SECURITY RESEARCH WHITE PAPER

vulnhunterai.com | Public Disclosure

Critical Authentication Vulnerabilities in GE Vernova Universal Relay Platform

IEC 60870-5-104 Protocol Implementation

CVSS 9.8 CRITICAL

19 Product Lines Affected	5 Firmware Versions	15+ Years Unpatched

Field	Detail	Field	Detail
Researcher	Ryan Sharpnack	**CVSS Score**	**9.8 CRITICAL**
Organization	VulnHunter AI	**CWE**	CWE-306, 287, 311, 862
Research Date	February 7-9, 2026	**Attack Vector**	Network / No Auth
Disclosure Date	March 12, 2026	**Vendor**	GE Vernova
CISA Submission	February 9, 2026	**Protocol**	IEC 60870-5-104

1. Executive Summary

This white paper discloses critical authentication and encryption vulnerabilities in GE Vernova's Universal Relay (UR) firmware platform affecting the IEC 60870-5-104 SCADA protocol implementation. This research was submitted to CISA via the VINCE coordinated disclosure platform on February 9, 2026. CISA has declined to formally coordinate the disclosure, citing the optional nature of IEC 62351-5 authentication as a standards-level issue rather than a specific exploitable defect. This white paper is published in the interest of public awareness and critical infrastructure protection.

CRITICAL FINDING
GE Vernova Universal Relay firmware version 8.70 — the latest production release as of November 2024 — implements IEC 60870-5-104 exclusively over unsecured TCP port 2404 with no authentication, no encryption, and no authorization checks. An attacker with network access to this port can execute circuit breaker control commands without any credentials. This vulnerability has persisted across 15+ years and five analyzed firmware versions.

1.1 What Was Found

IEC 60870-5-104 is the dominant SCADA protocol for electric utility networks in Europe, Asia, and Latin America. It is used to send control commands — including circuit breaker trip and close commands — between control systems and protection relays in substations. The GE Universal Relay platform is one of the most widely deployed relay families in the world, spanning 19 product lines.

Analysis of five firmware versions spanning from 2009 (v5.49) to November 2024 (v8.70) reveals that GE has consistently implemented IEC 104 exclusively over unauthenticated port 2404, while simultaneously implementing comprehensive TLS infrastructure and other IEC 62351 security standards within the same firmware — but not applying those security features to the IEC 104 protocol. This is not a technical limitation. It is a design decision.

1.2 Why It Matters

An attacker with network access to port 2404 on a GE Universal Relay can:

- Establish a TCP connection with no authentication challenge
- Send breaker control commands (Type ID C_SC_NA_1) that execute immediately
- Trip circuit breakers serving hospitals, emergency services, or entire distribution feeders
- Interfere with protection relay operation during actual fault conditions
- Cause cascading failures across interconnected grid infrastructure

This is not theoretical. The IEC 60870-5-104 protocol is publicly documented. Client libraries including lib60870 are freely available. The attack requires no specialized equipment, no reverse engineering, and no exploit development. Any attacker with network access and basic protocol knowledge can execute this attack.

1.3 The Standards Gap

The root cause is the optional nature of IEC 62351-5 — the security extension that defines TLS-based authentication for IEC 104. Because the standard is optional, vendors can ship IEC 104-capable devices with zero authentication and remain fully compliant with the published specification. Industry-wide adoption of IEC 62351-5 is estimated below five percent globally. The standard has existed since 2007.

1.4 Researcher Background

Ryan Sharpnack is an independent ICS security researcher and the founder of VulnHunter AI. He has submitted over 35 vulnerability disclosures to CISA covering the GE Universal Relay platform, including

findings in IEC 61850 GOOSE, DNP3, and Modbus protocol implementations. He is an accepted speaker at the SANS ICS Security Summit 2026 in Orlando, Florida. All research is conducted through static firmware analysis of publicly available firmware — no unauthorized access to production systems is performed.

2. IEC 60870-5-104 Protocol Background

2.1 Protocol Overview

IEC 60870-5-104 is an international standard published by the International Electrotechnical Commission that defines network access for IEC 60870-5-101 telecontrol messaging using TCP/IP. It is the dominant SCADA protocol for electric utility control systems in European, Asian, and Latin American markets, where it has largely displaced older serial-based protocols.

The protocol operates in a client/server model where a master station (SCADA control system) communicates with controlled stations (protection relays, RTUs, substation automation devices). Messages are structured as Application Protocol Data Units (APDUs) containing Application Service Data Units (ASDUs) that carry commands and measurement data.

2.2 Why This Protocol Controls Physical Infrastructure

IEC 104 is not merely a monitoring protocol. It carries control commands that directly operate physical equipment in substations. The critical command types relevant to this research include:

Type ID	Command Name	Criticality	Physical Action
C_SC_NA_1 (45)	Single Command	**CRITICAL**	Breaker trip / close
C_DC_NA_1 (46)	Double Command	**CRITICAL**	Two-state device control
C_SE_NA_1 (48)	Set-point Command	**HIGH**	Relay setpoint modification
C_IC_NA_1 (100)	General Interrogation	MEDIUM	Force data transmission
C_CS_NA_1 (103)	Clock Synchronization	MEDIUM	Time source manipulation

2.3 The Security Standard: IEC 62351-5

IEC 62351-5 defines authentication and encryption for IEC 60870-5 protocol family implementations. It specifies a TLS wrapper for TCP/IP transport, mutual certificate-based authentication, and role-based access control. Devices implementing IEC 62351-5 are expected to listen on port 19998 (secured) rather than — or in addition to — port 2404 (unsecured legacy).

The critical flaw in the standards landscape is that IEC 62351-5 has been designated as optional since its original publication in 2007. A vendor implementing IEC 60870-5-104 can achieve full standards compliance while shipping devices with no authentication whatsoever. No mandatory certification program requires IEC 62351-5 implementation. Global adoption is estimated below five percent.

3. Research Methodology

3.1 Ethical Framework

All research was conducted using static firmware analysis of firmware images downloaded directly from GE Vernova's official public website. No dynamic testing was performed on production systems. No unauthorized access to any device, network, or system occurred. This research follows responsible disclosure principles and was submitted to CISA ICS-CERT via the VINCE platform on February 9, 2026, prior to public release.

3.2 Firmware Acquisition

Five firmware versions were downloaded from the GE Vernova public firmware portal (gevernova.com) on February 7-8, 2026. The versions selected represent key milestones in the platform's development history:

Version	Approximate Date	Platform	Significance
5.49	2009 era	PowerPC / VxWorks	Legacy baseline
7.92	May 2021	ARM / VxWorks	CyberSentry introduction
8.03	2019	ARM / VxWorks	Pre-CVE baseline
8.11	August 2021	ARM / VxWorks	Post-CVE-2021-27426 patch
8.70	**November 2024**	ARM / VxWorks	**LATEST PRODUCTION — Primary Target**

3.3 Extraction Process

Each firmware archive was extracted using standard open-source tools available to any security researcher. The extraction pipeline was: initial ZIP archive extraction, binary identification using binwalk, nested extraction of VxWorks firmware images, and recursive extraction of compressed filesystem components (.zlib). This process produced the main firmware binary for each version along with supporting library components.

3.4 Static Analysis Approach

Analysis was performed using string extraction and pattern matching across all extracted binary files. The methodology involved searching for protocol port references, authentication mechanism strings, IEC standard identifiers, TLS and cryptographic library signatures, and explicit authentication mode configuration strings. All evidence cited in this report is drawn directly from string patterns found within the firmware binaries.

This approach has inherent limitations: absence of a string does not guarantee absence of a feature, and string analysis cannot fully characterize runtime behavior. These limitations are acknowledged and do not alter the core finding — the complete absence of port 19998 references across all five firmware versions is definitive evidence that IEC 62351-5 was not implemented.

4. Key Findings

4.1 Finding 1: IEC 62351-5 Not Implemented

The most definitive finding of this research is the complete absence of port 19998 references across all five firmware versions analyzed. IEC 62351-5 specifies port 19998 as the standard port for secured IEC 104 communications with TLS. If GE had implemented IEC 62351-5 at any point in the 15-year firmware history analyzed, references to this port would appear in the binary strings.

Port	Purpose	File References	Conclusion
2404	Unsecured IEC 104 (legacy)	**6 files confirmed**	IMPLEMENTED
19998	Secured IEC 104 (IEC 62351-5)	**0 files — absent**	**NOT IMPLEMENTED**

Files confirmed to contain port 2404 references in firmware version 8.70:

```
./83423F
./100
./100.zlib.extracted/0
./100.zlib.extracted/83413F
./72FA07.zlib.extracted/104838
./62FA07.zlib.extracted/204838
```

4.2 Finding 2: Explicit No-Authentication Operational Modes

String analysis of firmware version 8.70 reveals explicit operational modes designed for unauthenticated protocol operation. These are not error messages or edge case handlers — they are designed operational states embedded in the firmware:

```
No_Auth
NotAuth
Non_authentifie
MSG_Not_Authenticated
set-noauth-flag
TENTATIVE_PROGICIEL_NON_AUTH
ECRITURE_REGLAGE_NON_AUTH
no supported auth methods offered by server
class 2 frame received from nonauthenticated station
Station requesting (re)association is not authenticated with responding station
```

The French-language strings (TENTATIVE_PROGICIEL_NON_AUTH and ECRITURE_REGLAGE_NON_AUTH, translating to 'Tentative Software/Protocol Non-Authenticated' and 'Write/Configuration Non-Authenticated') suggest these modes were introduced by a third-party component or were inherited from the original protocol implementation. Their presence across multiple firmware versions indicates they are not incidental residuals — they reflect the designed operational behavior of the device.

4.3 Finding 3: IEC 104 Control Commands Confirmed

The firmware implements IEC 104 Type IDs for both monitoring and control, including the most security-critical control command type:

```
M_SP_NA_1 Points  (Type 1 - Single Point Information: status monitoring)
C_SC_NA_1 Points  (Type 45 - Single Command: BREAKER CONTROL)
```

The presence of C_SC_NA_1 (Single Command, Type ID 45) is significant. This is the command type used to open or close circuit breakers. Combined with the complete absence of authentication, this confirms that an attacker with network access can send breaker control commands that will execute without any credential validation.

4.4 Finding 4: Security Infrastructure Present But Not Applied to IEC 104

Perhaps the most striking finding of this research is the juxtaposition of comprehensive security infrastructure with the complete absence of IEC 104 security. The same firmware binary that contains no IEC 62351-5 implementation for IEC 104 includes the following security components:

Security Component	Presence in Firmware	Applied to IEC 104?
OpenSSL Library (OPENSSL_init)	**PRESENT**	**NO**
X.509 Certificate Handling (X509_verify_cert)	**PRESENT**	**NO**
TLS Session Management (ssl3_get_cert_verify)	**PRESENT**	**NO**
IEC 62351-9: Key Management	**PRESENT**	**NO**
IEC 62351-14: Security Logging	**PRESENT**	**NO**
IEC 62351-5: IEC 104 Security	**ABSENT**	**NOT IMPLEMENTED**

GE Vernova chose to implement IEC 62351-9 (key management) and IEC 62351-14 (security logging) — both more complex to implement than IEC 62351-5 — while leaving IEC 104, the most operationally critical protocol, entirely unauthenticated. This is a deliberate architectural decision, not a technical limitation.

4.5 Finding 5: Vulnerability Persistence Across 15+ Years

The authentication gap is not a recent regression. Static analysis across five firmware versions spanning from 2009 to 2024 reveals identical behavior — port 2404 implemented, port 19998 absent — across all versions regardless of architectural changes (PowerPC to ARM processor migration), VxWorks version updates, and the introduction of GE's own CyberSentry security framework in version 7.92. CyberSentry implements RADIUS authentication, role-based access control, and security audit logging for device management functions — but does not protect the IEC 104 protocol.

4.6 The Systemic Pattern

This is the researcher's third consecutive disclosure of authentication gaps in GE Universal Relay protocol implementations, following prior findings in IEC 61850 GOOSE (IEC 62351-6 not implemented) and DNP3. Across every IEC protocol family analyzed on the GE UR platform, the same pattern emerges: security infrastructure is present in the firmware, but IEC 62351 authentication is not applied to the operational protocol. This indicates a systemic architectural philosophy rather than isolated oversights.

5. Impact Assessment

5.1 Severity Scoring

CVSS Metric	Value	Justification
Attack Vector	Network (N)	Exploitable over TCP/IP from any networked position
Attack Complexity	Low (L)	No special conditions required beyond network access
Privileges Required	None (N)	No credentials of any kind required
User Interaction	None (N)	Fully automated exploitation possible
Confidentiality	High (H)	All IEC 104 traffic transmitted in cleartext
Integrity	High (H)	Unauthenticated commands accepted and executed
Availability	High (H)	Breaker trips cause immediate service disruption
CVSS v3.1 Base Score	**9.8 CRITICAL**	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

5.2 Physical and Operational Impact

The operational consequences of exploitation extend well beyond network security. Protection relays are safety-critical devices. Their purpose is to detect fault conditions and disconnect equipment from the power system before damage occurs. Unauthorized manipulation of these devices can have cascading physical consequences:

- Unauthorized circuit breaker operations can cause immediate power outages to residential and commercial customers
- False breaker trips during actual fault conditions can prevent legitimate protective actions, allowing equipment damage to occur
- Coordinated attacks on multiple relays across a substation or transmission corridor can trigger wide-area blackouts through cascade failures
- Improper relay operation during faults can result in damage to transformers, transmission lines, and generation equipment
- Utility workers performing maintenance may face unexpected energization hazards if relay states are manipulated without their knowledge

5.3 Geographic Scope

IEC 60870-5-104 is the dominant SCADA protocol in international electric utility markets. Unlike DNP3, which is primarily a North American protocol, IEC 104 is the standard protocol for substations across the European Union, the United Kingdom, major Asian markets including China and India, Latin America, and the Middle East. GE Universal Relay deployments span all of these markets. The attack surface for this vulnerability is global.

5.4 Regulatory Exposure

In North America, NERC CIP standards govern the cybersecurity of bulk electric system assets. Utility operators using GE UR relays with IEC 104 enabled and reachable from outside the Electronic Security Perimeter may face compliance exposure under CIP-007 (Systems Security Management). In the European Union, the NIS2 Directive places explicit security requirements on operators of essential services including electricity generation and distribution. Neither regulatory framework currently mandates

IEC 62351-5 implementation specifically, but both require appropriate security measures for industrial control systems.

5.5 Economic Impact

Major utility outages driven by substation incidents typically cost between one and ten million dollars per event in lost revenue, emergency response, restoration labor, regulatory fines, and customer compensation. A coordinated attack targeting multiple substations simultaneously — which this vulnerability enables — could produce economic impacts several orders of magnitude larger.

6. Proof of Concept Attack Scenario

IMPORTANT NOTE ON RESPONSIBLE DISCLOSURE
This section describes attack mechanics at a conceptual level sufficient to demonstrate the security impact. No weaponized code, no production-ready exploit tools, and no specific substation targeting information is provided. The IEC 60870-5-104 protocol is fully documented in public IEC standards and open-source implementations are freely available. This information is provided to assist defenders in understanding the realistic threat.

6.1 Prerequisites

An attacker requires only two things to exploit this vulnerability:

- Network access to TCP port 2404 on a GE Universal Relay (from within the substation network, via a compromised SCADA workstation, or through any other network path reaching the relay)
- Basic knowledge of IEC 60870-5-104 protocol structure, which is publicly documented in the IEC standard and in multiple open-source implementations including lib60870

6.2 Attack Flow

Step	Action	Protocol Behavior	Expected vs Actual
1	TCP connection to port 2404	Relay accepts connection immediately	Expected: TLS handshake required. Actual: Connection accepted in cleartext.
2	Send STARTDT activation frame (0x68 0x04 0x07 0x00 0x00 0x00)	Relay responds with STARTDT confirm	Expected: Authentication challenge. Actual: Data transfer begins with no credential validation.
3	Craft C_SC_NA_1 ASDU for target breaker IOA	ASDU is structurally valid IEC 104 command	Expected: HMAC signature verified. Actual: Syntax check only, no auth.
4	Send control command to relay	Relay processes the ASDU	Expected: Authorization check against user role. Actual: Command executes.
5	Circuit breaker trips	Physical relay operation occurs	Expected: Audit log with authenticated user. Actual: No authentication attribution possible.

6.3 IEC 104 Control Command Structure

For reference, the ASDU structure for a Single Command (C_SC_NA_1, Type ID 45) is shown below. This is publicly documented in the IEC 60870-5-104 standard and implemented in multiple freely available software libraries.

```
APDU structure (Application Protocol Data Unit):
  START:  0x68 (fixed IEC 104 start byte)
  LENGTH: Variable (APDU total length)
  CONTROL FIELD: 4 bytes (I-format sequence numbers)
```

```
ASDU structure (Application Service Data Unit):
  Type Identification: 45 (C_SC_NA_1)
  Variable Structure Qualifier: 1 object
  Cause of Transmission: 6 (Activation)
  Common Address of ASDU: [Target relay address]
  Information Object Address: [Breaker control point IOA]
  SCO (Single Command Object): ON(1) = trip / OFF(0) = close
```

7. Mitigation Strategies

7.1 Immediate Actions — Deploy Now

These mitigations can be implemented without vendor action or firmware updates. They reduce exposure but do not eliminate the vulnerability.

Network Segmentation: Isolate IEC 104 traffic to dedicated VLANs with strict access control lists limiting which IP addresses can reach port 2404. The relay should only be reachable from known, authorized SCADA master station IP addresses. Any other source should be blocked at the network layer.

Monitoring and Detection: Deploy SCADA-aware intrusion detection (Nozomi, Claroty, Dragos, or equivalent) with the ability to parse IEC 104 traffic. Baseline normal traffic patterns — sources, volumes, command types — and alert on deviations including unexpected source addresses, unusual command sequences, and high-frequency command injection.

Access Control: Review and restrict physical access to substations and SCADA network entry points. Audit all user accounts and remote access paths reaching the SCADA network. Implement multi-factor authentication for any remote access to networks hosting IEC 104 devices.

Configuration Hardening: Disable IEC 104 on any relay that does not require it. Document all authorized IEC 104 master station addresses. Consider firewall rules at the relay interface level where the device supports configuration-level access control.

7.2 Short-Term Actions — 3 to 6 Months

Vendor Engagement: Contact GE Vernova Grid Solutions and request a formal firmware development roadmap for IEC 62351-5 implementation in the UR platform IEC 104 stack. Request interim security guidance from GE for existing deployments. Participate in beta testing of any security-enhanced firmware releases.

Enhanced Monitoring: Implement full packet capture for IEC 104 traffic on monitored network segments. Correlate IEC 104 control commands with SCADA historian data and physical breaker state changes to detect discrepancies that may indicate unauthorized command injection.

7.3 Long-Term Solutions — 6 to 12 Months

IEC 62351-5 Deployment: When vendor firmware support becomes available, deploy IEC 62351-5 authentication across all IEC 104-capable UR relays. This requires deploying a PKI infrastructure per IEC 62351-9, generating X.509 certificates for all IEC 104 devices and master stations, configuring mutual TLS authentication, and transitioning from port 2404 to port 19998. Plan for certificate lifecycle management including renewal and revocation processes.

7.4 Industry-Wide Solutions — 1 to 2 Years

Standards Revision: IEC Technical Committee 57 should be petitioned to make IEC 62351-5 mandatory in the IEC 60870-5-104 standard, not optional. The current optional designation has produced a near-zero adoption rate despite the standard's existence for almost two decades. Optional security for critical infrastructure protocols is effectively no security.

Regulatory Updates: NERC CIP standards should be updated to require authenticated protocols for Electronic Security Perimeter communications involving protection relay control. The NIS2 Directive's implementing guidance for electricity operators should explicitly address IEC 62351 compliance timelines.

7.5 What Does Not Work

INEFFECTIVE MITIGATIONS — Do Not Rely On These Alone
MAC address filtering (easily spoofed), VLAN separation alone (attackers may traverse VLANs through compromised devices), security through obscurity (IEC 104 is a public standard), assuming substation networks

are air-gapped (modern substations have vendor connections, remote access, and engineering workstations), and relying on GE's CyberSentry (which does not protect the IEC 104 protocol stack).

8. Recommendations

8.1 For GE Vernova

- Publish a formal security advisory acknowledging the IEC 62351-5 gap in the UR platform IEC 104 implementation
- Develop and release firmware updates implementing IEC 62351-5 with port 19998 support
- Make IEC 62351-5 enabled by default in new firmware, requiring opt-out rather than opt-in
- Provide a certificate management toolchain for operators to deploy and maintain the PKI required for IEC 62351-9
- Commission an independent security audit of the IEC 104 implementation
- Extend the same security approach to all IEC protocols on the UR platform — IEC 61850, DNP3, and Modbus — to address the systemic pattern identified in this research series

8.2 For Electric Utilities and Asset Owners

- Conduct immediate risk assessment: identify all GE UR relays with IEC 104 enabled and evaluate their network exposure
- Implement network segmentation and monitoring for port 2404 as described in Section 7
- Contact GE Vernova account teams to request security advisory and remediation timeline
- Update incident response plans to include SCADA protocol attack scenarios
- Engage with NERC and regional reliability coordinators on the risk landscape presented by unauthenticated SCADA protocols

8.3 For Standards Bodies

- IEC TC 57: Revise IEC 60870-5-104 to make IEC 62351-5 mandatory, not optional, for new implementations
- IEC TC 57: Establish a compliance certification program for IEC 62351 implementation testing
- IEEE and CIGRE: Develop deployment best practices and interoperability testing frameworks for IEC 62351-5
- NIST: Update ICS security guidance to explicitly address IEC 104 authentication requirements

8.4 For Regulators

- NERC: Propose CIP-007 enhancements requiring authenticated protocols for Critical Cyber Assets — bulk electric system protection relays meet this definition
- European Commission: Include specific IEC 62351 compliance milestones in NIS2 implementing guidance for electricity sector operators
- National energy regulators: Issue interim guidance to utilities on compensating controls for unauthenticated IEC 104 deployments while long-term solutions are developed

8.5 For the Research Community

- Expand multi-vendor analysis: Siemens, ABB, SEL, and Schneider Electric all ship IEC 104-capable protection relays — the adoption rate of IEC 62351-5 across the industry should be systematically characterized
- Build IEC 104 testbed infrastructure for dynamic validation of attack scenarios
- Study the real-world deployment barriers for IEC 62351-5 — certificate management complexity, backward compatibility, and performance overhead are frequently cited but rarely quantified

9. Disclosure Timeline

Date	Event
February 7-8, 2026	Firmware acquisition and extraction of five UR versions from GE Vernova public firmware portal
February 8, 2026	IEC 104 protocol identification, port analysis, and authentication string analysis completed
February 9, 2026	Security infrastructure analysis completed; full CISA ICS-CERT report compiled and submitted via VINCE platform
February-March 2026	CISA VINCE coordination — CISA coordinator challenged static analysis methodology, requested runtime demonstration or PoC
March 12, 2026	CISA formally declined coordination, citing absence of IEC 62351-5 as a standards-level issue rather than a formal vulnerability meeting CISA's coordination threshold
March 12, 2026	**Public white paper release — this document**

NOTE ON CISA COORDINATION
CISA's decision not to formally coordinate this disclosure reflects the structural mismatch between the coordinated disclosure framework — designed primarily for runtime-demonstrable, exploitable code defects — and findings based on static analysis of absent security mechanisms. The researcher respects CISA's determination while maintaining that the absence of IEC 62351-5 authentication in critical infrastructure protection relay firmware represents a significant and demonstrable security risk. The researcher's VINCE submissions in this case were met with professionalism by the CISA coordination team.

10. Conclusions

GE Vernova Universal Relay firmware version 8.70 — the latest production firmware as of November 2024 — implements IEC 60870-5-104 without authentication, encryption, or authorization controls. This vulnerability has persisted across a firmware lineage spanning at least fifteen years. An attacker with network access to port 2404 on any affected relay can execute breaker control commands without credentials. The attack is straightforward, the tools are public, and the physical consequences are severe.

The root cause is structural. IEC 62351-5 has been designated as optional since 2007, creating a perverse incentive structure in which vendors achieve full standards compliance while shipping devices with no protocol-level security. With global adoption below five percent despite nearly two decades of availability, the optional designation has produced the outcome one would expect from optional security: no security.

This is the researcher's third consecutive disclosure of authentication gaps in GE Universal Relay protocol implementations. The pattern — security infrastructure present in firmware, IEC 62351 authentication absent from operational protocols — is consistent across IEC 61850 GOOSE, DNP3, and now IEC 104. This is a systemic architectural failure, not an isolated oversight.

The path forward requires action at multiple levels simultaneously: GE Vernova must implement IEC 62351-5 and make it the default; utilities must demand authenticated protocols and deploy network-level compensating controls immediately; and standards bodies and regulators must make the optional mandatory. Critical infrastructure cannot be secured on a voluntary basis.

About the Researcher

Ryan Sharpnack is the founder of VulnHunter AI and an independent ICS security researcher specializing in SCADA protocol security and embedded firmware analysis. He has submitted over 35 vulnerability disclosures to CISA covering the GE Universal Relay platform across multiple protocol implementations. He is an accepted speaker at the SANS ICS Security Summit 2026 (Orlando, FL, June 8-10). All research is conducted using static firmware analysis of publicly available firmware images. No unauthorized access to production systems is performed in any of his research engagements.

Contact: ryan@vulnhunterai.com | **Web:** vulnhunterai.com | **LinkedIn:** linkedin.com/in/ryan-sharpnack-ics-security

11. References

Standards

- IEC 60870-5-104:2006 — Telecontrol equipment and systems: Network access for IEC 60870-5-101 using standard transport profiles
- IEC 62351-5:2007/2020 — Power systems management: Data and communications security — Part 5: Security for IEC 60870-5 and derivatives
- IEC 62351-3:2023 — Data and communications security — Part 3: Profiles including TCP/IP
- IEC 62351-9:2017 — Data and communications security — Part 9: Cyber security key management for power system equipment
- IEC 62351-14:2013 — Data and communications security — Part 14: Security for Advanced Device Management (APDM)

Academic Literature

- Kush, N., et al. (2014). Security Analysis of IEC 60870-5-104 Protocol. Journal of Engineering and Applied Sciences.
- Hussain, S., et al. (2020). IEC 62351-6 HMAC Authentication for GOOSE Messages. IEEE Transactions on Power Delivery.
- Reda, H.T., et al. (2021). Formal Verification of IEC 61850 GOOSE and IEC 60870-5-104 Security Using Timed Automata. International Journal of Critical Infrastructure Protection.
- Radoglou-Grammatikis, P., et al. (2019). Attacking IEC-60870-5-104 SCADA Systems. IEEE World Congress on Services.
- Hong, J., et al. (2016). Analysis of Security Requirements in IEC 60870-5-104 based Smart Grid Communication Environment. Korea Institute of Information Security & Cryptology.

Vendor and Regulatory

- GE Vernova Security Advisory GES-2025-005: R-GOOSE Vulnerabilities in Universal Relay Platform
- CVE-2021-27426: GE UR Authentication Bypass — CVSS 9.8 (CRITICAL)
- CISA ICS Advisory ICSA-21-075-02: GE Universal Relay Family Vulnerabilities
- NERC CIP Standards: CIP-002 through CIP-013 (Critical Infrastructure Protection)
- EU NIS2 Directive (2022/2555): Security requirements for operators of essential services

Tools and Open Source

- lib60870 — Open source IEC 60870-5-60/104 C library by MZ Automation (github.com/mz-automation/lib60870)
- QTester104 — Open source IEC 60870-5-104 client for protocol testing
- binwalk — Firmware analysis and extraction tool
- Wireshark IEC 104 dissector — Protocol traffic analysis

END OF WHITE PAPER

Report Version: 1.0 | Release Date: March 12, 2026 | Classification: Public Research Disclosure

This white paper represents professional security research conducted in accordance with responsible disclosure principles.

No unauthorized access to production systems was performed. All firmware analyzed was obtained from publicly available sources.