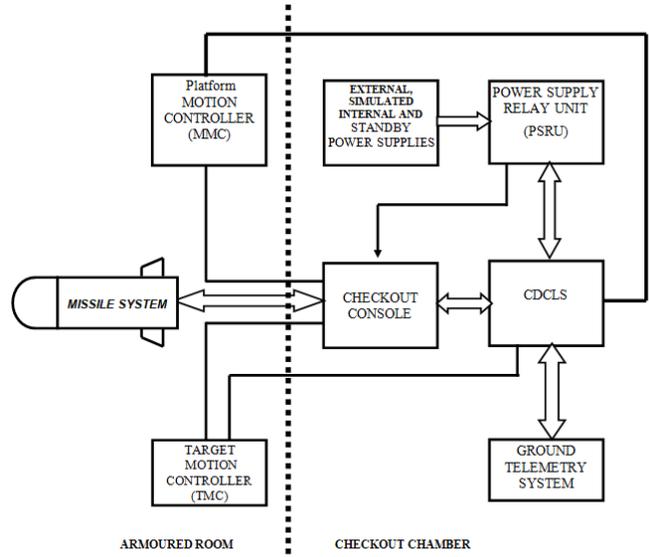


Figure 3. Test Configuration

N-Version Software fault tolerance is implemented in the CDCLS of the Missile System.

C. Design of Fault Tolerant Application Software Communication Protocols

The communication protocol between the checkout and device under test need to be fault tolerant [34]. Due to long length and capacitive effect of data communication lines between CDSLS and Onboard Computer, data may get corrupted specially at higher bit-rate and hence byte command is not recognized as a valid command thereby affecting system performance and mission. Therefore, it is strongly proposed that command bytes and mission critical data be sent thrice in consecutive manner. Critical Commands/Data should be accepted based on 2/3 logic. Timeout based communication mechanism provides deterministic behavior of the Checkout and Launch System.

VI. DESIGN OF SOFTWARE RELIABILITY ASSESSMENT MODEL

Assessment and determination of CDCLS software reliability is very important. Software reliability model described in fig. 3 is used for knowing confidence level of software reliability.

VII. TESTING AND VALIDATION

The system is tested elaborately at various levels- unit level, integrated level and system level considering various failure scenarios [35] [38] after performing defect analysis [36].

The test configuration is given in fig. 4. Various levels of tests that were conducted to ensure required reliability of the system are discussed in the following subsections.

A. Testing and Validation of Software Reliability in Standalone Mode

Well-planned comprehensive testing and evaluation of the Software is the main mechanism to achieve high reliability. Software faults are design defects, which, are harder to visualize, classify, detect, and correct. Therefore, in order to minimize software defects (syntactic and semantic), System level Test and Validation Setup simulating all modes of operation, failure modes, interlocks, time critical system behavior, graceful degradation in operating environment plays decisive role for achieving high system reliability. All test scenarios were simulated through the test configuration shown in fig. 4. Special attention needs to be paid to testing of mission/flight critical software modules, logical paths, operating modes.

B. Integrated System Validation Testing

Final validation testing of the integrated system in final operational configuration for ensuring functional compliance is essential. Over-all performance of the System in integrated mode is evaluated and systems level performance issues are addressed for achieving high system performance. Maximum possible failure modes and system interlocks (safety, operational, etc.) are simulated [37].

VIII. CONCLUSION

In view of mission criticality of the System, design of highly reliable CDCLS for Flight Vehicles/Missiles is, indeed, challenging. The system was successfully tested and proven for test scenarios'. The system could be effectively used for performing the checkout of various variants of device under test through configuration parameters, without modifying the system.

The design of the present CDCLS has achieved high level of maturity in terms of the important parameters like high reliability, modularity, usability, ease of reconfiguration, maintainability, expandability. Extremely successful performance has been achieved during Checkout and testing at Lab-level and Launch Missions at Field level.

REFERENCES

1. H. Hashempour, F. J. Meyer and F. Lombardi, "Test time reduction in a manufacturing environment by combining BIST and ATE," 17th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 2002. DFT 2002. Proceedings, Vancouver, BC, Canada, 2002, pp. 186-194.
2. W. Gosling, "Twenty years of ATE," Proceedings. 'Meeting the Tests of Time', International Test Conference, Washington, DC, USA, 1989, pp. 3-6.
3. L. Moskowit, "Virtual instruments: The future of ATE is here today," AU-TOTESTCON 93, San Antonio, TX, USA, 1993, pp. 203-206.
4. M.J. Gooding, "ATE technology trends." AUTOTESTCON 93, San Antonio; TX: USA, 1993, pp. 349-353.
5. J. Burden, P. A. Curry, D. Roby and F. Love, "Introduction to the next generation automatic test system (NGATS)," IEEE Autotestcon, 2005, Orlando, FL, 2005, pp. 16-19.
6. G.V. Yaswini Priya, Ch. Deepika Rajasree, Ch- Rupa, P. Lakshrai Madhavi aud PVRR Bhogendra Rao, "Distributed real-time Radar. Simulation Test bed for qualification of mission critical systems," 2016 International Conference on Computation System and

- Information Technology for Sustainable Solutions (CSITSS), Bangalore. 2016. pp. 184-187.
7. Thomas J. Black, "AUTOMATICTEST SYSTEM", US Patent Number. 4,774,462, Date of Patent Sep. 27, 1988.
8. Jonathan Fuller, Charles Crapuchettes, Stuart Nelson, "REMOTE TEST MODULE FOR AUTOMATIC TEST EQUIPMENT", US Patent No. US 6,275:962 B1, Date of Patent Aug. 14, 2001
9. M. Tripp, T. M. Mak and A. Meixner, "Elimination of traditional functional testing of interface timings at Intel," 2004 International Confereee on Test, Charlotte, NC, USA, 2004, pp. 1448-1454.
10. D. L. Jackson, "The emergence of Air Force Material Command and automatic test equipment (ATE) acquisition," Conference Record AUTOTESTCON '91 IEEE Systems Readiness Technology Conference Improving Systems Effectiveness in the Changing Environment of the '90s, Anaheim, CA, USA, 1991, pp. 363-367.
11. J. L. Anderson, "High performance missile testing (next generation test systems)," Proceedings AUTOTESTCON 2003. IEEE Systems Readiness Technology Conference., Anaheim, CA, USA, 2003, pp. 19-27.
12. 7. Toshihide Kadota, Poway, CA (US) Configurable Automatic-Test-Equipment System Patent No.US 7,343,558 B2 Date of Patent Mar. 11, 2008
13. R. Rajsuman, "An overview of the open architecture test system," Proceedings. DELTA 2004. Second IEEE International Workshop on Electronic Design, Test and Applications, Perth, WA, Australia, 2004, pp. 341-346.
14. K. Fowler, "Mission-critical and safety-critical development," in IEEE Instrumentation k. Measurement Magazine, vol. 7, no. 4, pp. 52-59, Dec. 2004.
15. JohnC- Knight, Safety critical systems: challenges and directions, ICSE '02: Proceedings of the 24th International Conference on Software Engineering May 2002 Pages 547550
16. D. C. Schmidt and H. van't Hag, "Addressing the challenges of mission-critical information management in next-generation net-centric pub/sub systems with OpenSplice DDS," 2008 IEEE International Symposium on Parallel and Distributed Processing, Miami, FL, 2008, pp. 1-8.
17. D. J. Musliner, J. A. Hendler, A. K. Agrawala, E. H. Durfee, J. K. Strosnider ' and C. J. Paul, "The challenges of real-time AI," in Computer, vol. 28, no. 1, pp. 58-66, Jan. 1995.
18. S. M. Schlosser, "The Third Generation of ATE," in IEEE Transactions on Instrumentation and Measurement, vol. 27, no. 2, pp. 122-126, June 1978.
19. gerfalk, Pr J. and Fitzgerald, Brian and Slaughter, Sandra A., "Introduction to the Special IssueFlexible and Distributed Information Systems Development: State of the Art and Research Challenges", Journal of Information Systems Research, vol. 20, no. 3 pp. 317-328, (2009)
20. J. J. Durgavich, M. N. Granieri and J. J. Woodfine, "Ate system architecture alternatives," International Automatic Testing Conference AUTOTESTCON '78., San Diego, CA, USA, 1978, pp. 199-209
21. H. A. Toku, "Developing new Automatic Test Equipments (ATE) using systematic design approaches," 2013 IEEE AUTOTESTCON, Schaumburg, IL. 2013, pp. 1-7.
22. Dan Breznitz, Darius Ornston, Steven Samford, "Mission critical: the ends, means, and design of innovation agencies", Industrial and Corporate Change, Volume 27. Issue 5, October 2018, Pages 883896
23. Shen Li, Shen Shituan, "Modeling design of general purpose ATE1', Journal of Beijing University of Aeronautics and Astronautics, School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing (2009-07)
24. ML1-HDBK-189C
25. Yongheng Yang, Huai Wang Ariya Sangwongwanich, Frede Blaabjerg, " Design for Reliability of Power Electronic Systems", Power Electronics Handbook Ed. 4, pp. 1423-1440 (2018)
26. H. Hashempour, F. J. Meyer and F. Lombardi, "Analysis and measurement of fault coverage in a combined ATE and BIST environment," in IEEE Transactions on Instrumentation and Measurement, vol. 53, no. 2, pp. 300-307, April 2004.
27. R. Hooper, "Next generation ATE software," 2013 IEEE AUTOTESTCON, Schaumburg7 IL, 2013, pp.1-6.

28. Madhavi Ponnappalli and P. V. R. R. Bhogendra Rao, "A Comparative Study of Software Architectures for Embedded Mission Critical Applications," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 741-746.
29. L. Wang, "Get real: Real Time Software Design for Safety-and Mission-Critical Systems with High Dependability," in IEEE Industrial Electronics Magazine, vol. 2, no. 1, pp. 31-40, March 2008.
30. Abhijit M Kulkarni, Vidyavati S Nayak and PVRR Bhogendra Rao, "Comparative study of middleware for C4I systems Web Services vis-vis Data Distribution Service," 2012 International Conference on Recent Advances in Computing and Software Systems, Chennai. 2012, pp. 305-310.
31. Gill Christopher, Kuhns Fred, Levine David, Schmidt Douglas, "Applying Adaptive Real-time Middleware to Address Grand Challenges of COTS-based Mission-Critical Real-Time Systems", Atlas, Aha. (2000).
32. V. Pasek and D. Lytle, "Mission-critical software development for a distributed and diverse user base," 2011 Aerospace .Conference, Big Sky, MT, 2011, pp. 1-12
33. K. Abhijit, B. Gautham Reddy, A. Aswini Kumar and P. V. R. R. Bhogendra Rao; "Automated decision support for response time analysis of real time task set an approach paper," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-4.
34. P. Pointl, "Interfacing, often a performance bottleneck between ATE and device under test," Proceedings of the 1st European Test Conference, Paris, France, 1989, pp. 94-99
35. Domenico Cotroneo, Antonio Pecchia, Roberto Pietrantuon, Stefano Russo, "A failure analysis of data distribution middleware in a mission-critical system for air traffic control", Proceedings of the 4th International Workshop on Middleware for Service Oriented Computing (MWSOC '09), November 2009 pp. 2530
36. Gabriella Carrozza, Roberto Pietrantuono, Stefano Russo, "Defect analysis in mis-sioncritical software System's detailed investigation", Journal of sw: Evolution and process. Vol. 27, Issue 1, January 2015, pp. 22-49.
37. J.L. Anderson, Z. E. Figuerres and A. Hovakemian, "Using ATE simulation to develop test procedures and verify testability for the STANDARD missile," 1998
38. IEEE AUTOTESTCON Proceedings. IEEE Systems Readiness Technology Conference. Test Technology for the 21st Century (Cat. No.98CH36179), Salt Lake City, UT, USA, 1998, pp. 28-34. 38. Michael J. LuValle, Bruce G. Lefevre, SriRaman Kannan, Design and Analysis of Accelerated Tests for Mission Critical Reliability, CHAPMAN & HALL/CRC, A CRC Press Company, 2004

AUTHORS PROFILE



Shivpal Singh, received his M.Tech in Computer Science from IIT, Madras. He has been working in DRDL as scientist for 30 years. His areas of defence research include design and development of mission critical checkout and launch control systems for aerospace flight vehicles, configurable distributed systems, reliability engineering, system simulators and automated test equipment. He has more than 20 publications in national/international conferences Mission critical systems received by him have been successfully inducted into service by armed forces. He has received DRDO path-breaking research award.



Dr PVRR Bhogendra Rao, received his M.Tech in Computer Science and Engineering and Ph.D in Computer Science from JNTU, Hyderabad. He has been working in DRDL as scientist for 27 years. He has been working in development of real-time c4I systems for various defence applications. His areas of interest include pattern oriented design, real-time systems, parallel and distributed systems, fault tolerant system design. He has more than 30 publications in national/international journals and conferences. He has received DRDO performance excellence award for his contribution towards development of various systems deployed by armed forces.