



Received: 2026/07/23
Revised: 2026/08/02
Accepted: 2026/08/28
Published: 2026/09/30

***Corresponding Author:**

Jae Sung Yu

333 Pangyo-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 13488, Republic of Korea
Tel: +82-31-5179-7284
E-mail: jaesung.yu@ligdna.com

Abstract

본 논문에서는 알고리즘 보안 제약으로 인해 M&S 도구의 사전 '설계 검증'이 제한되고 사후 비행시험 데이터로 이를 대체하는 유도무기 체계의 역순차적 V&V의 한계점을 분석한다. 이러한 방식은 시나리오 커버리지 부족과 오류 추적성 저하를 초래하여 M&S 신뢰성 확보를 저해한다. 이를 극복하기 위해, 본 논문에서는 기밀 컴퓨팅(TEE)과 국방 M&S 표준(FMI, HLA/RTI)을 결합한 보안 연합 M&S 설계 검증 프레임워크를 제안한다. 제안하는 프레임워크는 원천 기술의 IP를 런타임에서 보호하는 동시에, 실사격 이전 가상 환경에서 대규모 시뮬레이션을 통한 정상적인 하향식 설계 검증을 가능하게 한다.

In this study, we analyzed the limitations of reverse-sequential verification and validation in guided missile systems, where pre-design verification of modeling and simulation (M&S) tools is restricted by algorithm security constraints and substituted with post-flight test data. This approach limits M&S reliability by reducing scenario coverage and degrading error traceability. To address this issue, this study proposes a secure federated M&S design verification framework combining confidential computing with defense M&S standards such as FMI and HLA/RTI. This framework strictly protects the intellectual property of the original technology at runtime while enabling top-down design verification through large-scale simulations in a virtual environment prior to live-fire testing.

Keywords

국방 M&S VV&A(Defense M&S VV&A),
설계 검증(Design Verification),
기밀 컴퓨팅(Confidential Computing),
신뢰 실행 환경(Trusted Execution Environment),
역순차적 V&V(Reverse-Sequential V&V)

유도무기 체계의 역순차적 V&V 한계 분석 및 기밀 컴퓨팅(Confidential Computing) 기반 보안 M&S 설계 검증 프레임워크 연구

Limitations of Reverse-Sequential V&V in Guided Missile Systems and a Secure M&S Design Verification Framework Based on Confidential Computing

유재성^{1*}, 김정², 이성균², 고진용², 장재덕²

¹LIG 디펜스&에어로스페이스 M&S팀 선임연구원

²LIG 디펜스&에어로스페이스 M&S팀 수석연구원

Jae Sung Yu^{1*}, Jeong Kim², Sungkyun Lee², Jinyong Go², Jaedeok Jang²

¹Research engineer, M&S Team, LIG Defense&Aerospace

²Chief research engineer, M&S Team, LIG Defense&Aerospace

1. 서론

1.1 무기체계 연구개발에서의 M&S 도구 활용과 VV&A의 필요성

현대 유도무기 체계의 연구개발에 있어 실제 전장 환경에서의 시험(live test)은 무기체계의 최종 성능을 확인하기 위해 필수적이나, 현실적인 제약이 따른다. 고도의 정밀 타격이 요구되는 유도탄의 경우, 높은 발사 비용, 시험장 공역 확보의 어려움, 기상 악화, 안전 통제 문제 등으로 인해 개발 주기 내에서 수행할 수 있는 물리적 비행시험 횟수가 제한된다[1,2].

이러한 물리적, 경제적 한계를 보완하기 위해, 국방 획득 프로세스에서는 M&S(modeling & simulation) 기반의 가상 모델을 활용하여 실시험을 대체하거나 실사격 이전 단계에서 성능을 검증하는 방식을 채택하고 있다[1]. 그러나 컴퓨터 소프트웨어상에 구현된 M&S 도구의 산출물로 실제 물리적 시험을 대체하기 위해서

데이터를 활용하여 ‘데이터 검증 및 확인’을 선행하는 방식을 대안으로 채택하고 있다.

즉, 유도탄 발사를 통해 획득한 비행 궤적과 오차 데이터를 분석한 뒤, 이 결과가 목표 성능을 만족할 경우 내부에 탑재된 블랙박스 알고리즘의 초기 설계(논리 및 기능 구성) 또한 유효한 것으로 간주하여 ‘인정 결정’을 내리는 방식이다. 본 논문은 이러한 방식이 시스템의 신뢰성을 사전에 입증하여 실시험을 최소화하려던 M&S 도입의 본래 취지와 상충되는 한계가 있음을 지적한다. 가상의 시뮬레이션 공간에서 논리적 타당성이 사전 검증되어야 할 설계를 사후의 물리적 비행시험 데이터에 의존하여 증명하려는 것은 공학적 불확실성을 높일 수 있다[3].

따라서 본 논문은 역순차적 검증 방식이 지니는 시스템 엔지니어링 관점의 한계를 분석하고, 보안성을 유지하면서도 초기 단계에서 M&S 도구의 논리적 설계 타당성을 입증할 수 있는 보안 M&S 프레임워크 대안을 제시하고자 한다.

2. 유도무기 체계 V&V의 한계: 비행시험 의존적 검증의 불확실성 분석

2.1 설계 검증 부재가 미치는 영향

설계 검증 단계는 M&S 모델에 적용된 알고리즘 논리의 적절성과 개념모델 대비 기능 구성의 타당성을 평가하는 과정이다[2,3]. 그러나 입출력 규격만 정의된 블랙박스 모듈을 활용할 경우, 모델에 주입되는 입력 파라미터 변화에 따른 최종 출력값의 경향성만을 제한적으로 확인할 수밖에 없다.

이는 복잡한 상황에서 알고리즘이 궤적을 수정하는 수학적 논리, 엣지 케이스(edge case)에서의 한계점, 하위 기능들 간의 상호작용이 적절히 구성되었는지를 사전에 검토하는 과정을 제한하게 된다. 논리적 적절성에 대한 사전 평가가 부족한 상태에서 수행되는 데이터 검증 및 ‘인정 평가’는 검증의 완전성을 저하시킬 수 있으며, M&S 도구의 신뢰도 하락 요인이 된다[1,3].

2.2 역순차적 검증의 시스템 엔지니어링 관점 제약사항

표준 절차인 ‘설계 검증’을 생략하고 사후적인

‘데이터 검증 및 확인’ 결과를 통해 설계 논리를 정당화하는 프로세스는 다음과 같은 공학적 제약을 지닌다[4].

1. 검증 시나리오 커버리지의 한계: 실제 유도무기 교전 환경은 기상 조건, 표적의 회피 기동 패턴, 복합 전자전(EW) 재밍 등 다차원적 변수 공간을 형성한다. 반면, 물리적 비행시험은 비용 및 공역 통제의 한계로 통상 10회 미만으로 수행된다. 통제된 소수의 조건에서 도출된 성공적인 데이터만을 근거로 다양한 시나리오에 대응해야 하는 알고리즘 설계 전체의 타당성을 일반화하는 것은 통계적 신뢰도가 부족할 수 있다[2,3].

2. 오류 추적성(traceability) 저하: 비행시험 중 유도탄이 목표를 이탈하는 실패가 발생했을 때, 추적성 부족은 개발 과정에 지장을 초래할 수 있다[4]. 블랙박스로 처리된 설계 논리로 인해, 실패 원인이 탐색기 모델의 논리 결함인지, 관성항법 모델의 오차 누적인지 등 근본 원인 규명(root-cause analysis)이 구조적으로 제한된다. 이는 문제 해결 과정이 논리적 추론보다는 반복적 시행착오(trial and error)에 의존하게 만들 수 있다.

3. 후기 결함 발견에 따른 총수명주기비용(LCC) 증가: 시스템 엔지니어링 원칙상 결함이 수명주기 후반에 발견될수록 수정 비용은 크게 증가한다[4]. M&S 초기 ‘설계 검증’에서 알고리즘 논리의 부적절성이 식별되면 모델링 수정으로 낮은 비용에 해결이 가능하다. 그러나 역순차적 V&V 환경에서 비행시험 단계에 이르러 결함이 발견될 경우, 하드웨어 분석, 논리 재설계, 추가 실사격 등이 수반되어 개발 예산 증가와 일정 지연을 초래할 수 있다.

3. 기밀 컴퓨팅 기반 보안 M&S 체계의 이론적 배경

알고리즘 공급자의 지적재산권(IP) 보호와 체계 통합 관점의 논리적 타당성 검증이라는 상충되는 요구사항을 조율하기 위해, 본 연구는 최신 하드웨어 암호화 기술과 국방 M&S 표준 아키텍처의 융합을 이론적 대안으로 제시한다. 본 장에서는 제안하는 프레임워크를 구성하는 핵심 요소 기술들의 작동 원리와 공학적 특성을 분석한다.

3.1 하드웨어 기반 기밀 컴퓨팅과 신뢰 실행 환경(TEE)의 암호학적 구조

전통적인 정보 보안 기술은 데이터가 스토리지에 저장될 때(data at rest)나 통신망을 통해 전송될 때(data in transit)의 보호에 초점이 맞춰져 있었다[6]. 그러나 M&S 환경에서 블랙박스 알고리즘을 연산하기 위해서는 메모리에 데이터가 평문으로 적재되어야 하므로, 이 과정(data in use)에서 메모리 덤프나 디버깅을 통한 IP 유출 취약점이 발생한다.

기밀 컴퓨팅(confidential computing)은 이러한 취약점을 극복하기 위해 하드웨어 기반의 신뢰 실행 환경(TEE: Trusted execution environment, 예: Intel SGX, ARM TrustZone)을 활용한다[6-8]. TEE의 핵심 이론적 근거는 다음과 같다.

1. 메모리 격리 및 하드웨어 암호화(memory isolation & encryption): TEE는 CPU 내부에 물리적으로 격리된 ‘인클레이브(enclave)’라는 특수 메모리 영역을 생성한다[7]. CPU에 내장된 메모리 암호화 엔진(MEE)은 인클레이브 데이터를 캐시에서 메인 메모리(RAM)로 기록할 때 실시간으로 하드웨어 암호화를 수행한다. 따라서 운영체제(OS), 하이퍼바이저, 최고 관리자(root) 권한을 가진 공격자라도 메모리를 물리적으로 탈취하여 내부 논리를 해석하는 것이 불가능하다[6,9].

2. 원격 증명(remote attestation): TEE 아키텍처는 체계 종합 업체(또는 알고리즘 공급자)가 인클레이브 내부에 적재된 M&S 모델이 위변조되지 않은 정품임을 암호학적으로 확인할 수 있는 ‘원격 증명’ 기능을 제공한다[7,8]. 이는 블랙박스 모델의 무결성을 시스템 수준에서 보증하므로, M&S 도구의 VV&A에서 가장 중요한 ‘신뢰성 확보(creditation)’의 강력한 기술적 근거가 된다[1,6].

3.2 이기종 모델 보호 및 캡슐화를 위한 FMI(Functional Mock-up Interface) 표준

무기체계는 공기역학, 제어공학, 전자공학 등 다양한 도메인이 결합된 복합 시스템이므로 이기종 M&S 환경에서의 모델 통합이 필수적이다[12]. FMI는 다중 물리 시스템의 모델을 교환하고 연동 시뮬레이션

(co-simulation)하기 위해 정의된 국제 표준(IEC 규격)이다[11].

FMI 표준은 알고리즘의 IP 보호와 M&S 연동이라는 두 가지 목적을 동시에 충족하는 메커니즘을 제공한다. 모델 개발자는 시스템의 상미분방정식(ODE)이나 제어 로직을 C 코드나 컴파일된 동적 링크 라이브러리(DLL/SO) 형태인 FMU(functional mock-up unit)로 캡슐화한다[11,12].

* FMI-CS(co-simulation) 아키텍처: 특히 FMI-CS 규격은 FMU 내부에 수식뿐만 아니라 이를 연산하는 솔버(solver)까지 자체적으로 포함한다[11]. 체계 종합 업체의 마스터 시뮬레이터는 FMU의 내부 논리나 수식을 알 필요 없이, 표준화된 API(예: fmi2DoStep)를 호출하여 입력값을 전달하고 정해진 시간 스텝(time step) 이후의 출력값만을 반환받는다. 이는 유도제어 알고리즘의 ‘블랙박스화’ 요구사항을 표준화된 방식으로 구현할 수 있는 최적의 규격이다.

3.3 분산 시뮬레이션 환경의 실시간 연동을 위한 HLA/RTI 표준 아키텍처

기밀 컴퓨팅 환경에서 보호받는 블랙박스 FMU를 대규모 교전 M&S 인프라에 통합하여 설계 검증을 수행하기 위해서는, 물리적으로 분산된 시뮬레이터 간의 실시간 연동을 보장하는 미들웨어가 필요하다[10,13]. 이를 위해 미 국방성 주도로 개발된 HLA(high level architecture)와 이를 구현하는 RTI(run-time infrastructure, IEEE 1516) 표준이 적용된다[10].

HLA/RTI는 이기종 시뮬레이터(federate)들이 네트워크를 통해 단일 가상 전장(federation)을 구성할 수 있도록 다음과 같은 핵심 서비스를 제공한다.

1. 시간 관리 서비스(time management): 초음속 유도무기의 M&S는 1 ms 이하의 정밀한 시간 동기화가 요구된다. RTI는 각 시뮬레이터 간의 논리적 시간을 동기화하여, 보안 컨테이너(TEE) 내부에서 연산되는 알고리즘의 지연(latency)이 전체 시스템의 시계열적 인과성을 훼손하지 않도록 통제한다[10,13].

2. 데이터 분산 관리(data distribution management, DDM): 거대한 가상 환경에서 수많은 엔티티(표적, 재머, 유도탄 등)가 생성하는 데이터 중 특정 시뮬레이터(예: 탐색기 FMU)가 필요로 하는 데이터

만을 효율적으로 필터링하여 전송(publish/subscribe)함으로써 통신 부하를 최소화한다[10].

3.4 요소 기술의 융합: 보안 연합 M&S 아키텍처의 이론적 타당성

상기 세 가지 이론적 배경은 기존 M&S VV&A의 역순차적 한계를 극복하기 위해 상호 보완적으로 융합된다[6,10,11]. 기존에는 알고리즘 논리를 은닉하기 위해 모델을 물리적으로 격리하거나 제공 자체를 기피하였으나, 제안하는 방식에서는 FMI 표준을 통해 이기종 모델의 입출력 인터페이스를 규격화하여 블랙박스화하고, 이를 기밀 컴퓨팅(TEE) 인클레이브에 적재하여 런타임 환경의 물리적 보안과 원격 증명을 달성한다[6,11].

이렇게 보호된 M&S 모델은 HLA/RTI 미들웨어를 통해 체계 종합 업체의 대규모 가상 전장에 통합된다[10]. 결과적으로 이는 알고리즘 원천 기술 보유자의 정보 보호 요구를 하드웨어 레벨에서 100% 충족함과 동시에, 체계 종합 업체가 물리적 실사격 이전 단계에서 알고리즘의 논리적 한계와 엡지 케이스를 테스트할 수 있는 ‘설계 검증(design verification)’의 공학적 환경을 완벽하게 제공하는 이론적 기반이 된다[1,6,10].

4. 기밀 컴퓨팅 및 연합 M&S 기반의 설계 검증 프레임워크 제안

본 장에서는 역순차적 V&V의 공학적 한계를 극복하고 M&S ‘설계 검증’ 단계를 보완하기 위해, 앞선 이론적 배경을 융합한 ‘기밀 컴퓨팅 기반 보안 M&S 설계 검증 프레임워크’를 제안한다.

4.1 연합 M&S 기반 알고리즘 유통 및 런타임 연동 아키텍처

제안하는 시스템 아키텍처는 강화된 보안 통제와 원활한 시뮬레이션 환경 접근성을 네트워크 미들웨어와 하드웨어 TEE 기술을 통해 조화롭게 충족하도록 설계되었다[6,10].

1. 보안 인클레이브(Enclave) 내 M&S 모델 탑재: 알고리즘 개발 기관은 개념모델이 반영된 유도제어

논리를 FMI 표준 규격에 맞춘 바이너리 객체(FMU)로 빌드한다[11]. 이후 이 FMU를 체계 종합 업체 연산 서버의 격리된 공간인 ‘인클레이브’ 내부에 적재한다[7]. 적재 시 런타임 메모리 암호화가 활성화되어 외부의 역공학적 접근 시도가 제한된다[6].

2. HLA/RTI 미들웨어 기반 데이터 교환 계층 구축: TEE 외부에 위치한 서버 계층에는 HLA/RTI 기반의 통신 미들웨어를 배치한다[10]. 이 미들웨어는 비행 역학 시뮬레이터, 표적 기동 모의기 등으로부터 생성되는 다수의 모의 입력 파라미터를 전송받는 역할을 수행한다.

3. 보안 연산 및 결과 반환: 수신된 가상 교전 데이터는 암호화 채널을 거쳐 TEE 인클레이브 내부로 전달되어 복호화된다[6]. 이후 알고리즘 논리는 격리된 메모리 내에서 연산을 수행하여 유도 명령을 도출하며, 이 결과값은 다시 암호화되어 체계 시뮬레이터로 반환, 유도탄의 비행 궤적과 논리적 반응을 갱신한다[10,11].

4.2 M&S VV&A ‘설계 검증’ 단계의 적용 방안

본 아키텍처가 지니는 시스템 엔지니어링적 의의는, 보안 문제로 인해 단절되었던 “알고리즘 논리 타당성 확보를 위한 설계 검증 단계의 보완”에 있다[1,3]. 기존 환경에서는 내부 논리에 대한 접근 제한으로 인해 물리적 실사격 결과에 의존하여 사후 추론하는 방식에 한계가 존재했다. 그러나 제안된 프레임워크를 도입할 경우, 물리적 비행시험 이전의 가상 프로토타이핑 단계에서 수학적/논리적 모델의 적절성을 확인하는 설계 검증 활동을 수행할 수 있는 기반이 마련된다[1,6]. 체계 종합 업체는 내부 수식을 직접 확인하지 않더라도, TEE 환경을 통해 엡지 케이스를 포함한 다수의 몬테카를로 시뮬레이션을 수행할 수 있다[2]. 이를 통해 블랙박스가 개념모델에 정의된 요구 기능대로 적절한 논리적 반응을 보이는지 행위 기반(behavior-based)으로 분석함으로써, M&S 도구의 논리적 타당성을 점검할 수 있다[3].

5. 기대 효과 및 한계점

5.1 제안 프레임워크의 기대 효과

1. VV&A 프로세스의 인정(creditation) 신뢰성

향상: 제한된 샘플의 사후 데이터로 설계 논리의 적절성을 대체하던 기존 방식의 한계를 보완하고, 국방 획득 프로세스의 표준 절차 준수를 지원하여 M&S 신뢰성 확보에 기여한다[1,5].

2. 시나리오 커버리지 확장을 통한 설계 검증 고도화: 물리적 비행시험 횟수의 현실적 제약에서 벗어나, 다양한 교전 상황을 M&S 환경에서 모의할 수 있으므로 설계 논리의 수학적 타당성과 통계적 신뢰성 점검 범위를 확장할 수 있다[2,3].

3. 보안-협업 요구사항의 조율: 원천 기술 보유 기관의 IP 유출 우려를 TEE 아키텍처를 통해 효과적으로 방지함과 동시에[6], 체계 종합 관점에서는 설계 논리의 적절성 평가에 필요한 입출력 데이터를 획득할 수 있어 상호 신뢰 기반의 개발 환경 조성을 돕는다[11].

5.2 고려해야 할 기술적 제약사항

본 연구에서 제안한 기밀 컴퓨팅 M&S 환경은 TEE 메모리 영역 진출입 통제 및 암호·복호화 과정에 따른 하드웨어 연산 지연(overhead)을 동반할 수 있다[6,9]. 유도무기의 M&S는 짧은 실시간(real-time) 연산 주기가 요구되므로, TEE 도입이 전체 페루프(closed-loop) 시뮬레이션의 타이밍 정확도에 미치는 영향을 분석하고 비동기 데이터 처리를 통한 최소화 연구가 요구된다[10].

또한, 상용화된 TEE CPU의 보안 메모리 공간에는 물리적 한계가 존재하여[7], 대규모 파라미터를 다루는 복잡한 AI 탐색기 모델 전체를 적재하는 데는 제약이 따를 수 있다. 따라서 모델의 핵심 보안 연산부만을 분할(partitioning)하여 선별적으로 TEE 내에서 처리하는 최적화 기법에 대한 후속 연구가 필요하다.

6. 결론

현대 국방 복합 체계에 있어 핵심 알고리즘 기술의 보안 유지는 매우 중요한 요소이다. 그러나 보안을 사유로 M&S 도구 신뢰성 확보의 근간인 알고리즘 논리 타당성 평가 단계(설계 검증)를 부득이하게 생략하고 사후의 실사격 데이터로 대체하는 현행 방식은, 개발 예산 증가 위험과 다양한 환경에서의 신뢰성 검증 부재라는 한계를 지닌다[1,4].

본 논문은 이러한 한계를 보완하기 위해, 하드웨어 기반 정보 보호 기술인 기밀 컴퓨팅(TEE) 기법과 국방 M&S 표준(FMI, HLA/RTI)을 연계한 ‘보안 연합 M&S 기반 설계 검증 프레임워크’를 제시하였다[6,10,11]. 제안된 프레임워크는 알고리즘 공급자의 지적재산권을 런타임 환경에서 격리 및 보호하는 동시에, 체계 종합 관점에서는 물리적 제약이 완화된 가상 환경에서의 대규모 시뮬레이션을 가능케 함으로써 제한적이었던 설계 검증 체계를 보완할 수 있는 방안을 제공한다[1,6].

향후 적용 시 발생하는 연산 지연 최소화 방안과 분산 시뮬레이션 환경의 동기화 정밀도 보장을 위한 모델 분할 연구가 이어진다면, 국방 획득 프로세스의 비용 효율성 제고와 시뮬레이션 도구의 신뢰도 향상에 기여할 수 있을 것으로 기대된다.

참고문헌

- [1] Department of Defense (DoD), DoD Instruction 5000.61: DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (V&A), Washington, DC: U.S. Department of Defense, 2009.
- [2] Osman Balci, ‘Verification, Validation, and Testing,’ in Jerry Banks (Ed.), Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice, John Wiley & Sons, 1998, pp. 335–393.
- [3] Robert G. Sargent, ‘Verification and Validation of Simulation Models,’ Journal of Simulation, VOL. 7, 2013, pp. 12–24.
- [4] INCOSE (International Council on Systems Engineering), Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities (4th ed.), John Wiley & Sons, 2015.
- [5] 방위사업청, 무기체계 소프트웨어 개발 및 관리 매뉴얼, 2023.
- [6] Confidential Computing Consortium, A Technical Analysis of Confidential Computing, The Linux Foundation, 2021.
- [7] Victor Costan & Srinivas Devadas, ‘Intel SGX Explained,’ IACR Cryptology ePrint Archive, 2016, Article 086.
- [8] Sandro Pinto & Nuno Santos, ‘Demystifying Arm TrustZone: A Comprehensive Survey,’ ACM Computing Surveys (CSUR), VOL. 51, NO. 6, 2019, pp. 1–36.
- [9] Mark Russinovich, Manuel Costa, Cédric Fournet, David Chisnall, Antoine Delignat-Lavaud, Sylvan Clebsch, Kapil Vaswani, & Vikas Bhatia, ‘Toward Confidential Cloud Computing,’ Communications of the ACM, VOL. 64, NO. 6, 2021, pp. 54–61.
- [10] IEEE, ‘IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules,’ IEEE

Std 1516-2010, 2010, pp. 1-38.

[11] Torsten Blochwitz, Martin Otter, Johan Akesson, Martin Arnold, Christoph Clauß, Hilding Elmqvist, Markus Friedrich, Andreas Junghanns, Jakob Mauß, Dietmar Neumerkel et al., 'Functional Mock-up Interface 2.0: The Standard for Tool Independent Exchange of Simulation Models,' in Proceedings of the 9th International Modelica Conference, Munich,

Germany, 2012, pp. 173-184.

[12] Cláudio Gomes, Casper Thule, David Broman, Peter Gorm Larsen, & Hans Vangheluwe, 'Co-Simulation: State of the Art,' arXiv preprint arXiv:1702.00686, 2018.

[13] Frederick Kuhl, Richard Weatherly, & Judith Dahmann, Creating Computer Simulation Systems: An Introduction to the High Level Architecture, Prentice Hall PTR, 1999.