Journal of The Korea Society of Computer and Information
Vol. 20 No. 10, pp. 1-5, October 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.10.001

The Design of a Fault Tolerant Store Management System

Dongho Lee *, Hansol Park **

Abstract

Based on the dual hardware and software with distributed recovery blocks, the centralized type fault tolerant store management system(SMS) was proposed. As a result of trade off study related to mutiplex hardware system design, dual single board computer(SBC) was adapted. To verify redundancy function of the proposed structure, the prototype SMS and weapon simulator were used. The proposed SMS operated normally without being affected by a primary SBC failure. The switching time from primary SBC to shadow SBC was within 200 ms. The reliability of the proposed SMS was predicted and compared with the non fault tolerant SMS, thereby it was proved that the proposed SMS has a higher reliability than the non fault tolerant system within effective range.

▸ Keyword : Fault tolerant, Centralized, Store Management System, Distributed Recovery Block, Reliability

I. Introduction

최근 개발되는 전투기는 다수의 무장이 장착되며 표적의 특성에 따라 운용 방법을 변화시킨다. 따라서 효율적으로 무장을 발사하고 통제하기 위해 무장관리시스템(SMS: Store Management System)을 필수적으로 적용하고 있다[1]. SMS는 무장의 동작에 직접적으로 작용하므로 조종사나 기체의 안전을 위해 결함허용 구조가 적용되고 있다.

항공기에 적용되는 결함허용 구조는 비행제어컴퓨터에서 다양하게 연구되어 왔지만 무장의 운용을 제어하는 SMS와 기체를 제어하는 비행제어컴퓨터(FLCC: Flight Control Computer)는 시스템 운용 개념이 다르므로 SMS의 특성에 적합한 결함허용 구조에 대한 연구가 필요하다. 하지만 항공기 SMS의 구조는 무장의 특성과 밀접하게 연관되어 있어 전투기 개발 선진국들은 SMS 관련 연구는 공개 하지 않고 있다. 국내 전투기도 원할한 무장 운용을 위해 SMS를 적용하고 있지만 결함허용 구조를 적용한 사례는 없다. 하지만 결함은 예기치 않게 발생하므로 국내 전투기도 SMS 결함허용 구조를 적용할 필요가 있다.

따라서 본 논문에서는 SMS의 기본적인 시스템 설계를 살펴보고 중앙집중형 SMS의 결함허용 구조에 대한 연구를 수행하였다. 본론에서는 먼저 결함허용 설계와 관련된 연구 동향을 살펴보았다. 이를 바탕으로 하드웨어 설계와 소프트웨어 구조를 제안하였으며 실험을 통해 제안된 구조의 구현 가능성을 검증하였다. 마지막으로 결함허용 구조를 반영할 경우 시스템 신뢰도에 어떠한 영향을 미치는지를 결함허용 기능이 없는 시스템과 비교하였다.

II. Related Works

결함허용 설계란 예기치 않은 시스템의 오류가 발생하더라도 시스템 본래의 기능이 동작되도록 설계하는 것을 의미한다. 결함허용 설계는 하드웨어 설계와 소프트웨어 설계로 구분할 수 있으며 하드웨어 분야는 다중화 설계를 통해 신뢰성을 증가시키는 연구가 보고되었다[2]. 소프트웨어 분야에서는 자체 진단 설계[3], 복구 블록 설계[4], 분산 복구 블록 설계[5], 네크워크 감시 기법[6] 등이 연구되고 있다. 자체 진단이란 시스템 스스로가 기능의 이상 유무를 판단하는 것을 의미하며 항공기

• First Author: Dongho Lee, Corresponding Author: Dongho Lee
*Dongho Lee(dh922.lee@hanwha.com), Avionics Group, Hanwha Thales
**Hansol Park (hansol80.park@hanwha.com), Software Group, Hanwha Thales
• Received: 2015. 08. 07, Accepted: 2015. 09. 05. Accepted: 2015. 09. 08.

는 대부분의 하드웨어에 자체 진단 기능을 적용하고 있다. 복구 블록 설계는 연산 결과의 오류를 판단하여 연산의 실행 및 재실행을 판단하는 역방향 복구를 지원하는 알고리즘이다. 분산 복구 블록 설계는 주 노드와 부 노드로 나누어 병렬 연산을 실시하며 주 노드가 오류일 경우 부 노드가 다음 프로세스를 수행하는 전향적 복구를 지원한다. 따라서 실시간 고속 데이터 처리에 적합한 알고리즘이다. 네트워크 감시 기법은 주 노드 관리에 대한 다양한 방안을 제시한다.

항공기 FLCC의 경우 유인기와 무인기에 적용되는 시스템 모두 결함허용 설계가 적용되고 있다[7-9]. 유인 전투기 비행 제어 시스템의 경우 시스템의 신뢰도 향상을 위해 동일한 하드웨어와 소프트웨어를 가지는 시스템을 3중 또는 4중으로 구현하여 신뢰성을 증가시켰다. 일반적으로 FLCC의 하드웨어 분야는 다중화가 적용되었으며 소프트웨어는 자체 진단 설계, 복구 블록 설계 및 네트워크 감시기법이 적용된다.

SMS는 무장 연동 정보와 관련되어 있어 하드웨어 및 소프트웨어 설계에 대한 결함 설계 연구가 알려진 바 없다. 하지만 무장 운용 환경을 고려하면 결함 설계 기법 중 하드웨어 다중화와 고속 실시간 처리에 적합한 분산 복구 블록 기법이 적합하다고 판단된다. 따라서 본 논문에서는 다양한 결함 설계 기법 중 하드웨어 다중화와 분산 복구 블록 소프트웨어로 구성된 SMS 시스템를 논하겠다.

III. The Proposed SMS

3.1 SMS Architecture

SMS는 시스템 구조에 따라 중앙집중형 구조와 분산형 구조로 구분된다. 중앙집중형 구조는 Fig. 1과 같이 무장의 제어를 SMS가 직접 제어하는 구조이다. 분산형 구조는 Fig. 2와 같이 SMS Controller가 무장과 직접 연동하는 무장 스테이션 연동 장치(SSIU : Store Station Interface Unit)를 제어하는 구조로 구성된다[10]. 결함허용 관점에서 중앙집중형 구조는 소프트웨어의 중복 설계를 줄일 수 있고 분산형 구조는 Single Point of Failure(SPOF)의 위험성을 피할 수 있는 것이 대표적인 특징이다. 본 논문에서는 설계에 대한 검증을 수행하기 위해 시스템 구축이 간편한 중앙집중형 SMS를 선택하여 결함허용 설계를 논하겠다.

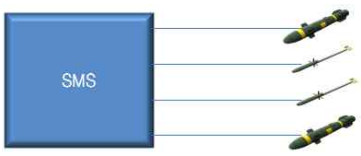


Fig. 1. Architecture of Centralize SMS

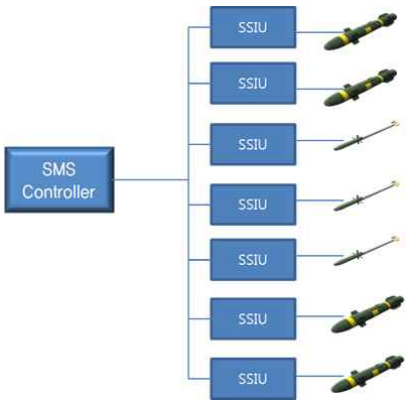


Fig. 2. Architecture of the Distributed SMS

3.2 Design of Fault Tolerant SMS

본 절에서는 하드웨어 다중 설계와 분산 복구 블록 소프트웨어를 적용하여 결함허용 특성을 가지는 중앙집중형 SMS를 제안한다.

하드웨어 다중화는 시스템의 신뢰도를 향상시키지만 반대로 중량 증가와 시스템 설계의 복잡성을 초래하므로 시스템 설계자의 판단에 따라 구조가 결정된다. 일반적으로 다중화를 고려하지 않은 중앙집중형 SMS는 Fig. 3과 같은 구조를 가진다.

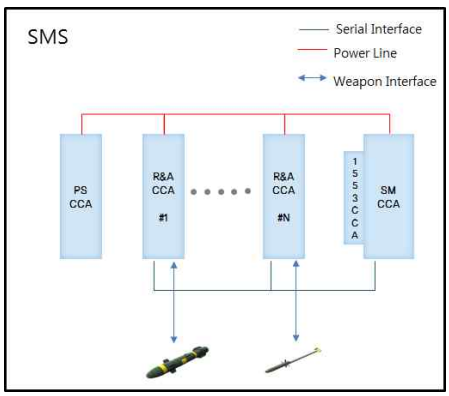


Fig. 3. Internal Structure of Centralized SMS

3.2.1 Hardware Design

SMS는 무장 제어를 담당하는 무장관리 회로카드조립체(SM CCA, Store Management Circuit Card Assembly), 전원 공급 회로카드조립체(PS CCA, Power Supply CCA)와 무장과 직접 연동하는 무장 투하 및 장전 회로카드조립체(R&A CCA, Release and Arming CCA)로 구성된다. 시스템 측면에서 SMS를 이중화하는 방법은 SMS 시스템 이중화와 SMS 내부 모듈 이중화로 구분할 수 있다. SMS 시스템을 이중화 시킬 경우 시스템의 신뢰도는 증가하지만 장비의 무게, 전력소모가 두 배로 증가하고 무장과 이중화된 SMS 시스템 사이에 능동형 연동 스위치가 들어가야 한다. 무게와 전력 소모가 증가할 경우 기체 설계에 부담을 주게되며 능동형 연동 스위치가 들어갈 경우 SMS 시스템의 고장 발생 확률이 높아지므로 시스템의 신뢰

도 측면에서 적합하지 않다. 따라서 본 논문에서는 SMS 내부의 모듈 이중화가 시스템 이중화보다 더 효율적이라 판단된다. 하지만 내부 모듈 중 R&A CCA를 이중화할 경우 이중화된 R&A CCA와 무장간 능동형 연동 스위치가 필요하며 PS CCA의 경우 비상 상황에서 동작할 수 있는 Capacitor가 있으므로 중량, 시스템 복잡도, 신뢰도를 고려하였을 때 SM CCA만 이중화하는 것이 SMS 결함허용 설계에 가장 적합하다고 판단된다. 이러한 검토 내용을 바탕으로 중앙집중형 SMS의 내부 구조를 Fig. 4와 같이 제안한다. PS CCA는 50 ms 동안 항공기 전원이 차단되어도 전원을 공급할 수 있도록 콘덴서와 결합되어 있다. SM CCA는 동일한 기능을 가지는 두 개의 모듈이 존재하며 분산 복구 블록 소프트웨어를 지원한다. 두 개의 SM CCA는 R&A CCA와 독립적으로 통신할 수 있도록 별도의 통신 네트워크를 구성하며 SM CCA 상호간에는 네트워크로 연결되어 주 노드의 비정상 동작을 감시할 수 있다.

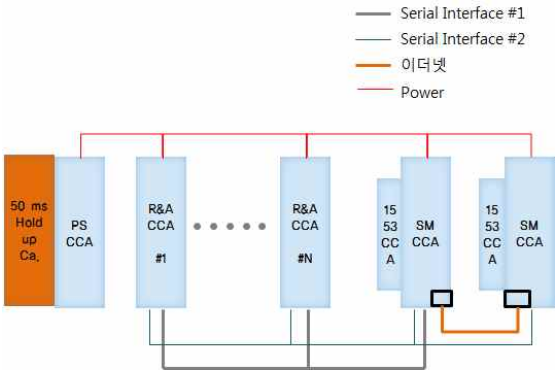


Fig. 4. Internal Structure of Centralized Fault Tolerant SMS

3.2.2 Software Design

제안된 SMS의 결함허용 동작을 지원하기 위해 소프트웨어는 Fig. 5와 같이 분산 블록 구조를 적용하여 설계하였다. SM CCA에 탑재되는 소프트웨어 모듈은 Ethernet과 무장 제어를 위한 I/O 처리 모듈, 내부 복구블록들을 제어하는 관리자 노드 모듈과 실제 무장제어를 수행하는 기능 모듈들로 구성된다. 복구 블록들은 내부에 실시간 동작을 위한 Time-triggered 스레드, 해당 스레드에 의해 동일 결과를 생성하는 무장제어 함수들과 결과를 검증하는 Acceptance Test 모듈로 구성된다.

각 단계별 로직은 Fig. 5와 같이 같은 기능을 수행하지만 서로 다른 형태로 작성된 Function A와 Function B로 구성되며, Function A와 B가 모두 실패하는 경우, 상대 노드로 절체 되게 된다. 동일한 하드웨어에 1개의 Pair로 구성된 Primary/Shadow Pair는 논리적으로는 3개의 분산 복구블록 Pair로 분리되는데 이는 무장관리를 위한 3단계의 로직이 각각 독립적인 분산 복구블록 Pair로 동작하기 때문이다.

무장을 제어하는 로직은 무장의 Primary 전원을 관리하는 모듈, 무장의 모드를 제어하는 모듈과 무장의 발사를 제어하는 모듈로 구성하였다. 정상 상태에서는 Primary노드의 복구블록들에 의해 무장제어 로직이 수행된다. 개별 복구블록에 의해 정상적으로 처리된 결과는 다음 복구블록의 입력 데이터로 입력되어 순차적으로 처리된다. 처리 중간에 Primary 노드에서 소프트웨어 오류가 발생하거나 하드웨어 결함이 발생하는 경우에는 Shadow 노드의 복구블록에서 Primary 복구블록의 결과를 받지 못해 결함상태를 선언하고, 해당 상태를 관리노드에게 전달한다. 관리노드에서는 상대 관리노드로부터의 입력과, 노드 내의 복구블록의 정보를 종합하여 최종적으로는 Primary 복구블록에서 Shadow 복구블록으로 처리가 전환된다. 최종 복구블록까지 정상적으로 처리가 완료되면 무장 제어에 필요한 신호가 무장 제어 I/O 모듈을 통해 생성된다.

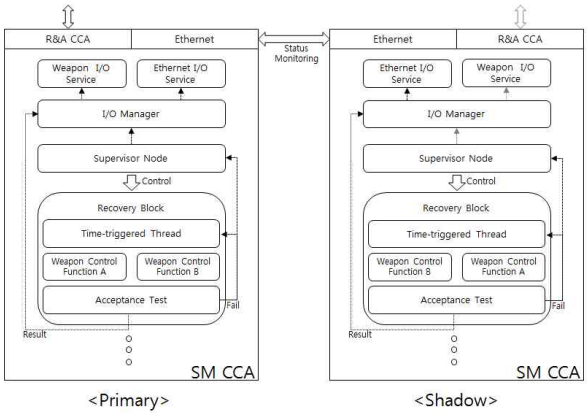


Fig. 5. Distributed Recovery Block Software Architecture

3.3 Verification of Fault tolerance and Prediction of Reliability

SM CCA의 이중화와 분산형 복구 블록 소프트웨어를 적용한 중앙집중형 SMS의 결함허용 동작을 검증하기 위해 Fig. 6과 같이 시험 환경을 구성하였다. 중앙집중형 SMS는 두 개의 MPC 8640 SM CCA, 두 개의 R&A CCA와 전원 공급 모듈로 구성하였다. SBC는 RS422을 통해 R&A CCA를 제어하며 각각의 SBC는 독립된 RS422 인터페이를 이용하여 R&A CCA를 제어한다. SMS와 연동하는 무장 모의기는 MIL-STD-1553카드가 장착된 상용컴퓨터를 사용하였다. 본 시험에서 SMS와 무장모의기간 연동 신호는 1553 신호로만 제한하였으며 이산 신호 동작은 고려하지 않았다. SMS는 A와 B 무장을 제어하는 것으로 정의했으며 각 무장의 ICD는 무장 동작 시퀀스에 적합하게 임의로 정의하였다. 분산형 복구 블록을 가지는 SMS 소프트웨어는 C++을 이용하여 구현하였으며 RTOS는 VxWorks를 적용하였다. 시험 시나리오는 SMS 내부의 Primary SM CCA가 정상 동작 중 고장나는 경우로 설정하였다. 고장 모의를 위해 고장의 경우를 복구블록 내에서의 소프트웨어 결함이 발생하는 경우와 하드웨어 결함이 발생하는 경우로 분리하였으며, 복구블록 내에서의 결함은 외부 고장주입 소프트웨어를 이용하여 고장을 주입하였고, 하드웨어 결함은 전원을 제어하여 고장 상태를 발생시켰다[11].

무장 제어를 위한 로직을 3개의 모듈로 구현하였으며

Primary SM CCA와 Shadow SM CCA는 이더넷으로 25Hz의 주기로 상호 모니터링 하는 것으로 구현하였고 정상 동작과 결함 상황을 확인하기 위하여 제어 신호의 출력을 모니터링 하였다. 실험 결과 SMS는 Primary SM CCA 에 고장이 발생한 것을 확인한 후 Shadow SM CCA가 동작하였으며 전환 시 소요되는 시간은 소프트웨어 결함이 발생하는 경우와 하드웨어 결함이 발생하는 경우 모두 200ms 이내임을 확인하였다. 단, Primary SM CCA와 Shadow SM CCA의 상호 모니터링 주기에 의존적이며, 교환 주기가 빨라지는 경우, 절체 시간은 변경될 수 있다.

Fig. 6. Experimental Setup for Verifying Fault Tolerance of the Proposed SMS

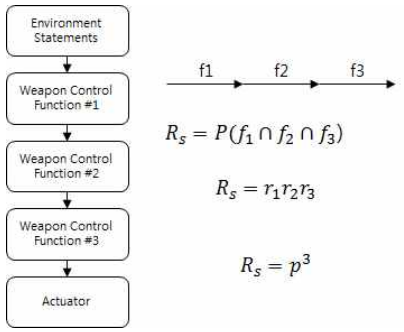
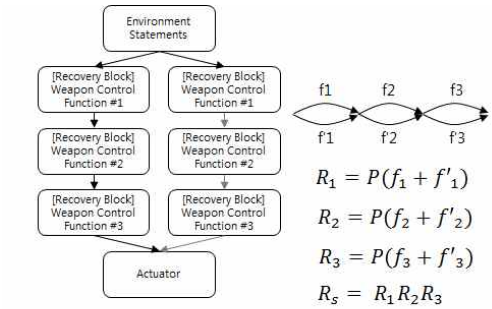


Fig. 7. Reliability of Non Fault Tolerant SMS



$$R_s = (r_1 + r'_1 - r_1 r'_1)(r_2 + r'_2 - r_2 r'_2)(r_3 + r'_3 - r_3 r'_3)$$
$$R_s = (2p - p^2)^3$$

Fig. 8. Reliability of Fault Tolerant SMS

신뢰도를 계산하기 위해 결함허용 기능이 없는 SMS 로직은 Weapon Control Function #1, #2, #3 이며 수식 상 표현은 Fig.6과 같이 f1, f2, f3로 표현한다[12]. 결함허용특성을 갖는 SMS의 경우 Fig.7과 같이 f'1, f'2, f'3으로 제어 로직을 표현한다. 본 논문에서 제안한 분산 복구블록을 이용한 경우, 3단계의 로직 중 하나가 결함이 발생하더라도 해당 분산 복구블록 Pair 단위의 절체가 일어나기 때문에 전체적인 운용에 문제가 발생하지 않으므로 3개의 Pair를 기준으로 신뢰도를 계산하였다.

각 로직들의 신뢰도를 r_x로 표현하고 시스템 전체의 신뢰도는 Rx로 표현한다. 신뢰도 계산 결과는 결함허용 기능이 없는 시스템의 경우 개별 로직들의 신뢰도가 p인 경우 Fig. 7과 같이 p^3이며, 결함허용 시스템은 분산 복구블록을 적용하여 Fig. 8의 $(2p-p^2)^3$이 된다. 신뢰도 p가 유효범위($0.1 \le p \le 0.9$) 내에 있을 때 시스템의 종합적인 신뢰도를 나타내면 Fig.9와 같다. 연두색 그래프가 결함허용 시스템의 신뢰도를 나타내며 적색이 결함허용 기능이 없는 시스템을 나타낸다. 결과를 분석해보면 결함허용 시스템을 적용하였을 경우 유효구간 내에서 신뢰도가 향상됨을 확인할 수 있다. 따라서 시험 결과와 신뢰도 분석을 통해 본 논문에서 제안한 결함허용 특성을 가지는 SMS가 조종사와 기체의 안전도를 향상 시킬 수 있다고 판단된다.

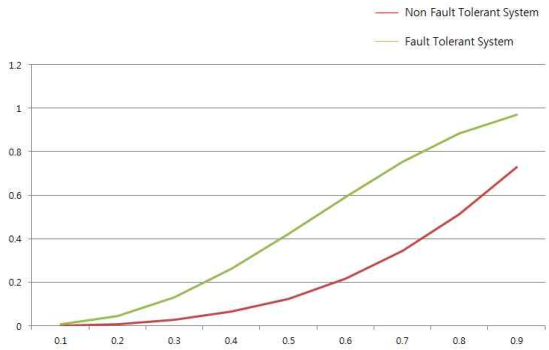


Fig.9 Comparison of Reliability between two SMS

IV. Conclusion

신뢰도가 증가된 결함허용 특성을 가지는 중앙집중형 SMS의 구조를 제안하였다. 제안된 시스템의 하드웨어는 신뢰도 향상, 중량 감소, 시스템 복잡도 감소를 동시에 고려하여 무장관리 회로카드조립체(SM CCA)의 이중화를 선택하였다. SMS의 소프트웨어는 고속 실시간 처리를 지원하는 분산 복구 블록 기법을 적용하였다. 제안된 SMS의 결함허용 특성은 SMS와 무장 모의기를 이용하여 검증하였다. 시험 결과 Primary SM CCA에 고장이 발생한 경우 200 msec 이내에 Shadow SM CCA로 권한이 이양되는 것을 확인하였다. 이를 통해 제안된 중앙집중형 SMS의 결함허용 특성이 실제 무장에 적용될 수 있음을 확인하였다. 이와 더불어 신뢰도 분석을 통해 중앙집중형 구조에서 결함허용특성을 가지는 SMS가 결함허용 기능이 없는 시스템보다 유효구간 내에서 높다는 사실을 알 수 있었다.

따라서 본 연구 결과는 실제 전투기 SMS의 결함허용 설계

에 도움을 주리라 판단된다. 향후에는 실제 무장 연동 정보를 적용한 분산형 결함허용 SMS의 연구를 진행하여 전투기 무장 관리 시스템의 설계에 필요한 기초 데이터를 구축하고자 한다.

REFERENCE

[1] I. Moir and A. Seabridge, "Military avionics systems," John Wiley & Sons, Ltd., pp. 335-370, 2006.

[2] G.S. Virk and J.M. Tahirt, "A fault tolerant optimal flight control system," International Conference on Control, Vol. 2, pp. 1049 -1055, 1991.

[3] S. Blanc and P.J. Gil, "Improving the multiple errors detection coverage in distributed embedded systems ," Proc. 22nd International Symposium on Reliable Distributed Systems, pp. 303 - 312, 2003.

[4] J.J. Horning, H.C. Lauer, P.M. Melliar-Smith and B. Randell, "Reliable computer systems," Springer Berlin Heidelberg, pp. 53 - 68, 1985.

[5] D. Nguyen and Dar-Biau Liu, "Recovery blocks in real-time distributed systems," Proc. Reliability and Maintainability Symposium, pp. 149-154, 1988.

[6] K.H. Kim, L. Bacellar and C. Subbaraman, "Primary-shadow consistency issues in the DRB scheme and the recovery time bound," Proc. 7th International Symposium on Software Reliability Engineering, pp. 319-329, 1996.

[7] B.J. Park, Y.S. Kang, S.S. Yoo and A. Cho, "Development of operational flight program for smart UAV," J. of the Korea Society for Aeronautical and Space Sciences, Vol. 41, No. 10, pp. 805-811, 2013.

[8] Y.H. Nam, J.Y. Ju and S.H. Jang, "Development of Dual-Redundant Flight Control Computer for Tilt Rotor UAV," Spring Conference of the Korean Society for Aeronautical & Space Sciences, pp. 1196-1199, 2013.

[9] S.H. Park, J.Y. Kim, I.J. Cho and B.M. Hwang, "Redundancy Management Design for Triplex Flight Control System," The Korean Society for Aeronautical & Space Sciences, Vol. 38, No. 2, pp. 169-179, 2010.

[10] D.H. Lee and H.J. Park, "Designing a Common Weapon Interface Module while Taking into Account the Fire Control System Architecture of a Light Armed Helicopter," J. of Korean Institute of Communication and Information Sciences," Vol. 39C, No. 11, 2014.

[11] S.W. Chun, W.H. Baek and J.P. La, "A Study on HILS for Performance Analysis of Airborne EOTS for Aircraft," J. of the Korea Society of Computer and Information," Vol. 18, No. 12, pp. 55-64, 2013.

[12] D.G Kwak, C.W Yoo and J.Y. Choi, "A Design and Implementation of Reliability Analyzer for Embedded Software using Markov Chain Model and Unit Testing," J. of the Korea Society of Computer and Information," Vol. 16, No. 12, pp. 1-10, 2011

Authors

Dongho Lee received the B.S., M.S. and Ph.D. degrees in Electronic Engineering from Kyungpook National University, Korea, in 1997, 1999 and 2006, respectively.

Dr. Lee worked for the Agency of Defense Development from 2006 to 2010. He joined the Hanwha Thales in 2010. He is currently a Cheif Engineer in the Avionics group of Hanwha Thales. He is interested in Embedded Software and Avioncs.

Han Sol Park received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Konkuk University, Korea, in 2004, 2006 and 2013, respectively.

Dr. Park worked for the Agency of Defense Development from 2008 to 2012. He is currently a senior engineer in the Department of Software Group, Hanwha Thales. He is interested in distributed real-time computing, fault-tolerance system, and avionics software.