실시간 수전해 전력변환시스템 제어를 위한 경량 암호화 통신 적용 및 성능 평가

(Implementation and Performance Evaluation of Lightweight Secure Communication for Real-Time Control of Water Electrolysis Power Conversion Systems)

김영국*, 김웅식**
(Young Kook Kim, Woong Sik Kim)

요 약

탄소중립 인프라 확충에 따라 1.25~2.5MW급 수전해 전력변환시스템(PCS)과 상위 제어망 간 연계가 필수적이나, Modbus TCP의 평문 구조는 데이터 스니핑 등 사이버 위협에 취약하다. 대안인 전송 계층 보안(TLS)은 암호화 오버헤드로 인한 통신 지연을 가중시켜 실시간 임베디드 제어에 치명적인 병목을 초래한다. 이를 극복하고자 본 연구는 실시간 제어에 최적화된 경량 보안 통신 아키텍처를 제안한다. Z840 테스트베드에서 상용 명령 기반 1만 회 벤치마크를 수행한 결과, 다중 페이로드를 병합하는 일괄 전송(Bulk Transfer) 기법이 단일 전송의 고정 암호화 오버헤드를 구조적으로 상쇄함을 규명하였다. 또한 타원곡선(ECDSA) 보안 스위트를 도입해 통상적 폴링 환경에서도 10ms 이내의 제어 성능이 확정적으로 보장됨을 검증하였다. 본 최적화 모델은 정적 및 동적 분석을 통한 정량적 신뢰성 평가를 위해 향후 차세대 64비트 제어 플랫폼에 이식될 예정이다.

■ 중심어 : 수전해 시스템 제어망 ; 모드버스 TCP (Modbus TCP) 통신보안 ; 전송 계층 보안 (TLS 1.2) 오버헤드 ; Z840 시뮬레이션 테스트베드 ; 경량 암호화 알고리즘 (ECDSA)

Abstract

Integrating 1.25 - 2.5-MW water electrolysis power conversion systems (PCSs) with supervisory networks is critical for carbon neutrality, yet Modbus TCP's plaintext architecture exposes these systems to cyber threats like data sniffing. While Transport Layer Security (TLS) mitigates these risks, its cryptographic overhead exacerbates latency, creating a severe bottleneck for real-time embedded control. To address this, this article proposes a lightweight secure communication architecture tailored for real-time operations. Empirical evaluations comprising 10,000 benchmark iterations on a Z840 testbed elucidate that a bulk transfer scheme aggregating multiple payloads structurally neutralizes the fixed encryption overhead inherent in single-transfer mechanisms. Furthermore, integrating an Elliptic Curve Digital Signature Algorithm (ECDSA) suite deterministically guarantees a control cycle under 10 ms in conventional polling environments. This optimization model will be ported to next-generation 64-bit platforms for quantitative reliability validation via static and dynamic analyses.

■ keywords : Water Electrolysis Control Network ; Modbus TCP Security ; TLS 1.2 Overhead ; Simulation Testbed ; Lightweight Cryptography (ECDSA)

Ⅰ. 서 론

1. 연구의 배경 및 필요성

탄소중립 실현을 위한 수소 에너지 인프라 확충에 따라, 1.25MW~2.5MW급 대용량 수전해 전력변환시스템(PCS)이 상위 제어망과 연계되는 비중이 급

* 정회원, 건양대학교 의료인공지능학과 박사과정
** 정회원, 건양대학교 인공지능학과
이 논문은 2025년도 건양대학교 학술연구비 지원에 의하여 이루어진 것임
접수일자 : 2026년 05월 08일
수정일자 : 2026년 06월 03일
게재확정일 : 2026년 06월 09일
교신저자 : 김웅식 e-mail : wskim@konyang.ac.kr

증하고 있다[16]. 과거 폐쇄망으로 운영되던 산업 제어망이 사물인터넷(IoT) 기술의 도입과 함께 개방형 사이버-물리 시스템(CPS)으로 전환되면서 운영 효율성이 제고된 반면, 외부 네트워크와의 접점이 늘어나며 새로운 통신 보안 위협이 대두되고 있다[3], [12], [13].

현재 수전해 PCS와 상위 제어기 간 통신에는 산업용 표준인 Modbus TCP가 주로 사용된다. 그러나 해당 프로토콜은 기기 간 상호 인증 체계와 데이터 암호화 기능이 원천적으로 부재하여, 제어 지령과 계측 정보를 평문(Plaintext)으로 전송하는 구조적 한계를 지닌다[5]. 이로 인해 제어망이 개방형 네트워크에 노출될 경우 데이터 스니핑(Sniffing) 및 악의적인 제어 지령 위조(False Command Injection)[6] 등의 사이버 공격에 취약해진다. 대용량 설비의 특성상 비인가 제어 지령은 스택(Stack) 손상과 같은 물리적 사고로 직결될 수 있어 프로토콜 계층에서의 보안 강화가 필수적이다[19].

이러한 취약점을 보완하기 위해 IEEE 1547.3[12] 등 국제 표준에서는 Modbus TCP에 전송 계층 보안(TLS)을 결합할 것을 권고한다[1], [8]. 하지만 통상 수십 밀리초(ms) 이내의 실시간 제어가 요구되는 전력변환시스템에 기존 암호화 프로토콜을 일괄 적용할 경우, 인증서 교환 및 암복호화 연산으로 인한 통신 지연(Latency)이 동반된다. 특히 연산 자원이 제한된 임베디드 엣지(Edge) 환경에서 이러한 고정 오버헤드는 제어 루프의 응답성을 저해하는 병목(Bottleneck) 요인으로 작용하므로[4], 제어 주기와의 간섭을 최소화하는 최적화된 보안 통신 모델이 요구된다[2][20][21].

2. 연구의 목적 및 기여도

본 연구는 1.25MW~2.5MW급 대용량 수전해 PCS 제어망에 통신 지연을 최소화하며 적용 가능한 경량 암호화 기반 보안 통신 아키텍처를 설계하고, 실증 모델을 통해 그 타당성을 검증하는 데 목적이 있다. 본 연구의 구체적인 학술적, 실무적 기여도는 다음과 같다.

첫째, 고성능 Z840 워크스테이션을 활용하여 임베디드 엣지 환경을 모사한 시뮬레이션 테스트베드를 구축하고, 순수 Modbus TCP와 6종의 이기종 TLS 보안 스위트(RSA, ECDSA 등)를 대상으로 총 1만 회의 반복 벤치마크를 수행하여 암호화 오버헤드 데이터를 정량적으로 확보하였다.

둘째, 실제 1.25MW~2.5MW 상용 시스템에서 실시간으로 취급되는 핵심 제어 지령(유·무효 전력) 및 상태 계측 데이터 명령 체계를 벤치마크 시나리오로 구성하여 실험 결과의 산업적 실효성을 제고하였다.

셋째, 실측 통계를 바탕으로 단일 전송(Single Read/Write) 시 발생하는 지연 시간 누적 메커니즘을 규명하고, 고정 오버헤드를 완화하기 위한 데이터 일괄 전송(Bulk Transfer) 아키텍처 및 타원곡선(ECDSA) 기반 경량 암호화 체계의 유효성을 실측 데이터를 통해 확인하였다.

본 연구에서는 독자의 혼선을 방지하기 위해 1개의 레지스터에 접근하는 방식을 '단일 전송(Single Transfer)', 다수의 연속된 레지스터를 한 번에 패킹하여 접근하는 방식을 '일괄 전송(Bulk Transfer)'으로 명확히 정의한다.

3. 논문의 구성

본 논문은 다음과 같이 구성된다. 제2장에서는 스마트그리드 통신 보안 표준과 선행 연구의 한계점을 고찰한다. 제3장에서는 수전해 PCS 특화 보안 통신 아키텍처와 지연 시간 누적 방지를 위한 수학적 모델링을 제안한다. 제4장에서는 Z840 기반 실증 테스트베드 및 벤치마크 시나리오 설계 방안을 기술한다. 제5장에서는 1만 회 실측 데이터를 바탕으로 통신 방식별 성능과 오버헤드를 심층 분석한다. 마지막으로 제6장에서는 연구 결과를 종합하고 향후 실증 계획을 제시하며 결론을 맺는다.

Ⅱ. 관련 연구

1. 산업 제어망의 구조적 취약점 및 보안 위협

전통적인 운영기술(OT) 기반의 전력 및 산업 제

어 시스템(ICS)은 외부 인터넷망과 물리적으로 차단된 에어갭(Air-gap) 상태를 전제로 설계되었으며, 이에 따라 통신 편의성과 호환성이 뛰어난 이더넷 기반의 Modbus TCP 프로토콜이 사실상의 산업 표준으로 채택되었다. 그러나 인더스트리 4.0 환경으로의 전환과 함께 IT와 OT 망의 융합이 가속화되면서 해당 프로토콜의 구조적 결함이 주요한 보안 취약점으로 대두되고 있다[3]. Modbus TCP는 송수신되는 페이로드(Payload)를 암호화하지 않고 평문(Plaintext) 상태로 전송하며, 통신 주체인 마스터(Master)와 슬레이브(Slave) 간의 상호 인증(Authentication) 및 메시지 무결성 검증 메커니즘을 지원하지 않는다[5]. 이는 네트워크 패킷 분석 도구를 통해 비인가자가 제어 지령 및 계측 데이터를 쉽게 열람하거나 조작할 수 있는 환경을 제공한다. 이러한 프로토콜의 취약점으로 인해 제어망이 개방형 사이버 공간에 노출될 경우 다양한 형태의 공격 벡터(Attack Vector)가 성립된다. 선행 연구들에 따르면, 공격자가 스니핑(Sniffing)을 통해 타깃 설비의 레지스터 맵(Register Map) 주소를 파악한 후 정상적인 제어기로 위장하여 임의의 전압 및 전류 지령을 주입하는 은밀한 데이터 위조 공격(Stealthy False Command Injection)[6]이 주요 위협 중 하나로 평가된다. 또한 통신 채널에 대량의 무의미한 연결 요청을 발생시켜 가용성을 저하시키는 서비스 거부(DoS) 공격[7]이나, 스마트 인버터 제어망을 타깃으로 한 랜섬웨어 공격[14] 가능성도 제기된 바 있다. 대용량 수전해 설비의 경우, 외부의 악의적인 밸브 제어 및 전력 변환 지령 조작은 스택(Stack) 과전압이나 수소 누출 등 물리적 사고로 이어질 우려가 있으므로 통신망 차원의 방어 기제가 요구된다.

2. 스마트그리드 통신 보안 표준 및 선행 연구 동향

태양광, 풍력, 수전해 설비 등 대용량 분산전원(DER)이 스마트그리드 계통과 연계됨에 따라, 국제 표준화 기구에서는 통신망 보안 강화를 위한 규격을 지속적으로 구체화하고 있다. 대표적으로 IEEE 1547.3 표준 가이드라인은 분산전원 기기의 사이버 보안 요구사항을 정의하며, 데이터의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장하기 위한 암호화 통신 채널의 적용을 명시하고 있다[16]. 아울러 에너지 관리 시스템(EMS) 및 마이크로그리드 보안을 다룬 다수의 문헌들은 개방형 네트워크상에서 가상 사설망(VPN)이나 전송 계층 보안(TLS)을 활용하여 논리적 터널을 생성하는 기법들을 제안해 왔다[11], [13].이러한 산업적 요구를 반영하여 Modbus 협회(Modbus Organization)는 2018년 기존 502번 포트 대신 802번 보안 포트를 할당하고, X.509 인증서와 TLS 1.2 이상의 프로토콜을 결합한 'Modbus/TCP Security Protocol Specification'을 공식 발표하였다[20]. 이 규격은 응용 계층의 Modbus 메시지 포맷을 유지한 채 전송 계층에서 패킷을 캡슐화하여 기밀성을 확보하는 방안을 제시한다. 그러나 이를 구현 및 평가한 기존의 선행 연구들[1], [8]은 주로 암호화 프로토콜의 논리적 연동 가능성이나 소프트웨어 기반의 단일 패킷 분석에 초점을 맞추는 경향이 있다. 수십 밀리초(ms) 이내의 실시간 응답성과 정밀한 PWM 제어 루프가 요구되는 전력변환시스템(PCS) 임베디드 제어 환경의 제약 조건을 충분히 반영한 실증 연구는 아직 미흡한 단계에 있다.

3. 실시간 제어 환경에서의 기존 연구 한계점 분석

전력변환시스템에 기존 TLS 프로토콜을 그대로 도입할 경우 직면하는 핵심적인 공학적 과제는 통신 지연(Latency)의 증가이다. 핸드셰이크(Handshake) 단계에서의 인증서 교환, 무거운 RSA(Rivest-Shamir-Adleman) 알고리즘 기반의 비대칭키 연산, 그리고 매 패킷마다 수반되는 대칭키 암복호화 및 메시지 인증 코드(MAC) 연산은 필연적인 암호화 오버헤드(Tcrypto)를 발생시킨다[4].

최근 스마트그리드 및 분산전원 제어망 보안과 관련하여 다양한 선행 연구들이 수행되어 왔으나, 실시간 제어 환경 적용 관점에서는 명확한 한계가 존재한다(표 1 참조). Ferst 등[1]과 Mlot 등[8]은 SunSpec Modbus와 TLS를 연동하여 보안 통신의 논리적 구현 가능성을 입증하였으나, 주로 단일 패킷 단위의 소프트웨어적 분석에 머물러 실제 전력 설비의 밀리초(ms) 단위 제어 주기를 충족하는지에 대한 하드웨어 이식 및 실증이 부족하다. 또한, Wang 등[2]과 Zhang 등[4]은 경량 암호화 알고리즘을 도입하여 지연 시간을 단축하고자 하였으나, 대용량 설비 제어 시 발생하는 대규모 레지스터 데이터의 연속적인 전송 상황을 고려하지 못했다.

표 1. 제어망 보안 통신 관련 주요 선행 연구 비교 분석

선행 연구	주요 연구 내용 및 초점	실시간 제어 주기 (Latency) 고려	데이터 일괄 전송 (Bulk Transfer) 적용	연구의 한계점
Ferst 등 [1] (2025)	SunSpec Modbus 및 TLS 프로토콜 연동 논리 구현	△	X	통신 프로토콜의 소프트웨어적 연동 검증에 그치며, 제어 응답성 실측 부재
Wang 등 [2] (2025)	Modbus TCP를 위한 경량 암호화 알고리즘 설계	O	X	알고리즘 자체 경량화에 집중하였으나, 다수 레지스터 전송 시 누적 지연 한계 존재
Zhang 등 [4] (2024)	ZUC 알고리즘 기반 초저지연 Modbus 보안 강화	O	X	단일 패킷 기준 지연 최소화에 초점, 수십 개 이상의 페이로드 환경 실증 부족
Mlot 등 [8] (2022)	산업용 분산전원 시스템 보안 SunSpec 테스트베드	X	X	암호화 연산에 따른 병목 현상 및 오버헤드의 정량적 지표 제시 미흡
본 연구	대용량 수전해 PCS 제어망 특화 보안 아키텍처	O (1만 회 벤치마크)	O (구조적 오버헤드 상쇄)	통제된 벤치마크를 통해 다중 전송 시 고정 오버헤드 상쇄 효과(O(N) → O(1)) 실측 입증

대용량 수전해 설비는 가동 중 수십에서 수백 개의 계측 데이터(전압, 전류, 온도 등)와 제어 지령을 지속적으로 교환해야 한다. 단일 레지스터를 개별적으로 요청하는 기존의 단일 전송(Single Read/Write) 방식으로 암호화 통신을 수행할 경우, 앞서 언급한 고정 오버헤드가 매 요청마다 누적되어 통신 지연을 크게 가중시킨다. 연산 자원이 한정된 임베디드 엣지(Edge) 환경에서 이러한 오버헤드의 지수적 누적은 실시간 제어 루프의 응답성을 저하시키는 주요 병목(Bottleneck) 요인으로 작용할 수 있다[12].

이를 극복하기 위해 데이터를 연속된 레지스터에 맵핑하여 한 번에 묶어 보내는 일괄 전송(Bulk Transfer) 아키텍처 단위의 통신 최적화가 필요하다. 하지만 표 1에서 나타나듯, 관련 통신 구조의 변경이 보안 오버헤드 상쇄에 미치는 영향을 1.25MW~2.5MW급 실제 설비 시나리오를 바탕으로 수만 회 단위의 벤치마크를 통해 정량화한 선행 연구는 아직 충분히 이루어지지 않은 실정이다. 본 연구는 이러한 한계를 보완하여, 실증적 데이터에 기반한 최적화 모델을 제시하고자 한다.

Ⅲ. 수전해 PCS 보안 통신 아키텍처 및 지연 시간 분석 모델

1. TLS 1.2 기반 보안 통신 구조 및 오버헤드 정량화

본 연구에서 다루는 수전해 PCS 보안 통신 아키텍처는 상위 에너지 관리 시스템(EMS)과 임베디드 엣지(Edge) 제어기 간의 Modbus TCP 통신 계층에 국제 표준 암호화 규격인 TLS 1.2를 결합한 형태이다. 이 아키텍처는 응용 계층(Application Layer)의 Modbus 메시지 포맷을 유지하면서 전송 계층(Transport Layer)에서 패킷 전체를 캡슐화하여 데이터의 기밀성과 무결성을 확보한다. 이러한 보안 기제는 외부 네트워크로부터의 데이터 유출이나 변조를 차단하는 데 유효하지만, 실시간 응답성이 필수적인 PCS 제어 환경에서는 암호화 연산에 따른 지연 시간(Latency)의 정량적 분석이 선행되어야 한다.기존 비암호화 상태의 순수 Modbus TCP 1회 트랜잭션 소요 시간 $T_{standard}$는 네트워크 전송 시간(T_{net})과 제어기 메시지 처리 시간(T_{proc})의 합으로 정의된다.

$$T_{standard} = T_{net} + T_{proc} \quad (1)$$

반면, TLS 1.2 보안 통신이 적용된 모델의 소요 시간 T_{secure}는 기본 소요 시간에 대칭키 암호화(T_{enc}), 복호화(T_{dec}), 메시지 인증 코드(MAC) 연산 시간(T_{mac})을 포함하는 고정 암호화 오버헤드(T_{crypto})가 추가된다.

$$T_{secure} = T_{net} + T_{proc} + T_{enc} + T_{dec} + T_{mac} = T_{standard} + T_{crypto} \quad (2)$$

연산 자원이 제한적인 임베디드 환경에서 T_{crypto}는 전체 통신 응답성의 주요 병목 요인으로 작용하므로, 이를 최소화하기 위한 암호화 알고리즘의 선별과 통신 아키텍처의 구조적 최적화가 요구된다.

2. 타원곡선 암호(ECDSA) 기반의 경량 보안 체계 적용

수전해 PCS의 제어 루프는 전력 계통의 변동에 즉각적으로 대응하기 위해 높은 실시간성을 유지해야 한다. 따라서 초기 세션 연결 시 발생하는 핸드셰이크(Handshake) 연산 부하를 저감하기 위해, 기존의 RSA(Rivest-Shamir-Adleman) 방식 대신 타원곡선 암호학(ECC)에 기반한 ECDHE-ECDSA 스위트를 적용한다. 타원곡선 이산대수 문제(ECDLP)의 수학적 복잡성을 활용하는 ECC는 유한체 F_p 상에서 다음과 같은 바이어슈트라스(Weierstrass) 방정식으로 정의된다.

$$y^2 \equiv x^3 + ax + b \pmod{p} \quad (3)$$

단, $4a^3 + 27b^2 \neq 0 \pmod{p}$를 만족하여 비특이 곡선을 형성해야 한다. ECDSA는 256비트의 짧은 키 길이만으로도 RSA 3072비트와 대등한 보안 강도를 제공하므로, PCS 제어 보드 환경에서 디지털 인증서의 크기를 축소하고 서명 검증 속도를 단축시키는 데 유리하다. 또한 ECDHE(Elliptic Curve Diffie-Hellman Ephemeral) 알고리즘은 매 세션마다 독립적인 일회성 키를 생성하여, 장기 키 유출 시에도 과거 통신 내역의 보안성을 유지하는 순방향 비밀성(Perfect Forward Secrecy, PFS)을 보장한다.

3. 지연 시간 누적 상쇄를 위한 일괄 전송(Bulk Transfer) 분석 모델

1.25MW~2.5MW급 상용 수전해 설비는 운용 중 수십 개 이상의 계측 데이터와 제어 지령을 실시간으로 교환한다. 보안 통신 환경에서 개별 레지스터를 순차적으로 요청하는 단일 전송(Single Read/Write) 방식을 N번 수행할 경우, 누적 지연 시간 T_{single_total}은 다음과 같이 고정 암호화 오버헤드가 N배로 증폭되는 구조적 한계를 나타낸다.

$$T_{single\_total} = \sum_{i=1}^{N} (T_{standard\_i} + T_{crypto\_i}) \approx N \times (T_{standard} + T_{crypto}) \quad (4)$$

이러한 지연 시간의 지수적 증가를 방지하기 위해, 데이터를 연속된 레지스터 맵(Register Map)에 배치하여 단일 트랜잭션으로 패킹하는 데이터 일괄 전송(Bulk Transfer) 아키텍처를 도입한다. 페이로드의 크기가 증가하더라도 대칭키 알고리즘인 AES-GCM의 연산 효율성으로 인해 암호화 연산 시간의 증분은 상대적으로 미미하다. 따라서 일괄 전송 시의 전체 지연 시간 T_{multi_total}은 다음과 같이 단일 트랜잭션의 오버헤드 수준으로 수렴한다.

$$T_{multi\_total} = T_{standard\_bulk} + T_{crypto\_bulk} \approx 1 \times (T_{standard} + T_{crypto}) \quad (5)$$

결과적으로 $T_{multi_total} \ll T_{single_total}$의 관계가 성립하며, 이는 보안 통신 환경에서 레지스터 최적화를 통한 일괄 전송 방식이 실시간 제어 주기 보장을 위한 필수적인 요건임을 시사한다. 이어지는 장에서는 구축된 실증 테스트베드를 통해 이 분석 모델의 유효성을 실측 데이터로 검증한다.

Ⅳ. 실증 테스트베드 구축 및 벤치마크 시나리오 설계

1. 아키텍처 검증을 위한 Z840 기반 실증 테스트베드 구축 및 방법론적 타당성

본 연구에서는 제안하는 보안 통신 아키텍처의 구조적 성능 개선 효과를 정량적으로 분석하기 위해, 고성능 Z840 워크스테이션 환경에서 상위 EMS와 임베디드 엣지 제어기를 가상화한 실증 테스트베드를 구축하였다. 본 연구의 궁극적인 적용 대상은 연산 자원이 제한적인 수전해 PCS 임베디드 보드이나, 벤치마크에서는 워크스테이션을 선제적 실증 환경으로 채택하였다. 이는 임베디드 하드웨어 사양(프로세서 클럭, 메모리 대역폭 등)에 종속적으로 발생하는 가변적 병목 현상을 통제하고, 순수하게 통신 프로토콜의 구조적 최적화(단일 전송 대 일괄 전송)와 암호화

알고리즘 자체의 오버헤드 편차만을 독립적으로 추출하기 위함이다.본 논문에서 제안하는 일괄 전송 아키텍처의 핵심은 개별 데이터 요청 시 발생하는 N번의 네트워크 왕복(Round-trip) 지연과 고정 오버헤드를 구조적으로 단일화($O(N) \rightarrow O(1)$)하는 데 있다. 통제된 고성능 환경에서의 실증은 하드웨어 성능과 무관하게 지연 시간 누적을 근본적으로 상쇄할 수 있음을 실측을 통해 검증하였다. 연산 능력이 열악한 실제 임베디드 보드 이식 시, 절대적인 암복호화 연산 시간은 증가하더라도 본 연구에서 규명한 '다중 전송 최적화에 따른 상대적 오버헤드 감소율(%)'의 이득은 유지된다.또한, 매 통신마다 발생하는 핸드셰이크 부하를 방지하기 위해 Session Resumption 기법을 적용하여 최초 1회만 비대칭키 교환을 수행하고 이후에는 대칭키(AES) 레코드 패킷만 암복호화하도록 네트워크를 구성하였다. 실험군은 비암호화 기반 Modbus TCP(Port 5020)와 TLS 보안 스위트 6종(Port 8020, 8021 등)으로 구성되었으며, IP 서브넷과 포트 라우팅을 분리하여 외부 트래픽 간섭을 차단하였다.

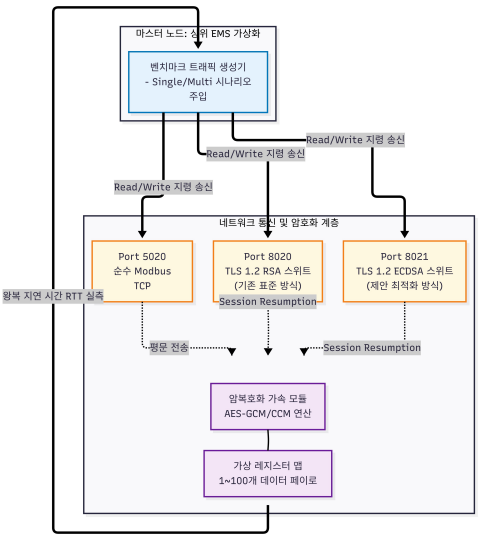

그림 1. 통신 지연 시간 실측을 위한 Z840 기반 벤치마크 테스트베드 구성 및 실험 절차도

표 2. 제안 아키텍처 성능 검증을 위한 벤치마크 실험 설계 및 변수 통제표

구분	변수명	설정 및 적용 내용	비고
통제 변수 (Control Variables)	하드웨어 환경	HP Z840 Workstation (Dual Intel Xeon)	하드웨어 사양에 따른 가변적 연산 병목 통제
	네트워크 환경	로컬 격리망 (외부 트래픽 간섭 0%)	순수 알고리즘 및 프로토콜 지연 시간만 추출
	반복 횟수	각 시나리오별 왕복 (Round-trip) 10,000회	통계적 신뢰도 확보 및 우발적 Jitter 보정
독립 변수 (Independent Variables)	통신 스위트	비암호화 Modbus TCP (1종) TLS 기반 보안 스위트 (6종)	RSA, ECDSA 등 암호화 알고리즘 비교
	전송 아키텍처	단일 전송 (Single Read/Write) 일괄 전송 (Multi Read/Write)	레지스터 페이로드 크기 최적화 유무 비교
	페이로드 크기	Read (1개, 100개) / Write (1개, 50개)	실제 1.25~2.5MW 상용 설비의 레지스터 맵 기준
종속 변수 (Dependent Variables)	통신 지연 시간 (End-to-End Latency)	마스터의 지령 송신부터 슬레이브의 암복호화를 거쳐 최종 응답 수신까지 걸린 시간 (단위: ms)	제안 모델의 고정 오버헤드 상쇄 효과 증명 지표

2. 1.25MW~2.5MW 상용 수전해 설비 제어 시나리오 구성

벤치마크 테스트의 신뢰성과 결과의 산업적 실효성을 확보하기 위해, 1.25MW~2.5MW급 상용 수전해 설비의 실제 현장 운용(FAT 및 상업 운전) 조건을 시나리오에 엄격히 반영하였다. 대용량 수전해 PCS는 실시간 모니터링 및 정밀 제어를 위해 스택(Stack) 전압, 전류, 온도, 냉각수 상태 등 수십 개 이상의 계측 레지스터를 주기적으로 교환해야 한다. 이러한 트래픽 특성을 반영하여 전체 통신 패턴을 단일 레지스터 읽기/쓰기(Single Read/Write, 각 1개 전송)와 다중 레지스터 읽기/쓰기(Multi Read 100개, Multi Write 50개)의 네 가지 형태로 세분화하였다. 특히 다중 읽기 시나리오의 100개 레지스터 단위는 상용 설비가 단일 제어 주기 동안 필수적으로 취득해야 하는 핵심 데이터의 실무적 규모를 기준으로 산정되었다.

3. 성능 평가 및 벤치마크 수행 지표

성능 평가는 앞서 구성된 7종의 통신 스위트와 4가지 전송 패턴을 교차 조합하여 진행되었다. 통신 과정에서의 우발적인 지연 변동(Jitter)을 통계적으로 보정하고 데이터의 신뢰도를 확보하기 위해, 각 실험 조건당 10,000회의 왕복 통신(Round-trip)을 연속 수행하였다.

측정 지표는 상위 제어기가 지령을 송신한 시점부

터 슬레이브 노드의 암복호화 처리를 거쳐 최종 응답을 수신하기까지 소요된 전체 통신 지연 시간(Latency, 단위: ms)으로 설정하였다. 본 벤치마크를 통해 확보된 실측 데이터는 제5장에서 단일 전송 방식의 고정 오버헤드 누적 문제와 일괄 전송(Bulk Transfer) 도입에 따른 상쇄 효과를 분석하는 근거로 활용된다.

Ⅴ. 성능 평가 및 벤치마크 결과 분석

1. 보안 통신 스위트별 벤치마크 실측 결과 종합

본 연구에서 구축한 Z840 워크스테이션 기반 시뮬레이션 환경에서 순수 Modbus TCP(비암호화) 및 6종의 이기종 TLS 보안 스위트를 대상으로 각 10,000회 왕복 통신(Round-trip)을 수행한 평균 지연 시간(Latency) 실측 결과는 표 1과 같다. 통신 패턴은 단일 읽기(Single Read, 1개 레지스터), 다중 읽기(Multi Read, 100개 레지스터), 단일 쓰기(Single Write, 1개 레지스터), 다중 쓰기(Multi Write, 50개 레지스터)로 구분하여 측정되었다.

표 3. 제어망 7종 통신 스위트 정밀 벤치마크 결과 (평균 지연 시간, 단위: ms)

통신 스위트 (Cipher Suite)	Single Read	Multi Read	Single Write	Multi Write
순수 Modbus TCP (비암호화)	0.9100	0.9951	0.8407	0.7155
RSA + AES-128-GCM	6.0196	6.0089	5.8363	5.9889
RSA + AES-256-GCM	5.8129	5.8491	5.7752	5.9772
ECDHE-RSA + AES-128-GCM	6.0422	5.9774	5.7794	5.9941
ECDHE-ECDSA + AES-128-GCM	5.0298	5.3338	5.0771	5.0404
ECDHE-ECDSA + AES-256-GCM	5.2935	5.1376	5.0658	5.2313
ECDHE-ECDSA + AES-128-CCM8	5.0384	5.1084	5.3137	9.9543

표 3에서 주목할 점은 ECDHE-ECDSA + AES-128-CCM8 스위트의 Multi Write 지연 시간이 9.9543ms로 다른 스위트 대비 유독 높게 측정되었다는 점이다. 이는 암호학적 구조의 한계에 기인한다. GCM(Galois/Counter Mode)은 내부적으로 병렬 처리가 가능하여 페이로드가 커져도 암호화 속도 저하가 적은 반면, CCM 모드는 CBC-MAC 기반으로 데이터 블록을 반드시 순차적으로 처리해야 하므로 50개의 레지스터 데이터를 전송하는 Multi Write 시나리오에서 연산 병목이 발생한 것이다.

2. 경량 암호화(ECDSA) 적용에 따른 고정 오버헤드 감소 분석

표 3의 측정 데이터를 살펴보면, 비암호화 상태인 순수 Modbus TCP의 1회 통신 지연은 Single Read 기준 평균 0.9100ms로 나타났다. 반면 산업 표준에서 보편적으로 사용되는 'RSA + AES-128-GCM' 스위트를 적용할 경우 평균 6.0196ms로 증가하여, 전송 계층 암호화로 인해 약 5ms 수준의 고정 오버헤드가 추가 발생함을 확인하였다.

이에 반해 본 연구에서 제안한 타원곡선 기반의 'ECDHE-ECDSA + AES-128-GCM' 스위트를 적용한 결과, 동일한 Single Read 조건에서 지연 시간이 평균 5.0298ms로 측정되었다. 이는 기존 RSA 기반 아키텍처 대비 암호화 연산 오버헤드를 약 16.4% 감축한 결과이다. 연산 성능이 제한된 PCS 제어 보드 환경을 고려할 때, 타원곡선 알고리즘의 짧은 키 길이와 고속 서명 검증 프로세스가 통신 응답성 개선에 유의미하게 기여함을 입증하는 수치이다.

3. 통신 아키텍처(Single vs Multi) 최적화에 따른 지연 누적 상쇄 효과

본 벤치마크 실측 결과에서 도출된 가장 주요한 분석점은 통신 아키텍처(단일 전송 대 일괄 전송)에 따른 지연 시간의 비대칭적 증가 양상과, 이를 활용한 통신 최적화 모델의 실효성 입증에 있다. 1.25MW~2.5MW급 대용량 수전해 설비는 실시간 모니터링을 위해 최소 100개 이상의 레지스터 데이

터를 주기적으로 교환해야 한다.

만약 기존 방식대로 RSA 기반 암호화 통신 하에서 100개의 데이터를 단일 읽기(Single Read)로 개별 요청할 경우, 1회 지연 시간(6.0196ms)이 누적되어 총 601.96ms라는 과도한 통신 지연을 유발한다. 이는 수십 ms 이내의 제어 주기가 요구되는 전력변환시스템에서 통신 타임아웃을 유발할 수 있는 구조적 한계를 나타낸다.

그러나 본 연구의 최적화 모델에 따라 ECDSA 기반 암호화와 레지스터 일괄 전송(Multi Read 100개) 아키텍처를 결합한 결과, 실측 지연 시간은 5.3338ms로 측정되었다. 페이로드(Payload) 크기가 1개에서 100개로 대폭 증가했음에도 대칭키 암호화 연산의 효율성으로 인해 전체 통신 시간의 증분은 0.304ms 증가하는 데 그쳤다.

결과적으로 데이터 일괄 전송 아키텍처를 도입함으로써 기존 방식의 단순 누적 지연(601.96ms) 대비 데이터 수집 소요 시간을 약 99.1% 이상 단축시키는 최적화 결과를 도출하였다. 이는 제3장에서 제시한 다중 전송 지연 시간 근사화 모델이 실제 시스템 하에서도 유효하게 성립함을 수치적으로 뒷받침하며, 실시간성이 요구되는 보안 제어망 구축 시 레지스터 구조 최적화가 필수적으로 수반되어야 함을 실측 결과로 확인하였다.

페이로드 크기가 1개에서 100개로 대폭 증가했음에도 암호화 연산 시간의 증분이 불과 0.304ms에 그친 이유는, 대칭키 알고리즘(AES-GCM)의 블록 병렬 처리 효율성 때문이다. 실제 암호화 연산 자체에 소요되는 시간은 마이크로초 단위이며, 전체 지연 시간의 대부분은 패킷 조립 및 네트워크 계층 통과 등 프로토콜의 고정 오버헤드가 차지한다.

이러한 실측 결과를 바탕으로 저사양 임베디드 보드(AM335x 등)로의 이식 상황을 공학적으로 추정할 때, 보드 사양의 한계로 인해 절대적인 연산 지연이 워크스테이션 대비 수 배 증가하더라도 일괄 전송이 제공하는 99.1%의 상대적 단축 효과를 통해 전체 통신 지연을 10ms 이하로 억제할 수 있다. 특히 현재의 수전해 제어망이 이벤트 방식이 아닌 기본 폴링(Polling) 방식으로 동작하는 제약 속에서도, 제안하는 아키텍처는 네트워크 왕복 횟수 자체를 단일화하므로 10ms 이내의 실시간 제어 주기를 안정적으로 보장할 수 있는 유효한 설계 기준임을 확인하였다.

Ⅵ. 결 론

본 연구에서는 1.25MW~2.5MW급 대용량 수전해 PCS 제어망의 보안성을 확보함과 동시에 실시간 제어 주기를 보장하기 위한 경량 암호화 기반 통신 아키텍처를 설계하고 실증하였다. 전송 계층 보안(TLS 1.2)을 도입하였으며, 고정 오버헤드 누적 문제를 해결하기 위해 타원곡선(ECDSA) 기반 일괄 전송(Bulk Transfer) 기법을 결합한 최적화 모델을 구축하였다.

Z840 테스트베드 실증 결과, 100개의 레지스터를 일괄 전송하는 아키텍처를 적용하여 단일 전송 누적 지연(약 601.96ms) 대비 데이터 수집 소요 시간을 5.33ms 수준으로 단축시켰다. 본 측정 결과는 통제된 고성능 x86 환경에서 도출된 결과이므로 실제 임베디드 보드 이식 시 절대적 지연 시간은 증가할 수 있다는 한계가 존재한다. 그럼에도 불구하고, 일괄 전송 아키텍처의 상대적인 지연 상쇄 효과는 연산 자원이 부족한 저사양 환경에서 오히려 유지되어 실시간 제어 주기를 안정적으로 보장할 수 있을 것으로 사료된다.

향후 본 연구의 통신 최적화 모델은 64비트 아키텍처 기반의 차세대 산업용 제어 플랫폼에 이식될 예정이다. 특히 산업 현장에서 발생하는 원인 불명의 통신 장애 및 정지 현상 등을 객관적으로 규명하고 구조적으로 해결하기 위해, cppcheck를 비롯한 정적 코드 분석(Static Analysis)과 런타임 동적 분석(Dynamic Analysis) 도구를 교차 활용하여 제어 소프트웨어의 신뢰성을 코드 레벨에서 정량적으로 검증할 계획이다. 이를 통해 대용량 분산전원 시스템에 범용적으로 적용 가능한 표준 보안 가이드라인 수립에 기여하고자 한다.

REFERENCES

[1] M. K. Ferst, G. W. Denardin, C. M. O. Stein, E. G. Carati, J. P. da Costa, and R. Cardoso, “Implementation and analysis of a secure communication with SunSpec Modbus and Transport Layer Security protocols for short-term energy management systems,” *IEEE Access*, vol. 13, pp. 1-15, 2025.

[2] Y. Wang, X. Li, and Z. Chen, “A security-enhanced scheme for ModBus TCP protocol based on lightweight cryptographic algorithm,” *Electronics*, vol. 14, no. 18, pp. 3456-3470, 2025.

[3] M. T. Loukas and K. V. P. Kumar, “Unraveling the threat landscape of CPS: Modbus TCP vulnerabilities in the era of I4.0,” *Proc. IEEE Int. Conf. Cyber Secur. Resil. (CSR)*, pp. 112-118, 2024.

[4] D. Zhang, Y. Gao, Q. Pan, and C. Yang, “Ultra-low latency security hardening of Modbus/TCP protocol based on ZUC cryptographic algorithm,” *Proc. IEEE 12th Int. Conf. Inf., Commun. Netw. (ICICN)*, pp. 25-30, 2024.

[5] G. F. C. Silva and T. R. Oliveira, “Securing Modbus TCP communications in I4.0: A penetration testing approach using OpenPLC and Factory IO,” *Proc. IEEE 19th Int. Conf. Fact. Commun. Syst. (WFCS)*, pp. 1-8, 2023.

[6] W. Alsabbagh, S. Amogbonjaye, D. Urrego, and P. Langendörfer, “A stealthy false command injection attack on Modbus based SCADA systems,” *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, pp. 1-9, 2023.

[7] A. Rahman, G. Mustafa, A. Q. Khan, M. Abid, and M. H. Durad, “Launch of denial of service attacks on the Modbus/TCP protocol and development of its protection mechanisms,” *Int. J. Crit. Infrastruct. Prot.*, vol. 39, pp. 100568, 2022.

[8] E. D. G. Mlot, J. Saldana, and R. J. Rodríguez, “Towards a testbed for critical industrial systems: SunSpec protocol on DER systems as a case study,” *Proc. IEEE 27th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, pp. 1-8, 2022.

[9] S. A. Ghauri, M. F. Tahir, and A. Q. Khan, “A new hybrid wavelet transform-deep learning for smart resilient inverters in microgrids against cyberattacks,” *IEEE Access*, vol. 13, pp. 10234-10245, 2025.

[10] M. A. A. E. M. E. Sayed and S. K. Mazumder, “Resilient, auditable, and secure IoT-enabled smart inverter firmware amendments with blockchain,” *IEEE Internet Things J.*, vol. 11, no. 5, pp. 8304-8318, 2024.

[11] J. Qi and A. Hahn, “Cybersecurity for distributed energy resources and smart inverters,” *IEEE Power Energy Technol. Syst. J.*, vol. 11, pp. 45-56, 2024.

[12] R. Fu, M. E. Lichtenwalner, and T. J. Johnson, “A review of cybersecurity in grid-connected power electronics converters: Vulnerabilities, countermeasures, and testbeds,” *IEEE Access*, vol. 11, pp. 113543-113559, 2023.

[13] L. Yuanliang and J. Yan, “Cybersecurity of smart inverters in the smart grid: A survey,” *IEEE Trans. Power Electron.*, vol. 38, no. 5, pp. 6254-6270, 2023.

[14] B. Ahn, A. M. Jenkins, and T. Kim, “Exploring ransomware attacks on smart inverters,” *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 2, pp. 1563-1574, 2023.

[15] N. Gajanur, M. D. R. Greidanus, and S. K. Mazumder, “Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter,” *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11782-11795, 2022.

[16] P. K. Singh and A. K. Jain, “High performance switched moded power conversion for photovoltaic integrated hydrogen based energy system,” *Proc. 3rd IEEE Int. Conf. Smart Technol. Power Energy Control (STPEC)*, pp. 1-6, 2023.

[17] J. Johnson, M. E. Ralph, and C. B. Jones, “Evaluation of interoperable distributed energy resources to IEEE 1547.1 using SunSpec modbus, IEEE 1815, and IEEE 2030.5,” *IEEE Access*, vol. 9, pp. 142129-142146, 2021.

[18] H. Zhang, B. Liu, and H. Wu, “Smart grid cyber-physical attack and defense: A review,” *IEEE Access*, vol. 9, pp. 29641-2965

[19] 지일환, 전승호, 서정택, "전력계통 네트워크 통신방식 변화에 따른 사이버위협 분석 및 대응방안 제시," 스마트미디어저널, 제12권, 제2호, 91-102쪽, 2023년 3월

[20] 윤기하, 박성모, "128비트 LEA 암호화 블록 하드웨어 구현 연구," 스마트미디어저널, 제4권, 제4호, 39-46쪽, 2015년 12월

[21] 윤기하, 박성모, "LEA 암·복호화 블록 파이프라인 구현 연구," 스마트미디어저널, 제6권, 제3호, 9-14쪽, 2017년 9월

저 자 소 개

김영국(정회원)

2006년:인하대학교 컴퓨터정보공학과 (공학석사)
2008년 ~ 2022년 전력 AMII 사업 참여
2022년 ~현재 : 데스틴파워 책임.
2023년~현재:건양대학교 의료인공지능학과 (박사과정)

<주관심분야 : 스마트그리드, 수전해시스템, 인공지능>

김웅식 (정회원)

1989년 2월:인하대학교 정보공학(공학석사)
2007년 2월:인하대학교 컴퓨터정보공학과 (공학박사)
2006년 3월 ~현재:건양대학교 인공지능학과 교수

<주관심분야 : 딥러닝,머신러닝,의료공학>