SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I12P104

Volume 11 Issue 12, 36-52, December 2024

Original Article

Cybersecurity and IEC 62351 for SCADA Systems of Power Grid

V. Shivakumar[1,3], M.B. Veena[2,3]

[1]*Smart Grid Research Laboratory, Central Power Research Institute, Karnataka, India.*
[2]*Department of Electronics & Communication Engineering, BMS College of Engineering, Karnataka, India.*
[3]*Visvesvaraya Technological University, Karnataka, India.*

[1]*Corresponding Author : shiva@cpri.in*

Received: 03 October 2024 Revised: 04 November 2024 Accepted: 02 December 2024 Published: 31 December 2024

Abstract *- As Information and Communication Technology (ICT) brought automation and improved the efficiency and performance of electric power supply systems from generation to end utilization of electricity by consumers, it has also increased the chances of cyber attacks and threats. However, automation is inevitable, and it is required to take care of the prevention, detection and mitigation of cyber threats and make the grid resilient. Globally, work is happening in this direction, especially in the last decade, as more and smarter grid systems are being deployed, which involves extensive use of ICT and automation of grid operation. The national and international standards organizations are also working towards developing standards for making the grid resilient to cyber threats. The International Electrotechnical Commission (IEC) is one of the important standardization organizations that brought out a series of IEC 62351 standards (IEC 62351:2024 SER Power systems management and associated information exchange - Data and communications security - ALL PARTS) for data and communication security for power system operation. In this paper how the IEC 62351 series of standards could be applied to the SCADA systems in making the grid resilient to cyber threats with more focus emphasized on the Remote Terminal Unit (RTU) communication with the SCADA control centre of the Power system operation has been explained. Also, laboratory testing of RTUs for conformance to IEC 62351 standards and its results are discussed. The laboratory testing of sample RTUs shows that many of the manufacturer's implementations differ from the standard specifications. Deployment of RTUs not following the IEC 62351 specifications in the field may lead to security threats such as man-in-the-middle attacks.*

Keywords *- Critical Infrastructure Security, Cyber Security, RTUs, SCADA systems, Smart grids, Standards.*

1. Introduction

The modern power supply system is a complex network consisting of not only electrical infrastructure but also information technology infrastructure connected with all the domains of the power system, namely generation, transmission, distribution, markets, operation, service provider and customers through the communication system.

The communication technology includes both utility-owned and third-party communication service provider networks and has connectivity between the Operational Technology (OT) network like Supervisory Control and Data Acquisition System (SCADA) / Energy Management System (EMS) / Distribution Management System (DMS) / digital substations and with that of utility's enterprise's network Information Technology (IT) for operational simplicity with a thin air gap or almost a converged system of OT & IT. Hence, vulnerability to cyber-attacks on the OT system increases, thus making utility engineers address this new requirement of preventing cyber security attacks and threats and handling the situations of cyber incidents. Due to this, power engineers also require basic expertise in cyber security and best practices knowledge of associated standards and consciousness of security threats/vulnerability [1, 2]. In the dynamic landscape of the 21st century, the power sector stands as a foundational pillar of modern civilization, invisibly powering houses, industries, and critical infrastructure.

Amid the complex processes of the power supply system, the power sector not only fuels societies but also emerges as a prime target for malicious attacks in this digital age. The integration of digital technologies and the expansive interconnectivity of the power grid has created a vulnerable attack surface, demanding a proactive approach to address potential threats that could disrupt the flow of electricity and the consumers, impacting the economy, public safety and the environment. To minimize the risks due to cyber threats and incidents, it is essential to see how the fundamental requirements or objectives of cyber security, namely 'Availability', 'Integrity' and 'Confidentiality', have been

implemented in the OT and IT systems, including the equipment/components used in the utility automation and control systems.

Today's power supply system consists of three different layers, viz., the electrical network infrastructure, the telecommunication infrastructure and the operational control center and energy market. The exchange of information occurs between the electrical network infrastructures, control centers, and energy market through the telecommunications layer. This requires a secured communication system to protect against any cyber threats that may cause damage to the system or life or environment or interruption in the supply of electricity to consumers or all of the above.

The field devices installed in electrical substations utilize a variety of communication protocols, which must be robust and secure. Since the Stuxnet incident at an Iranian nuclear plant in 2010, cyber security has become one of the important subjects in the power sector. The reporting of cyber incidents on Ukraine's electricity distribution system during the years 2015 and 2016 proved that cyber incidents could lead to severe consequences apart from electricity supply interruptions [3]. Especially during the coronavirus pandemic and post-pandemic, the amount of cyber incidents increased in critical infrastructure, including the power sector.

Cyber Security is a continuous process involving People, Processes and Technology, and all these components are crucial and need to be treated as a system and not as discrete components for providing the best protection against cyber security threats. Thus, cybersecurity requirements need to be addressed at all four levels, forming the cyber security ring as described:

1. Manufacturer/vendor security certifications (product development Process and Technology).
2. Individual product/component level security conformance certifications (Technology).
3. Asset owners like Electricity generation/transmission/distribution/utility service provider/load dispatch centre/electricity market/energy exchange security certifications (Process and policy) and
4. Engineer / authorized personnel handling critical infrastructure operations certifications (or training) (People).

The cyber security ring concept can also be considered as a defense in depth protection. Figure 1 shows how Cyber Security Ring provides defense in depth kind of protection from the perspective of testing phases of SCADA system implementation. The concept of cyber security shall start from the product (hardware or software or embedded system including firmware) design phase itself (secure product development process and then to the product security conformance phase). Once the product moves out for the deployment phase, it is important to see how the product is installed in the networked system in the field and the network architecture robustness from the perspective of cyber security without compromising the power system requirements like latency and bandwidth [4].

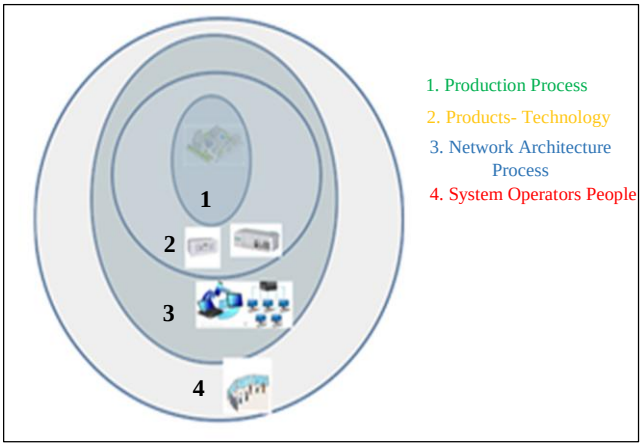

Fig. 1 Defense in-depth - testing process at various stages for cyber Security

Ultimately, the power system operator who will be accessing the system and product through the networked system for the day-to-day operation of the power system and his / her awareness of cyber security best practices plays a vital role in minimizing the cyber risk and attacks even though the product and network architecture are designed for best cyber security protection [5].

In this paper, a comprehensive study of test requirements and test results of the second quadrant of security ring, i.e. products/devices security conformance testing and certifications, are described. This second quadrant also becomes part of Supply Chain Risk Management (SCRM), wherein product testing for cyber security is one of the requirements. The authors of the reference paper [6] discuss various methods of risk assessment methods for SCADA systems, including ISO / IEC 27005: 2011 Information technology–Security Techniques–Information Security Risk Management. The IEC 62443 - The Security for Industrial Automation and Control Systems - Part 4-2: Technical security requirements for Industrial Automation and Control Systems (IACS) components standard describes security requirements for the products.

The IEC 62351 series of standards provides technical guidance for the implementation and testing of products for security requirements. The RTU, which is one of the important components/elements in the electric utility automation system, and the laboratory testing experience for cyber security requirements as per IEC 62351 standards are discussed in this paper. The International Electrotechnical Commission (IEC) has published a series of IEC 62351 standards to address the cyber security requirements for the

RTUs and Intelligent Electronic Devices (IED), which are predominately used electric power substations for automation and control. Though these standards were published a long time ago, implementation of same in these devices by manufacturers was not uniform, and there were no standard test procedures. Only during the years 2018 and 2020 IEC published test procedure standards. However, third-party testing tools were available in the open market, and the samples tested were very limited. The test requirements increased as the power sector work scenario changed during the Covid pandemic, forcing some of the power system automation works to be handled remotely and using personal devices like smartphones and laptops to access operational technology equipment like RTUs and IEDs.

As the subject evolves, the IEC has also initiated the revision of a few standards under the IEC 62351 series. As the interpretation of standards differs among the manufacturers, the implementations are also varying. To overcome this issue and provide feedback to the standardizing organization, a good number of samples (in this case (RTU) are to be tested as per standards, and the outcome of test results needs to be analyzed. This paper focuses on these issues and attempts to consolidate the test results for further studies.

This paper is organized into different sections. Section 2 introduces a brief description of the RTU communication protocol, which, in this case, is the IEC 60870-5-104 protocol. Section 3 briefly discusses the security objectives and attacks. Section 4 introduces the IEC 62351 series of standards in general and in particular IEC 62351-3 (Part 3: Communication network and system security - Profiles including TCP/IP) and IEC 62351-5 (Part 5: Security for IEC 60870-5 and derivatives) which specify security requirements for IEC 60870-5-104 communication protocol. Section 5 describes laboratory conformance testing of RTUs for security requirements with a few sample test cases. Section 6 discusses the analysis of laboratory test results, and section 7 concludes with a summary.

2. IEC 60870-5-104 Communication Protocol

2.1. RTU Connection in Field

RTU will be used in substation and feeder level automation to collect the status of isolators, circuit breakers and other status signals and also analog measurement values like the voltage, current, power, energy consumption, PF, etc., of feeders for processing by SCADA Control Centre for energy management and distribution management functions. Apart from RTU, it also controls isolators, circuit breakers, transformer tap changers and other control activities from the control centre commands.

Figure 2 shows a typical RTU connected in the substation. The RTU will have the required number of digital inputs and outputs, Analog inputs and outputs, serial communication interface (RS 232 / RS 485) for analog measurement parameters in Modbus or in other protocols, and USB or Ethernet port for configuring RTU apart from Ethernet port for communicating to control centre through a network router and switch combinations. The router will be connected to a service provider broadband network or utility-owned private network using various communication mediums like fibre optic, wireless (RF Radio network), satellite or copper wired system.

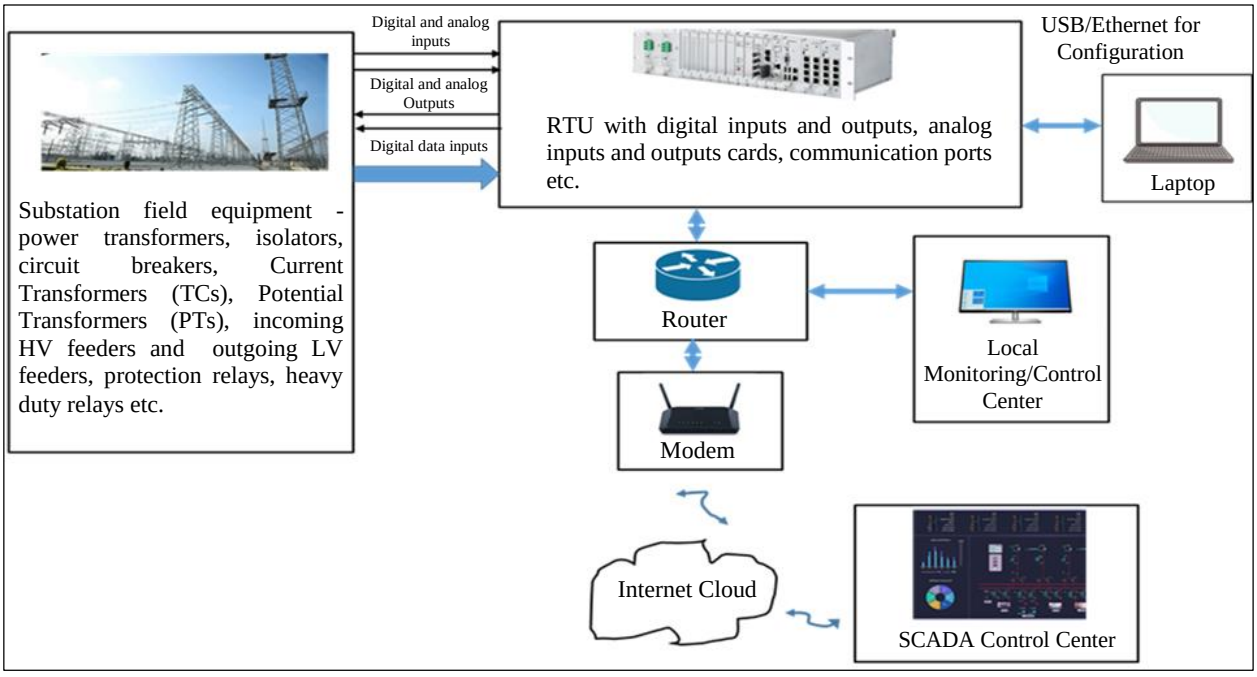

Fig. 2 Typical block diagram of RTU connection in Substation

Power Line Carrier Communication (PLCC) was also used in older systems, but it is now not being used because of bandwidth limitations, latency, and connectivity limitations on the LV network due to noise. It can be noted from Figure 2 that if anyone intervenes in the communication network and is able to gain access to the RTUs, the complete electric network of the substation can be controlled or alter the various status and measurement values used for power system operation, and it can lead to outages and puts in risk for life, environment or economy or all of these. If RTUs are designed to protect from cyber security risks, even if network-level intrusion happens, a second layer of protection can prevent or minimize the risk due to cyber threats, as RTU will have its own access control and authentication requirements apart from data encryption.

2.2. Protocol Structure

While communication systems make smart grids viable, they also expose vulnerabilities to cyber-attacks. The power sector faces multifaceted vulnerabilities, including interconnected systems, reliance on legacy infrastructure, remote operations, supply chain risks and the human element. These factors make the sector an attractive target for cyber attackers, posing risks to both economic stability and public safety. The power sector's significance as a critical infrastructure cannot be overstated; playing a vital role in economic growth, public health, safety, and national security. The expanding attack surface due to increased reliance on digital technologies necessitates robust cyber security measures. Types of cyber-attacks could include phishing attacks, ransomware, Distributed Denial of Service (DDoS), Internet of Things (IoT) vulnerabilities, and zero-day exploits. In power sector applications, instances like Cyber-attacks on RTUs / Feeder / Field RTUs (FRTUs) have serious consequences, including the disruption of operations, compromise of data and the potential for physical damage to the equipment and life. The first step in device compliance requirements against cyber threats is the proper implementation of communication protocols and access control through password, authentication, encryption and digital key management. The proper implementation of the above minimizes the risks against cyber threats. IEC has developed a series of standards known as IEC 60870-5-xxx for telecontrol equipment and systems. These standards specify communication protocols to ensure interoperability among the various makes of devices or products used in the utility SCADA and automation systems.

The IEC developed standards for communication protocols for SCADA and utility automation during 1995-2000, the period during which cyber security in the power sector was not a subject since closed communication systems like PLCC or private communication systems are not connected to the outside of utility communication system. The SCADA and automation system facilitate data exchanges, including control between the substations / generating stations and control centres/load dispatch centres. The IEC has developed standard IEC 60870-5-101 for serial communication-based systems and IEC 60870-5-104 for TCP/IP-based network systems, and in this paper, the latter is being discussed. The use of IEC 60870-5-101-based systems is diminishing due to the advantages of TCP / IP systems. Like most embedded systems, the IEC 60870-5 protocol uses three layers of the 7-layer ISO OSI model, namely the application layer, link layer and physical layer. The IEC 104 protocol frame is known as the Application Protocol Data Unit (APDU) and contains the Application Protocol Control Information (APCI) and Application Service Data Unit (ASDU). For control purposes, only APDU without ASDU is transmitted. Start or stop bits for ASDUs are not used, as IEC 60870-5-104 uses a TCP interface. A start character (0x68) is included for each APCI, along with the length of the ASDU and the control field, as shown in Figure 3, to detect the start and end of the ASDUs.

The length of the APDU body is determined by the APDU length byte. The APDU includes the four control field octets of the APCI and the ASDU. The first octet counted is the initial octet of the control field, and the last counted octet is the final octet of the ASDU. Since the maximum value for the APDU length field is 253 and the control field length is 4 octets, the maximum ASDU length is 249 octets (APDU max = 255 minus start and length octets). The packets can be of a fixed length (without ASDU) or with a variable length with ASDU. There are three types of frame formats decided by the last two bits of the first Control Field (CF1).

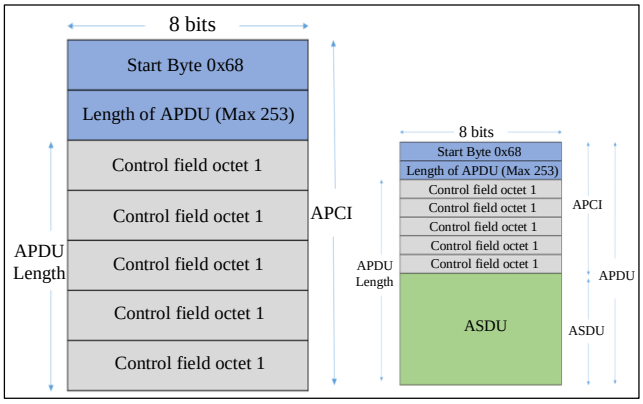

Fig. 3 APDU frame format

I - Format (Information Transfer Format), the Last Bit of CF1 is 0.

- This format is used for transferring numbered information between controlled and controlling stations, and its length is variable.
- I format APDU always contains ASDU.
- Message direction is indicated by Control fields of I-formats. Two 15-bit sequence numbers are used, and they will be sequentially increased by one for each APDU and in each direction.

- The Right interpretation of sequence numbers is determined by using the position of Least Significant Bit (LSB) and Most Significant Bit (MSB). Thus, 15 bits form the length of sequence numbers of I-format.

S - Format (Numbered Supervisory Functions), Last Bits of CF1 are 01.

- These fixed-length bits are used to perform numbered supervisory functions.
- S-format APDUs always consist of one APCI only.
- Before a timeout occurs, a buffer overflows, or the maximum number of allowed I-format APDUs is exceeded without acknowledgement; in cases of unidirectional data transfer, S-format APDUs must be sent in the opposite direction for acknowledgement.

U-Format (Unnumbered Control Functions), the Last Bits of CF2 are 11.

- These fixed-length bits are used to perform unnumbered control functions.
- U-format APDUs consist solely of one APCI. At any given time, only one function-TESTFR (Test Frame), STOPDT (Stop Data Transfer), or STARTDT (Start Data Transfer)-can be active. U-format is used for the activation and confirmation mechanism of STARTDT, STOPDT and TESTFR.
- STARTDT and STOPDT are used by the controlling station to control the data transfer from a controlled station.
- Checking the status of all established connections to detect any communication problems as soon as possible is done by the controlling and/or controlled station. This is done by sending TESTFR frames.

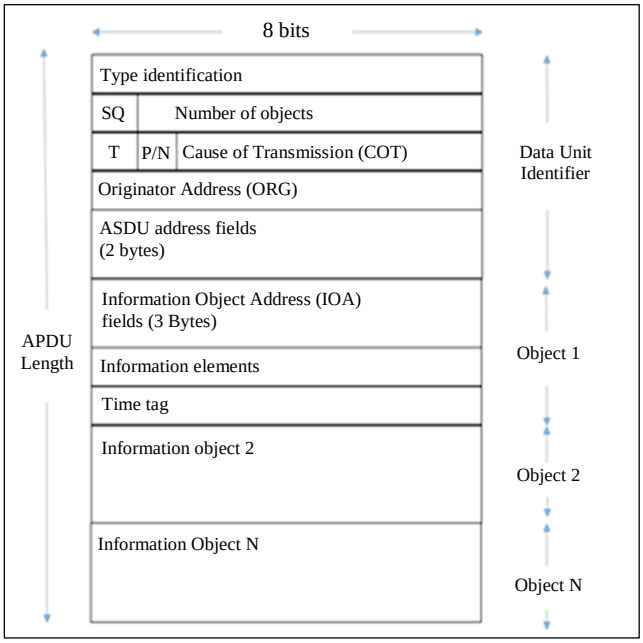

Fig. 4 ASDU format

2.2.1. SDU Format

The ASDU is composed of two primary parts: a data unit identifier that has a length of six bytes and the data itself, which consists of information objects of atleast one or more. The specific type of data is determined by the data unit identifier, which addresses and pinpoints the precise identity of the data and comprises additional details, such as the Cause of Transmission (COT). Each ASDU can transmit a maximum of 127 objects. The format of ASDU is shown in Figure 4. More details of various fields of ASDU are given in [7, 8].

3. Security Objectives and Attacks

3.1. Cyberattacks

As seen from the discussions in section 1, more and more automation with open communications systems also brings cyber threats and attacks. These cyberattacks on the SCADA system of the power system could be deliberate or inadvertent. The deliberate threats could be due to disgruntled employees, industrial espionage, vandalism, or cyber hackers, whereas inadvertent threats may be due to safety failures, design faults, equipment failures, carelessness or natural disasters. The common threats to SCADA systems are briefed below.

The cyber-attack could be due to a compromised computer connected to the OT network or due to movable physical media usage like USB in the OT network systems. The compromised computer may come to the OT network due to the use of physical media or through the network (OT or IT) due to poor network configuration or improper protection to the network like improper firewall policy or not following properly the cyber security policy or due to zero-day attack (vulnerability in the supplied systems/applications by vendors) [9].

3.2. Cyber Security Objectives

In any cyber security (OT or IT), it is important that how confidentiality (C), integrity (I) and availability (I) are implemented at the device level as well as at the system level, which forms the foundational pillar in minimizing cyber security attacks & threats and incidents. The CIA triad is shown in Figure 5, and the same is briefly explained below to help understand how cyber security measures could be implemented [10].

3.2.1. Availability

Unlike in the IT system, Availability is the first and foremost priority element of the CIA cyber security triad in the OT system/power system SCADA [11]. Availability refers to preventing denial of service and ensuring authorized access to information. The operator is an integral part of the OT / SCADA system, and timely non-availability of the system, i.e. denial of access to the system, makes him / her delay in getting required information or taking action, which may impact the power system operation. As a part of availability, authorization is also one of the key elements. Authorization refers to permission for whom access to the system and

information is granted. The authorization could be for the operator for the device itself or for both, and this will be achieved using login information to access the human-machine interface and interact with the system or between devices.

3.2.2. Integrity

Integrity involves protecting information from unauthorized modification or theft. The information made available to the operator or the intended user/device shall be genuine and the same as it originated from the source; otherwise, it will impact the decision, resulting in loss of money or lives or, environmental contamination or all of these.

3.2.3. Confidentiality

Confidentiality refers to preventing the unauthorized access to information. However, in OT, this aspect has the least priority, and it is necessary to prevent the availability of information to unauthorized users to safeguard the safety of the system.

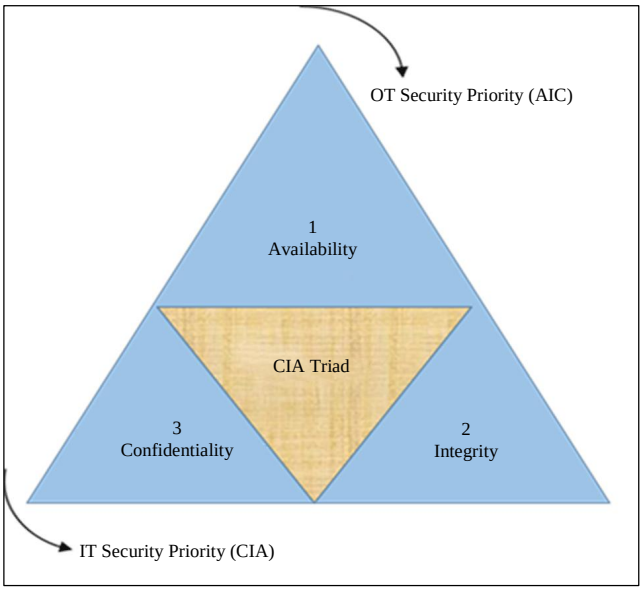

Fig. 5 CIA triad

Over and above, the following are also the objectives of cyber security.

Non-Repudiation

Non-repudiation, or accountability, ensures that an individual cannot deny an action that occurred or claim an action that did not take place. In certain scenarios, like where the source device can't be identified, then this is when the receiver should immediately discard the message.

Replay Protection

Another important security objective, though it is not considered a part of the triad, is necessary to have protection against replay messages. The replay attacks could be like sending messages multiple times by an adversary that was already sent. As a result, this can greatly exhaust the receiver's computational resources by requiring the same task to be executed multiple times, thus bringing the system down.

4. Applying IEC 62351 Standard for IEC 60870-5-104

As IEC 60870, a series of standard-based telemetering protocols were developed for communication between the field devices and control centre, assuming no security threats since these networks were closed networks and not exposed to global internet connections (obscurity). Security aspects like authentication, encryption and other security functionalities were not implemented in these protocols [12-18].

However, due to the emergence of the smart grid and the expectation of more functionalities in the automation systems for improving the operational efficiency of the electricity supply chain system, i.e. from generation, transmission, and distribution to end consumers, it became inevitable to adopt the new technologies, including TCP / IP based communication system, cloud-based systems and third party communication services providers network for utility communication (data, voice and video (e.g. substations CCTV images / live stream)).

Since this makes Operational Technology (OT) be interfaced with the business network (or Information Technology (IT)) of utility, which almost converges or leaves a thin air gap, the OT network needs to take all the measures to protect from cyber security threats. IEC developed a series of IEC 62351 standards which specify procedures and algorithms for securing the operation of IEC protocols, including how to provide confidentiality, integrity protection, and message level authentication for SCADA and telecontrol protocols [19-23].

In this paper, laboratory testing for the conformance of the application of IEC 62351 standards for the RTUs based on protocol IEC 60870-5-104 and analysis of the results of the testing have been discussed. The IEC 62351 series of standards includes multiple parts, and most of them are published, and others are in the various stages of publication. For the works related to the security of the IEC 60870-5-104 protocol, the IEC 62351-3 and IEC 62351-5 describe the implementation aspects of security measures.

The IEC 62351-100-1 (Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 (Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)) and IEC 62351-100-3 (Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP) specify the test procedures.

4.1. IEC 62351-3

IEC 62351-3 outlines the methods for ensuring confidentiality, integrity, and message-level authentication for SCADA and telecontrol protocols used by devices such as Remote Terminal Units (RTUs) that employ TCP/IP as a transport layer to implement cybersecurity measures. The Operational Technology (OT) environment, compared to Information Technology (IT) applications, has distinct operational requirements despite utilizing TLS for security purposes. A critical difference lies in the duration of TCP/IP connections that require security maintenance; OT environments often demand long-term, or even "permanent," connections, in contrast to the short-duration connections typically used in IT protocols, which allow for encryption algorithms to be renegotiated during connection re-establishment.

In power systems management and related information exchange, longer-duration connections are common, necessitating special considerations. Specifically, OT environments require protection for these “permanent” connections, making it essential to implement a mechanism for updating session keys. This standard addresses this requirement by leveraging TLS features such as session resumption and session renegotiation while also accounting for the relationship with certificate revocation state information. To ensure interoperability, the standard mandates at least one common cipher suite and a set of TLS parameters to facilitate compatibility across different systems.

This part of the IEC standard covers security and TCP / IP requirements only for the communication transport layers (OSI layers 4 and lower) [19]. The threats considered in IEC 62351 - 3 for the transport layers are listed below:

- Modification of messages or insertion of messages through message-level authentication to provide integrity protection of messages.
- To ensure confidentiality protection, message-level encryption of messages is used to counter unauthorized access or leakage of information.

By implementing the required specifications and recommendations of IEC 62351 – 3, the following security attack can be mitigated.

- Man-in-the-middle: By using the Message Authentication Code (MAC) mechanism specified within this standard, a man-in-the-middle attack can be mitigated.
- Replay: By using specialized processing state machines, the ‘Replay’ attack could be avoided.
- Eavesdropping: This threat is countered through the use of encryption.

The performance evaluation of the device (RTU) claiming conformance to this standard was tested and studied. Selected test cases based on the laboratory testing of RTU for conformance to IEC 62351-3 and IEC 62351-5 are explained in the subsequent sections.

4.2. IEC 62351-5

The IEC 62351 standard outlines messages, procedures, and algorithms designed to enhance the security of protocols defined in other IEC 60870-5 series standards, focusing specifically on application layer authentication and associated security challenges. This paper centers on the IEC 60870-5-104 protocol. The IEC 62351 series standard encompasses security requirements for both IEC 60870-5-101 (serial communication) and IEC 60870-5-104 (TCP/IP-based communication) protocols. It specifies application layer authentication to safeguard against spoofing, replay attacks, message modification, and, to some extent, Denial-of-Service (DoS) attacks.

However, since the standard does not include encryption measures, it does not offer protection against eavesdropping, traffic analysis, or repudiation. The security framework is based on the Challenge-Handshake Protocol Authentication, with the Hashed Message Authentication Code (HMAC) employed to ensure source authentication and message integrity. Figure 6 shows how the packet structure appears after applying IEC 62351-3 and IEC 62351-5 to the IEC 60870-5-104 protocol.

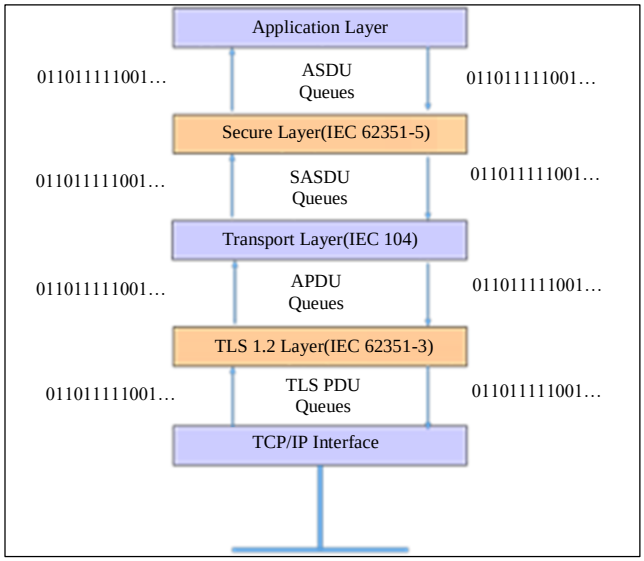

Fig. 6 Applying IEC 62351 to IEC 104 protocol

5. Conformance Testing

The initial step in ensuring device compliance with cyber threat requirements involves the correct implementation of communication protocols, access controls via passwords, authentication mechanisms, encryption methods, and digital key management. Effective implementation of these measures significantly reduces the risk of cyber threats. The test setup is illustrated in Figures 7(a), while Figure 7(b) provides a visual

of the laboratory setup with the test sample. The test environment comprises the following components:

- Device under Test (DUT): In this case, it is a Remote Terminal Unit (RTU) utilizing the IEC 60870-5-104 protocol.
- DNV UniGrid Telecontrol test tool software: A protocol simulator test system functioning as a single-node controlling station. Additionally, the DNV UniGrid Telecontrol 104 Analyser test tool software is employed as a protocol test analyzer.
- Ethernet switching hub.
- Ethernet connection between the test system and DUT.

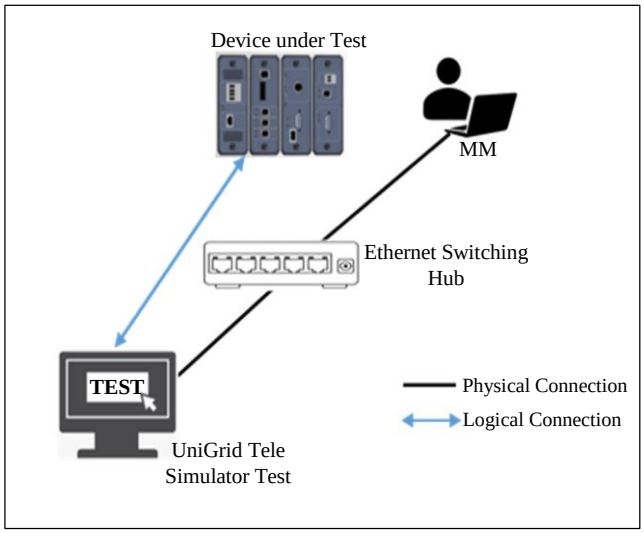

Fig. 7(a) Laboratory test setup

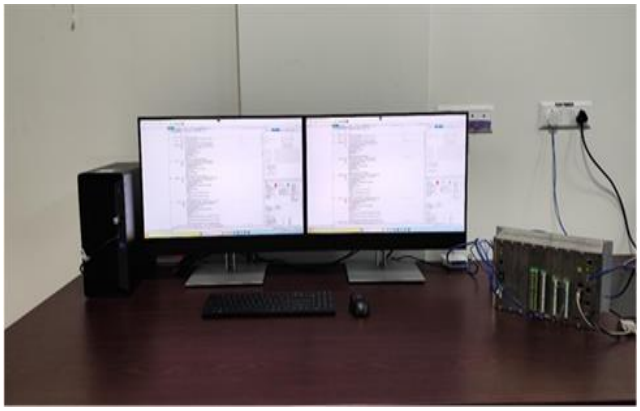

Fig. 7(b) Laboratory test setup photo

Before commencing testing, the DUT shall be configured and the general requirements of DUT for testing are as follows.

- The DUT should display the values of Information Elements as specified in the I/O list and map them to visible Man-Machine Interface (MMI) elements.
- The communication should be manually paused or frozen to verify the displayed or analyzed data.
- Manually shut down and restart or equivalent.
- Manually cut-off the connection to the communication link.
- The supported Basic Application Functions are to be activated manually.
- Direct physical connection is to be established with the communication link.

The DUT and Test System must be configured with appropriate IP addresses. The RTU manufacturer is responsible for providing the Protocol Implementation Conformance Statement (PICS), which serves as the foundation for the relevant test cases as outlined in the standard.

The DUT should be capable of independently enabling the profile for IEC 62351-3 and/or IEC 62351-5. After configuring the RTU and Test tool, test cases are executed, and logs are recorded automatically. The test tool is semiautomatic, and it requires manual analysis of logs with reference to IEC 62351-100-1 and IEC 62351-100-3 to decide whether the RTU is confirming the requirements as specified in these standards.

5.1. IEC 62351-3 and IEC 62351-5 Test Cases

Figure 7 shows the execution of the single point command, which is used to operate the circuit breaker in the electric substation. Figure 8(a) shows the single command from the Master (Tool) and the response from the slave (RTU). These packets start from 68H. From Figure 8(b) and 8(c), it can be seen from the logs of Wireshark that the complete packet structure is visible as the security extension as per IEC 62351-3 is not activated.

Similarly, Figures 9(a), 9(b) and 9(c) shows the execution of a single command with security extension enabled. It can be seen in Figure 8 that the single point command packet from Master (Tool) and Slave (RTU) are based on the MAC calculation, which authorized only User 1 (in this test case) to execute the commands. Also, if we see the same packets in the Wireshark, it shows the encrypted data as the security extension as per IEC 62351-3 encrypts these packets based on the selected cipher suites while the same packet is visible in Master (Tool), which have the private key for decryption.

Similar to above, packet analysis for the Time Synchronization command is also shown in Figures 10 (without security enabled) and 11 (with security enabled). Figure 12 shows the DNV UniGrid Telecontrol Test tool software Graphical User Interface (GUI). Before commencing the test, the configuration parameters of RTU, as well as the other parameters from the Protocol Implementation Conformance Statements (PICS) document of RTU, need to be configured in the test tool.

>M 3	17:43:55:147	APDU	0000: 68 0E 00 00 00 00 2D 01 : 06 00 E1 2E 0A 00 00 01
		APCI	L=14 Information Frame, Send Sequence Nr: 0, Receive Sequence Nr: 0
		ASDU	<45> single command
			SQ=0 Number of elements=1
			Cause of transmission: <6> activation
			Originator address: 0
			Common address: 12001: Bla
			IOA=10
			Single command state (SCO) : (SCS=<1> ON QU=<0> no additional definition S/E: execute)
<S 4	17:43:55:163	APDU	0000: 68 0E 00 00 02 00 2D 01 : 07 00 E1 2E 0A 00 00 01
		APCI	L=14 Information Frame, Send Sequence Nr: 0, Receive Sequence Nr: 1
		ASDU	<45> single command
			SQ=0 Number of elements=1
			Cause of transmission: <7> activation confirmation
			Originator address: 0
			Common address: 12001: Bla
			IOA=10
			Single command state (SCO) : (SCS=<1> ON QU=<0> no additional definition S/E: execute)

Fig. 8(a) Single point command without security enabled (log from test tool)

Fig. 8(b) Single point command without security enabled (Tool log from Wireshark)

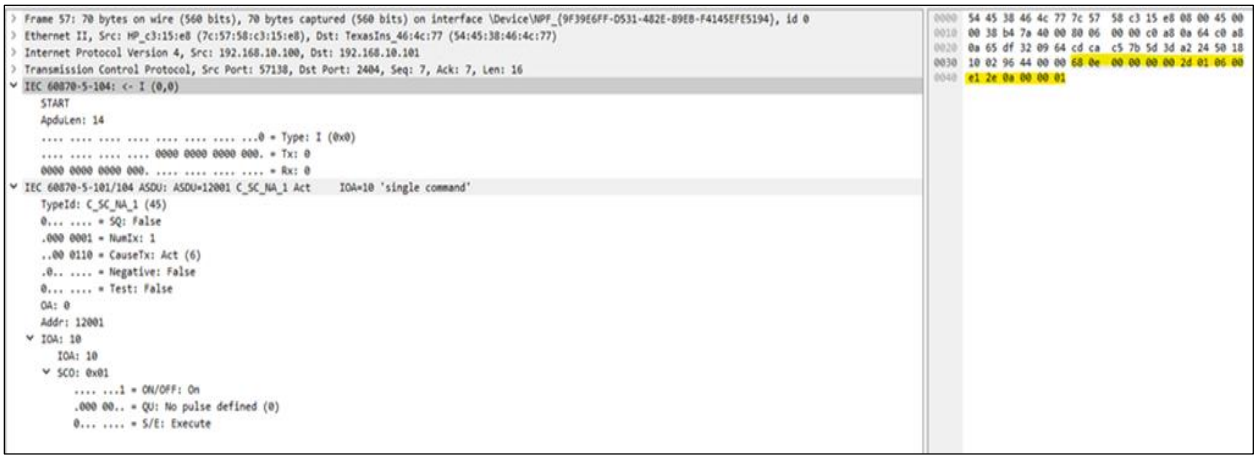

Fig. 8(c) Single point command without security enabled (RTU log from Wireshark)

>M 46	10:07:41:075	APDU	0000: 68 2B 0E 00 3E 00 53 01 : 0E 00 E1 2E C0 2D 01 06 : 00 E1 2E 0A 00 00 01 03 : 00 00 00 01 00 B9 35 67
			0020: 60 3B 23 72 BD 7C 08 29 : 9D F7 4F 13 D9
		APCI	L=43 Information Frame, Send Sequence Nr: 7, Receive Sequence Nr: 31
		ASDU	<83> Aggressive mode authentication request
			SQ=0 Number of elements=1
			Cause of transmission: <14> authentication
			Originator address: 0
			Common address: 12001: Bla
			ASDU Segmentation Control (ASC): FIN=<1> Final segment FIR=<1> First segment ASN=0
			Segmented data: 2D010600E12E0A000001
			<45> single command
			SQ=0 Number of elements=1
			Cause of transmission: <6> activation
			Originator address: 0
			Common address: 12001: Bla
			IOA=10
			Single command state (SCO) : (SCS=<1> ON QU=<0> no additional definition S/E: execute)
			Challenge sequence number (CSQ): 3
			User number (USR): <1> Default
			MAC value (HLN): B93567603B2372BD7C08299DF74F13D9
<S 47	10:07:41:091	APDU	0000: 68 2B 3E 00 10 00 53 01 : 0E 00 E1 2E C1 2D 01 07 : 00 E1 2E 0A 00 00 01 03 : 00 00 00 01 00 D1 E5 32
			0020: 70 B8 D9 33 9C ED E1 46 : 69 7B B5 E4 D9
		APCI	L=43 Information Frame, Send Sequence Nr: 31, Receive Sequence Nr: 8
		ASDU	<83> Aggressive mode authentication request
			SQ=0 Number of elements=1
			Cause of transmission: <14> authentication
			Originator address: 0
			Common address: 12001: Bla
			ASDU Segmentation Control (ASC): FIN=<1> Final segment FIR=<1> First segment ASN=1
			Segmented data: 2D010700E12E0A000001
			<45> single command
			SQ=0 Number of elements=1
			Cause of transmission: <7> activation confirmation
			Originator address: 0
			Common address: 12001: Bla
			IOA=10
			Single command state (SCO) : (SCS=<1> ON QU=<0> no additional definition S/E: execute)
			Challenge sequence number (CSQ): 3
			User number (USR): <1> Default
			MAC value (HLN): D1E53270B8D9339CEDE146697BB5E4D9

Fig. 9(a) Single point command with security enabled (log from the tool)

Fig. 9(b) Single point command with security enabled (Tool log from Wireshark)

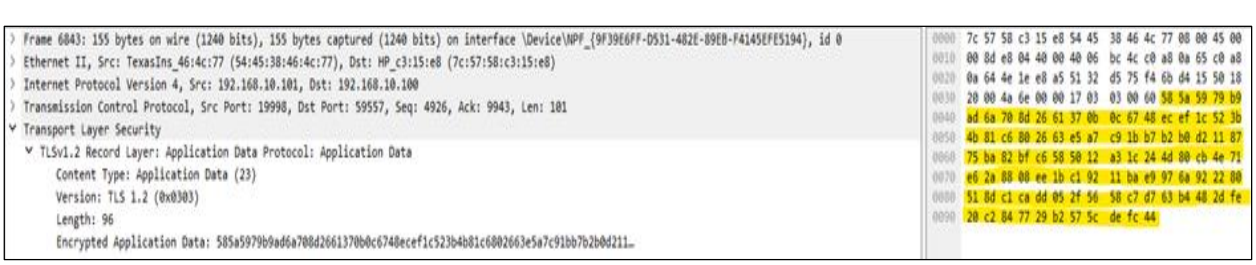

Fig. 9(c) Single point command with security enabled (RTU log from Wireshark)

>M 3	15:09:01:298	APDU	0000: 68 14 00 00 00 00 67 01 : 06 00 E1 2E 00 00 00 F3 : 04 09 0F 9C 09 17
		APCI	L=20 Information Frame, Send Sequence Nr: 0, Receive Sequence Nr: 0
		ASDU	<103> clock synchronisation command
			SQ=0 Number of elements=1
			Cause of transmission: <6> activation
			Originator address: 0
			Common address: 12001: Bla
			IOA=0
			Time: <0> valid, <0> winter/not used, Thursday 28-09-2023 15:09:01.267
<S 4	15:09:01:313	APDU	0000: 68 14 00 00 02 00 67 01 : 07 00 E1 2E 00 00 00 CB : 04 89 0F 1C 09 17
		APCI	L=20 Information Frame, Send Sequence Nr: 0, Receive Sequence Nr: 1
		ASDU	<103> clock synchronisation command
			SQ=0 Number of elements=1
			Cause of transmission: <7> activation confirmation
			Originator address: 0
			Common address: 12001: Bla
			IOA=0
			Time: <1> invalid, <0> winter/not used, Day of week: <0> not used 28-09-2023 15:09:01.227

Fig. 10(a) Time synch command without security enabled (log from tool)

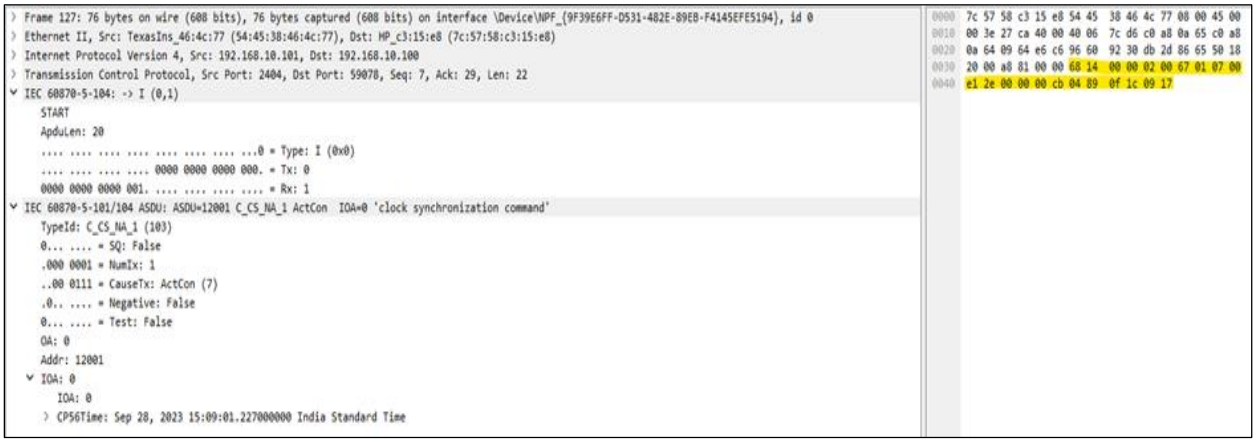

Fig. 10(b) Time Synch command without security enabled (tool log from Wireshark)

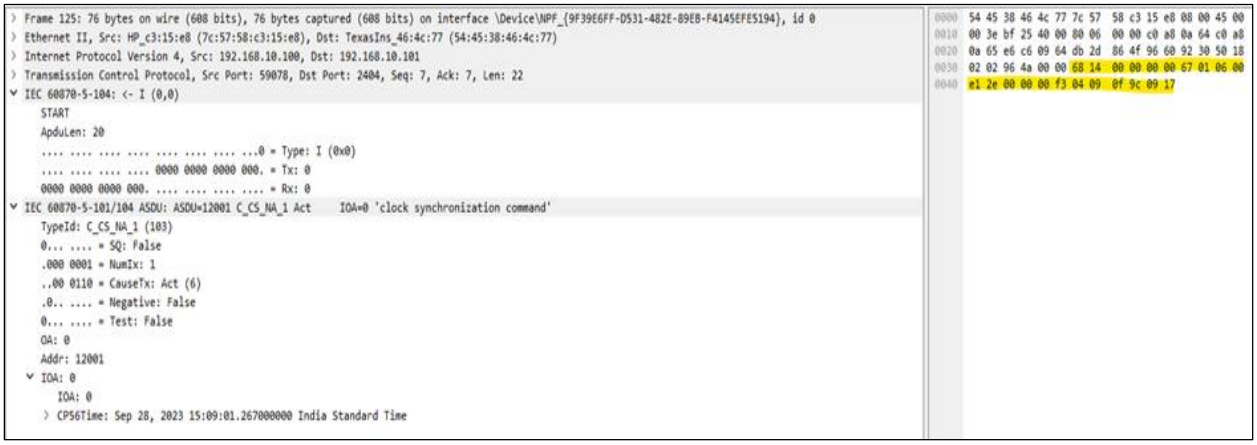

Fig. 10(c) Time synch command without security enabled (RTU log from Wireshark)

>M 13	16:11:32:865	APDU	0000: 68 31 0A 00 0A 00 53 01 : 0E 00 E1 2E C0 67 01 06 : 00 E1 2E 00 00 00 4D 80 : 0B 10 67 02 18 09 00 00
			0020: 00 01 00 7B B2 E0 A1 56 : C1 2C 05 8B 0F A7 AC 28 : 3A 7E 89
		APCI	L=49 Information Frame, Send Sequence Nr: 5, Receive Sequence Nr: 5
		ASDU	<83> Aggressive mode authentication request
			SQ=0 Number of elements=1
			Cause of transmission: <14> authentication
			Originator address: 0
			Common address: 12001: Bla
			ASDU Segmentation Control (ASC): FIN=<1> Final segment FIR=<1> First segment ASN=0
			Segmented data: 67010600E12E0000004D800B10670218
			<103> clock synchronisation command
			SQ=0 Number of elements=1
			Cause of transmission: <6> activation
			Originator address: 0
			Common address: 12001: Bla
			IOA=0
			Time: <0> valid, <0> winter/not used, Wednesday 07-02-2024 16:11:32.845
			Challenge sequence number (CSQ): 9
			User number (USR): <1> Default
			MAC value (HLN): 7BB2E0A156C12C058B0FA7AC283A7E89
<S 14	16:11:32:880	APDU	0000: 68 31 0A 00 0C 00 53 01 : 0E 00 E1 2E C1 67 01 07 : 00 E1 2E 00 00 00 8D 21 : B5 0E 07 02 18 09 00 00
			0020: 00 01 00 29 57 BE DE E5 : 81 2A DB 88 7A EE 93 D2 : C5 D0 69
		APCI	L=49 Information Frame, Send Sequence Nr: 5, Receive Sequence Nr: 6
		ASDU	<83> Aggressive mode authentication request
			SQ=0 Number of elements=1
			Cause of transmission: <14> authentication
			Originator address: 0
			Common address: 12001: Bla
			ASDU Segmentation Control (ASC): FIN=<1> Final segment FIR=<1> First segment ASN=1
			Segmented data: 67010700E12E0000008D21B50E070218
			<103> clock synchronisation command
			SQ=0 Number of elements=1
			Cause of transmission: <7> activation confirmation
			Originator address: 0
			Common address: 12001: Bla
			IOA=0
			Time: <1> invalid, <0> winter/not used, Day of week: <0> not used 07-02-2024 14:53:08.589
			Challenge sequence number (CSQ): 9
			User number (USR): <1> Default
			MAC value (HLN): 2957BEDEE5812ADB887AEE93D2C5D069

Fig. 11(a) Time Synch command with security enabled (log from tool)

Fig. 11(b) Time Synch command with security enabled (tool log from Wireshark)

Fig. 11(c) Time Synch command with security enabled (RTU log from Wireshark)

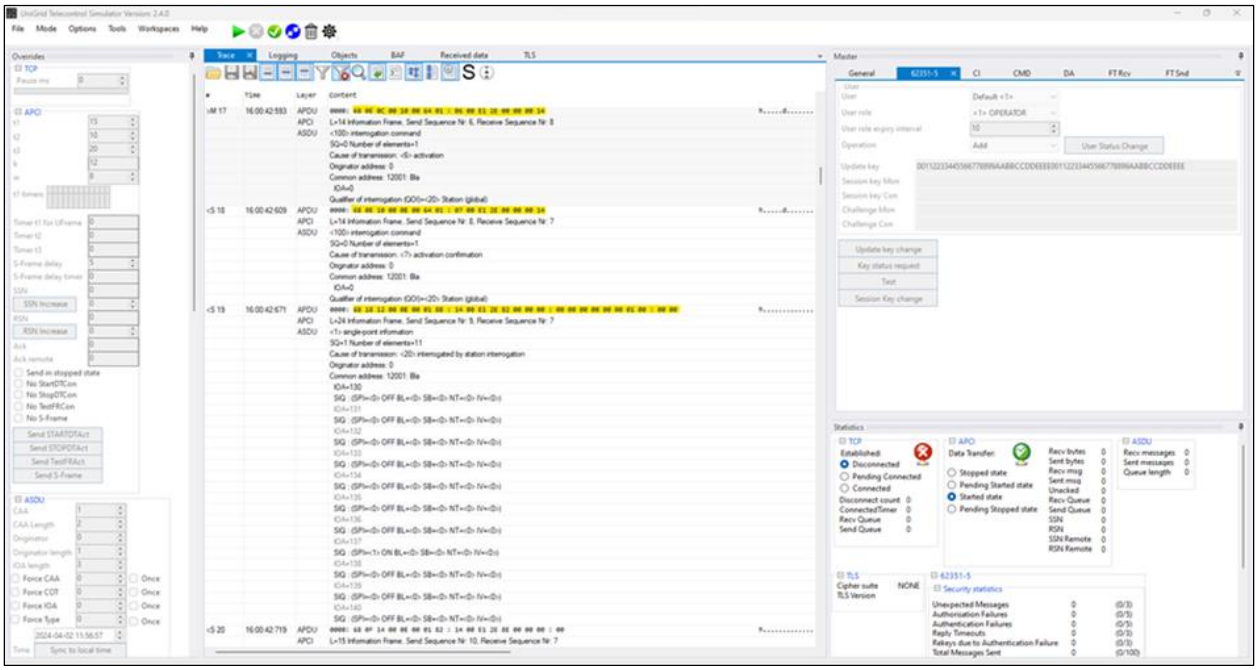

Fig. 12 Test tool GUI

6. Test Results Analysis

From the analysis of packets as explained in the previous section, after activation of security extension as per IEC 62351-3, the flow of packets between RTU and SCADA cannot be visualized from outside as it needs the private key to decrypt these packets. Also, with the activation of IEC 62351-5, unauthorized users cannot execute the commands as it requires the MAC calculation, which is configured only for authorized users.

Implementing Information Security Management System (ISMS) as per ISO / IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements standard for power utilities provides only first line of control for cyber safe operation, but many more sector-specific controls and testing of products and systems for cyber security requirements are essential. Primary electrical equipment, such as circuit breakers, are interconnected through field devices like Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), and other devices to enable control and automation of power system operations.

As RTUs, IEDs and field devices control power system operation and also exchange data (control, events, measurements and other information) between these devices and the SCADA / Control system software and Human Machine Interface (HMI) application software, these devices need to comply with the security requirements for ensuring cyber safe operation. IEC TC 57 Working Group 15 (Data and Communication Security) has developed various standards under the IEC 62351 series [18]. These standards provide specifications for implementing security requirements like authentication, encryption, role-based access, key management, and other aspects of standard communication protocols used in power system operation and conformance testing. In laboratory testing, the test procedures as defined in these standards are followed to conclude whether the DUT complies with the standard or not.

The conformance testing for base protocol in this case (IEC 60870-5-104) shall be performed before performing the security extension conformance testing as per IEC 62351-100-1: 2018 Power systems management and associated information exchange – Data and communications security - Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 The conformance testing does not include application logic and operational test system and only tests for protocol elements and functions as per the protocol implementation document provided by the manufacturer. The conformance test cases are grouped into ‘Verification of Configuration parameters’, ‘Verification of Communication’ ‘and ‘Verification of Procedures’. Verification of Configuration parameters ensures that protocol implementation is consistent with the change in configuration parameters.

Verification of the communication test clause and sub-clauses ensures that the device under test can meet the implementation of test security extension messages as per IEC 60870-5-7 standard, which cross-references the IEC 62351 series of standards. Verification of Procedures clauses establishes that the device undergoing testing could execute the security extensions procedures as per IEC 62351-5

standard. The security extension procedures conformance testing is grouped into User management, Update key maintenance, Session key maintenance, Challenge/reply authentication and Aggressive Mode Authentication. These procedures are executed in sequence.

The 'IEC 62351-100-3: 2020 Conformance test procedures are also grouped into 'Verification of configuration parameters' and 'Verification of IEC 62351-3 requirements'. Similar to IEC 62351-100-1, the clauses under verification of configuration parameters ensure that protocol implementation is consistent with the change in configuration parameters. 'Verification of configuration parameters' includes testing for 11 sub-clauses as per IEC 62351-100-3. These clauses include the Transport Layer Security (TLS) version, TLS Cipher suites, Public key lengths, certification revocation check methods and other parameters as per standard. Verifying IEC 62351-3 requirements ensures that the device under testing conforms to the requirements of IEC 62351-3, which includes how the device would behave during normal execution of procedures and when a fault or abnormal procedures execution is encountered, i.e. resiliency or negative test cases.

During the laboratory testing for conformance of RTUs of various makes, it was noticed that a few implementations were different from the standards. Table 1 lists a few test cases performed on three different makes of samples. From Table 1, it may be noted how implementation differs from manufacturer to manufacturer. The table lists selected test cases of failure resulting in non-compliance with the standard. Three sample RTUs, A, B and C, from different manufacturers, are considered in the study. The Sl. No. 2 is one of the test cases in which two manufacturers (A & B) implemented the standard requirement (IEC 62351-5 and IEC 62351-100-1) in different ways, and both failed as it is not as per the standard requirement.

The Key Challenge Data Length (KCL) and Key Status Challenge Data (KCD) shall be zero if the Key Status (KST) is not equal to one. But in both cases, KST is not equal to one. In spite of that, DUT reported that KCL was equal to some numerical value. Furthermore, sample a reported KCL equal to four while the minimum requirement is between 8 and 64. This leads to the conclusion that some of the standards statements require refining as interpretations of standards are different among the different manufacturers, and there is also a detailed study of standards by manufacturers.

The criteria for the testing for conformance is that the DUT shall provide the expected output in the form of messages as defined in the IEC 62351-100-1 and IEC 62351-100-3. The technical working group is also addressing these issues. The challenge is that cyber security technology is rapidly changing and making it difficult to bring revision/amendments to all the relevant parts of standards in the series, which are interlinked to each other at the same time. Many of these standards from the IEC 62351 series have been published in recent years, and only limited manufacturers have implemented these standards requirements in the devices. Additionally, it is not reported in the literature on third-party testing for security conformance. Also, commercial test tools for security conformance as per IEC standards are limited in the market. Only laboratory tests not for conformance testing of actual devices are reported in [24, 25].

The cyber security subject in the power sector has been gaining momentum since the global pandemic hit the world in 2020, and the situation forced the power system operators to relook into security aspects. Further distributed energy resources like solar and wind energy-based generation systems are also adding to the capacity in large numbers and are interconnected with the load dispatch operation from isolated places, thus increasing the cyber threat landscape. These all call for robust testing of field devices for security conformance and implementation of security policy and security auditing [26-28].

7. Conclusion

From the samples of RTUs of different manufacturers tested at a laboratory for conformance of IEC 62351-100-1 and IEC 62351-100-3, it is observed that implementations of security requirements as specified in IEC 62351-3 and IEC 62351-5 were differing among the manufacturers and some RTUs eventually failed to meet the standard requirements for some of the test cases. In this paper, an attempt is made to study the implementation of IEC 62351 standards in RTU by various manufacturers, and it helps the standardizing bodies in bringing amendments/revisions to standards for uniform understanding and also for manufacturers in better understanding of standards. As this subject of cybersecurity is continuously evolving, more samples of different makes and models' conformance testing results further help the industry improve the design of the products.

As technology advances with smart grids, IoT devices, and renewable energy sources are at the forefront and expanding, the power sector must remain vigilant, adapt to emerging threats, and build resilience to any possible cyber-attacks. The security of the power sector is not only a national concern but a global imperative, impacting economic growth, quality of life, technological progress, national security, and the preservation of critical infrastructure. Implementing robust cybersecurity measures is crucial for protecting critical infrastructure.

Key measures include testing products for communication protocols and security conformance as per standards and best practices, such as risk assessment, security policies, network segmentation, access control, patch management, firewalls, encryption, incident response plans, backup and recovery, employee training, regulatory

compliance, continuous monitoring, and security audits to minimize risks due to cyber threats. Laboratory tests help develop secure products and fix bugs before field deployment. Testing for the cyber requirements as per the IEC 62351 series of standards ensures proper implementation of the protocol, encryption, authentication and certificate management / key management, which forms part of defence depth protection for field devices like RTU against attacks on availability, integrity and confidentiality. Also, studies on the impact of cyber incidents and threat model analysis of SCADA control centers can be carried out in the laboratory environment.

This work is planned in the next phase of activities. Testing for devices/products in isolation is only one part of security assessments, and further testing is required as a system when these devices are deployed in the field, as the characteristics for security posture may change due to network architecture even though the device/product meets/exceeds the security requirements as specified in the standards.

Power utilities are inevitable to adopt changing technologies and automation systems to improve operational efficiency and meet regulatory requirements and customer expectations. However, automation systems also bring cybersecurity threats. Utilities can minimize risks due to cyber threats by adopting proper security measures, standards, and best practices.

Cybersecurity is a continuous process. As new technologies are developed, new developments also happen to breach security measures. Hence, standards are evolving as new technologies emerge. Utilities are migrating to cloud-based applications, considering their advantages over on-premises data centers, and must follow the security requirements of cloud-based systems. The future of quantum computing is also expected to bring many changes to conventional security technologies, especially in cryptography.

Acknowledgments

The authors sincerely appreciate the support provided by the management of CPRI for this work and extend their thanks to the management of BMS College of Engineering for their encouragement in pursuing this project. The authors thank the entire SGRL team of CPRI for their support in carrying out laboratory testing experiments. The authors wish to express special thanks to Mr. Shailesh Kapoor, CPRI, for his support in carrying out laboratory testing of sample devices.

References

[1] Teodor Sommestad, Göran N. Ericsson, and Jakob Nordlander, "SCADA System Cyber Security - A Comparison of Standards," *IEEE PES General Meeting*, Minneapolis, MN, USA, pp. 1-8, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[2] Göran N. Ericsson, "Cyber Security and Power System Communication - Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[3] Steve Livingston et al., "Managing Cyber Risk in the Electric Power Sector Emerging Threats to Supply Chain and Industrial Control Systems," *Deloitte Insights*, 2019. [Google Scholar] [Publisher Link]

[4] Darshana Upadhyay, and Srinivas Sampalli, "SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations," *Computer Security*, vol. 89, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] György Dán et al., "Challenges in Power System Information Security," *IEEE Security & Privacy*, vol. 10, no. 4, pp. 62-70, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yulia Cherdantseva et al., "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security*, vol. 56, pp. 1-27, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Matoušek Petr, "*Description and Analysis of IEC 104 Protocol*," Technical Report, Faculty of Information Technology BUT, Brno University of Technology, Czech Republic, 2017. [Google Scholar] [Publisher Link]

[8] International Electrotechnical Commission, *Telecontrol Equipment and Systems - Part 5-104: Transmission Protocols - Network Access for IEC 60870-5-101 Using Standard Transport Profiles*, IEC 60870-5-104:2006+AMD1:2016 CSV Consolidated Version, 2016. [Publisher Link]

[9] Isaac Monroy, "*Security Analysis and Implementation of DNP3 Multilayer Protocol for Secure and Safe Communication in SCADA Systems*," M.S Thesis, Texas University, EI Paso, USA, 2022. [Google Scholar] [Publisher Link]

[10] Dimitrios Pliatsios et al., "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942-1976, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Tim Krause et al., "Cybersecurity in Power Grids: Challenges and Opportunities," *Sensors*, vol. 21, no. 18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Péter György, and Tamás Holczer, "Attacking IEC 60870-5-104 Protocol," *1st Conference on Information Technology and Data Science (CITDS)*, vol. 2874, pp. 140-150, 2020. [Google Scholar] [Publisher Link]

[13] László Erdődi et al., "Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104," *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] János Csatár, Péter György, and Tamás Holczer, "Holistic Attack Methods against Power Systems Using the IEC 60870-5-104 Protocol," *Infocommunications Journal*, vol. 15, no. 3, pp. 42-53, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. Kerkers, "*Assessing the Security of IEC 60870-5-104 Implementations Using Automata Learning*," Master Thesis, University of Twente, 2017. [Google Scholar] [Publisher Link]

[16] Engla Rencelj Ling et al., "Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis," *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Agus Syamsul Arifin et al., "Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol," *2021 International Conference on Technology and Policy in Energy and Electric Power (ICT-PEP)*, Jakarta, Indonesia, pp. 46-51, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Petr Matoušek, Ondřej Ryšavý, and Matěj Grégr, "Increasing Visibility of IEC 104 Communication in the Smart Grid," *6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR)*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] International Electrotechnical Commission, *Power Systems Management and Associated Information Exchange - Data and Communications Security - All Parts*, IEC 62351:2024 SER, IEC 62351 Series, 2024. [Publisher Link]

[20] Anna Volkova et al., "Security Challenges in Control Network Protocols: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 619-639, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] IEC, "*Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment*", International Electrotechnical Commission (IEC), Switzerland, IEC Technology Report, 2019. [Publisher Link]

[22] Frances Cleveland, "IEC TC 57 WG 15: IEC 62351 Security Standards for the Power System Information Infrastructure," 2014. [Google Scholar] [Publisher Link]

[23] Roman Schlegel, Sebastian Obermeier, and Johannes Schneider, "Assessing the Security of IEC 62351" *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, pp. 11-19, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[24] Luis Salazar et al., "Towards a High-Fidelity Network Emulation of IEC 104 SCADA Systems," *CPSIOTSEC 2020 -Proceedings of the 2020 Joint Workshop on CPS & IoT Security and Privacy*, pp. 3-12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Mauro G. Todeschini, and Giovanna Dondossola, "Securing IEC 60870-5-104 Communications Following IEC 62351 Standard: Lab Tests and Results," *2020 AEIT International Annual Conference (AEIT)*, Catania, Italy, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] Rafał Leszczyna, "Standards on Cyber Security Assessment of Smart Grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70-89, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[27] Sukumara T. et al., "Cyber Security - Security Strategy for Distribution Management System and Security Architecture Considerations," *24th International Conference & Exhibition on Electricity Distribution (CIRED)*, vol. 2017, no. 1, pp. 2653-2656, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[28] International Electrotechnical Commission, *Information Technology - Security Techniques - Information Security Management Systems - Information Security Controls for the Energy Utility Industry*, First Edition, ISO / IEC 27019: 2017, 2017. [Publisher Link]

Appendix

Table 1. Laboratory testing on sample RTUs - selected test cases results

SI. No.	Test Case & Standard Reference Number	Test Case Description	Sample A	Sample B	Sample C
1	6.3.3.11 IEC 62351-100-1	KCL: Key Status Challenge Data Length Value range = <8...64>	DUT responds with KCL= 4 during session key status (ASDU 85) while the minimum requirement of KCL = 8.	-	-
2	6.3.3.12 IEC 62351-100-1	KCD: Key Status Challenge Data Sequence of octets of length specified in KCL shall be zero if KST is not equal to one	DUT responds with KCL = 4 with key status challenge data when KST is not equal to one, while the requirement is that key status	DUT responds with KCL = 8 with key status challenge data when KST is not equal to one. Also, KCL = 0 with no key status challenge	-

			challenge data shall be zero when KST is not equal to one.	data when KST is equal to one.	
3	6.3.4.15 - 6.3.4.19 IEC 62351-100-1	DUT shall respond using ASDU 83	DUT does not respond to the Aggressive Mode Authentication Request in Aggressive mode.	-	-
4	5.4.11.1 IEC 60870-5-604	If COT=47 is NOT supported, any message received by the controlled station containing an Undefined IOA should be mirrored with P/N=1 negative.	-	-	DUT doesn't send any response for GI requests with undefined IOA. Also, for File Transfer ASDUs (Controlling Direction), DUT accepts IOA values that are not configured or not applicable.
5	5.4.11.1 IEC 60870-5-604 (With Secure)	If COT=47 is NOT supported, any message received by the controlled station containing an undefined IOA should be mirrored with P/N=1 negative	-	-	DUT doesn't send any response for GI requests with undefined IOA. Also, for File Transfer ASDUs (Controlling Direction), DUT accepts IOA values that are not configured or not applicable.
6	6.3.3.10 IEC 62351-100-1	MAL: MAC Algorithm Values = 0, 3, 4, 6 This value shall be 0 if no valid Session Key Change message was previously received (i.e. if there is no Session Key).	-	DUT responds with MAL = 4 for KST is not equal to one with no MAC data, while MAL shall be zero for KST is not equal to one	-
7	7.5.3.1.4 IEC 62351-100-1	Set Session Key Status to NOT_INIT for that USR	-	DUT does not set the session key status to NOT INIT after exceeding the configured number for the Expected Session Key Change Request.	-
8	7.5.3.2.2 IEC 62351-100-1	Reset Authentication Failures Statistic.	-	DUT does not reset the Authentication Failure Statistic.	-