EUROPEAN UNION AGENCY
FOR CYBERSECURITY

POWER SECTOR DEPENDENCY ON TIME SERVICE

Attacks against time sensitive services

APRIL 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHOR

Dr. Georgios STERGIOPOULOS, Adjunct Lecturer - Researcher, ATHENS UNIV. OF ECONOMICS & BUSINESS

EDITOR

Dr. Konstantinos MOULINOS, Information Security Expert, ENISA

ACKNOWLEDGEMENTS

Keith BUZZARD, IT Risk & Security Officer, ENTSO-E

Dr. Michail MANIATAKOS, Assistant Professor - Electrical and Computer Engineering, NEW YORK UNIVERSITY

Christophe POIRIER-GALMICHE, Cybersecurity expert, ENEDIS

Michael ROTZINGER, SWISSGRID

Michael KNUCHEL, SWISSGRID

Michał SWIEGONSKI, Senior Expert, Polskie Sieci Elektroenergetyczne S.A.

LEGAL NOTICE

ISBN 978-92-9204-344-5, DOI 10.2824/496449

TABLE OF CONTENTS

1. TIME MEASUREMENT TECHNOLOGIES 5

2. POWER SECTOR DEPENDENCY: SCENARIO DESCRIPTION 6

2.1. ARCHITECTURE 6

2.2. RISK OF POTENTIAL ATTACKS AGAINST TIME SYNCHRONISATION 7

2.2.1. Assumptions 7
2.2.2. Threats and attack vectors 7
2.2.3. Impact analysis 11

2.3. SECURITY GOOD PRACTICES 12

3. CHALLENGES AND RECOMMENDATIONS 17

4. BIBLIOGRAPHY 18

EXECUTIVE SUMMARY

Power systems utilize precise timing measurements to monitor grid operation, power balancing and the state of underlying stations during transmission as well as distribution of energy. In modern smart grids, power data acquisition and synchronization need to share time sources to enable decentralized analysis and effective coordination of power production.

Cyber-attacks against time services might have a big impact on power grids and the current publication demonstrates such a scenario. The scenario mostly focuses on modern phasor measurement technologies, since automation trends dictate that these types of devices are considered more appropriate to support the power grid of the future. The presented scenario also takes into account some major legacy input vectors although this publication does not delve into extended details concerning legacy systems. The goal of this scenario is to highlight the importance of quality timing in power distribution, identify risks and present guidelines for consistent time synchronisation.

To do so, this publication is providing an introduction to the technologies used for getting measurements and it continues with the description of a typical architecture which supports the measurement service. Then it describes the threats as well as the attacks against the CIA (confidentiality, integrity, availability) of the service and it provides a set of mitigation measures. Finally, it concludes with some recommendations to technology vendors and energy operators.

1. TIME MEASUREMENT TECHNOLOGIES

Measurements are necessary for various tasks such as power load analysis, differential protection, condition monitoring over time as well as identification of unwanted events, such as physical phenomena or system failures that affect the power grid[1,2]. Due to the usually large geographical area being covered by multiple substations, different measurements need to be synchronised to common time references to facilitate the analysis of data. As a result, the automated processing of substation data is becoming a mission-critical task. Electric power utilities must synchronize across large-scale distributed power grids to enable grid and production balance.

Substation devices can utilize various technologies to create time-sensitive measurements, from legacy Medium-Wave (AM) radio time sources that send timing data using AM frequencies to NTP/PTP servers and modern phasor measurement units (PMUs) able to create phase-angle measurements in real-time. A NTP server uses various time sources and the Network Time Protocol (NTP) to circulate accurate time information to sub-devices for clock synchronization.

PMUs are commonly used, amongst other technologies, **to time-stamp** measurements **against a time source** such as the **Global Positioning System (GPS)**, load balancing, and operator decision support and power distribution. Other (legacy) implementations of underlying networks may also utilise the **Network Time Protocol (NTP)** with relevant servers to communicate data between stations and distribution centres.

PMU measurements are becoming increasingly valuable, since they provide real-time information and enable enhanced monitoring and decision support for automating processes by providing feedback of high accuracy; most often by sampling power-time measurements more than 30 times per second. A cyberattack on these systems can potentially lead to synchronization failures and monitoring errors between the Transmission/ Distribution operator and the power stations.

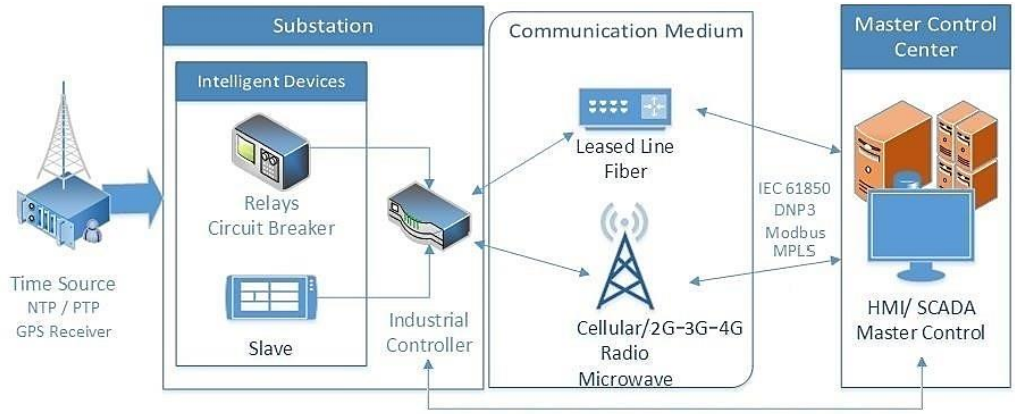
[1] Time Synchronization in the Electric Power System, Report, NASPI Time Synchronization Task Force, The North American Synchrophasor Initiative, March 2017.
[2] Konstantinou, Charalambos, et al. "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment." IET Cyber-Physical Systems: Theory & Applications 2.4 (2017): 180-187. POWER SECTOR DEPENDENCY: TIME SYNCHRONISATION ATTACKS

2. POWER SECTOR DEPENDENCY: SCENARIO DESCRIPTION

2.1. ARCHITECTURE

Figure 1 presents the functional architecture upon which the attack scenario is based. Still, it should be noted that potential risks depend on the type of systems and their implementations at each substation. Dependencies of the power sector on telecommunications differ based on technologies used (e.g. Phasor Measurement Units or NTP/PTP servers), actors involved (manufacturers, government sectors etc.) as well as the actual setup of devices and systems.

Figure 1: Functional architecture of time-phase data processing on the power grid



MIND THE SETUP

Different threats affect different implementations. Potential attacks differ based on technologies used (e.g. Phasor Measurement Units or NTP/PTP servers), actors involved (manufacturers, government sectors etc.) as well as due to the actual setup of devices and systems.

Communication between a power station and the control centre can either be one-way or two-way. Concerning substations, slave equipment can either be PMUs or legacy controllers and/ or similar remote terminal units (RTUs). One-way communications usually involve receiving data from a SCADA system while two-way communications involve both receiving data from a SCADA system and sending back commands through different channels. Industrial controllers (also known as industrial automation controllers, IACs) are often used as middleware between the substation and the control centre, acting as a filter for unifying device protocols and relayed commands. This means that potential attackers must also compromise the (often proprietary) software and systems of the IAC before being able to manipulate any PMUs at the substation.

PMU applications involve the visualisation of wide-area power systems and modelling, modal analysis of power balancing and production, post-event analysis that may trigger relay trip-close functionality, synch checks for substations and flow analysis. One of the most prevalent and often used application involves the detection of oscillations before major system failures[3].

It is noteworthy that potential cyber attacks that exploit the dependency of the power sector on telecommunications are different to engineering challenges. Attacks are triggered by malicious intent and may exploit engineering issues, but they always focus on instances and

[3] Novosel, Damir, Miroslav M. Begovic, and Vahid Madani. "Shedding light on blackouts." IEEE Power and Energy Magazine 2.1 (2004): 32-43.

implementations of systems and technologies. Engineering challenges are shortcomings and current functional limitations in modern technologies and should be approached with a more macroscopic point of view.

2.2. RISK OF POTENTIAL ATTACKS AGAINST TIME SYNCHRONISATION

The threat list (see section 2.2.2) takes into account multiple input vectors and different technologies based on the functional diagram depicted in Figure 1. We consider both legacy technologies along with systems and services that will be widely used in the near future for power grid automation. In general, attacks can occur in various stages of obtaining measurements. Attackers will search to exploit the weakest input vector, which can occur both at the communications network as well as in systems and devices used within the power stations. A key issue with attacks on the power grid relates to stability and provision of power to consumers and to the industry. Both unintentional as well as malicious threats can have an impact on both the integrity and availability of measurements, thus affecting the overall stability of the system in cases where high automation relies on power measurements for decision support and control.

Today, energy operators are more dependent on telecommunication services than they were in the past due to the development of the smart grids. For example, power stations are spread over large geographical areas and devices usually only communicate one-way to send measurement data to control centres. Consequently, decisions and data analysis are performed in centralised systems that may be unaware of the state of GPS receivers, NTP servers and relays in remote stations. Moreover, different stations utilize different technologies. With the advent of phasor measurement units (PMUs), power systems are automating processes and some decisions are now being made on-the-fly without human interruption. As automation spreads to all distribution and transmission systems, the impact from integrity errors and attacks on measurement data will increase proportionally. These features increase the risk of the dependency and at the same time shape potential attack routes and vectors.

Specifically, for PMUs, it is expected that a large part of the power industry will increase their use in the coming years, in an effort to cope with the needs for automating monitoring processes in the distribution and transmission layers, to better control load balancing and service provisions to customers.

2.2.1. Assumptions

The following assumptions are valid for the scenario:

- scenario considers a modern power (smart) grid with PMUs and industrial controllers;
- the grid supports information for automated decision-making concerning power distribution in large urban areas; and
- none to minimum security measures are in place, so as to properly reflect the worst-case scenario of adverse effects.

The presented scenario focuses on attacks at the distribution and transmission layers. Attacks on the consumer end (e.g. smart meters) are considered out of scope.

2.2.2. Threats and attack vectors

Different input vectors exist and different threats may manifest, depending on:

(i) the technology and devices used in the substations;
(ii) intermediate systems and actors; and
(iii) the overall grid structure. Typical implementations utilize a master-slave architecture. Even simpler implementations still use simple internal clocks on substation slaves over radio signals.

The following are some examples of these threats:

(i) If the architecture utilizes PMUs, then the GPS receiver can act as an input vector for spoofing the GPS signal and attacking the integrity of the phase measurement data. This can result in erroneous clock offsets within the PMU, which in turn will introduce an error in the PMU's phase measurement[4]. Depending on the utilization of PMU data and the level of automation on the power grid, these errors can affect control points and even provide a means towards grid destabilization.

(ii) GPS jamming can also be used to attack the availability of data measurements. Some PMUs will revert to local oscillators to determine time and compute phasor measurements. Over time, potential drifting of measurements or incorrect time-stamps may introduce errors in phase angle calculations that will probably increase over time[5]. Moreover, GPS jamming (blocking the reception of GPS L1 1575.42MHz signals) and GPS spoofing, continue to cause serious threats to the precision and accuracy of the timing deriving by GPS. Apart from the potential drifting of measurements and/ or incorrect timing, the jam-to-spoof of the GPS input could potentially trigger real-time process control equipment, like circuit breakers and relays, to shutdown substations and create a blackout.

(iii) Implementations that utilize an NTP/PTP server for producing measurements at the substation are potentially vulnerable to integrity attacks on the supplied data, either at the network level, the application level or both.

(iv) Remotely and directly spoofing and affecting the circuit breaker could potentially disturb the sequence of the timestamps. As a result, the relevant platform for monitoring and analyzing such events will indicate the disturbance. Any attempt to restore and repair such an event, could potentially introduce errors into the systems.

Following the previous analysis and based on the architecture presented in Figure 1, the following list of attack vectors are feasible. All attack vectors presented are based on selected technologies, taking into account both legacy and modern smart grid devices.

Table 5: Attack vectors of potential threats

Communication mediums		
Input vector	**Attack type**	**Description**
4G / LTE / Cellular network	Availability	• Signal jamming: Malicious node interference (physical attacks) • Physical tampering/breakdown of device (physical attacks) • DoS: IP hijacking to disconnect the devices (if IP routing is used) (availability)
	Integrity	• Rogue base stations for man-in-the-middle integrity and confidentiality attacks. Requires physical proximity
Fixed line	Availability	• Line cuts
	Confidentiality	• Eavesdropping with voltage detectors over cable

[4] Konstantinou, Charalambos, et al. "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment." IET Cyber-Physical Systems: Theory & Applications 2.4 (2017): 180-187.

[5] Time Synchronization in the Electric Power System, Report, NASPI Time Synchronization Task Force, The North American Synchrophasor Initiative, March 2017

Communication Protocols		
DNP3 (industrial protocol) **IEC 61850 (industrial protocol)** **Modbus (industrial protocol)** **NTP / PTP (time protocol)** **TCP / UDP (transport protocol)**	Availability	• Network DoS / jamming on measurement packets by deletion of packets
	Integrity	• Packet insertion or packet replay attacks introduce offsets and data mismatch in magnitude of seconds
	Confidentiality	• Eavesdropping of commands and measurements over protocol implementations
Sensors and devices		
Input vector	**Attack type**	**Description**

Phasor Measurement Units (PMU)	Integrity	• Spoofing GPS coordinates injects incorrect phase-angle measurement. Radio-Frequency equipment (integrity).
		• GPS unavailability may trigger fallback to other sources.
		• Device synchronizes to a spoofed time signal to maintain an incorrect stream of time-stamps.
		• Potential drifting of measurements over time.
		  ○ Need for close proximity to PMU equipment.
		  ○ Changes in synchrophasor and phase angle calculations[6].
		• Data manipulation through software (Supply chain attack)

	Confidentiality	• Backdoor access on vendor device (Supply chain attack)

NTP/PTP server	Integrity	• Master announcing wrong time. Manipulation of control loop packets for controlling clocks at slave (integrity).
		  ○ Synchronizes to a spoofed time signal to maintain an incorrect stream of time-stamps
		  ○ Affects all kinds of packets (sync, delay-request/-response packets).
		• Delaying the slave clock causes an offset of μs, which escalates in the order of mrad in the synchrophasor estimation (software/ component attack)

Industrial Controllers	Availability	• DoS on the real-time clock (Malicious/ Accidental insiders)
	Integrity	• Adverse effects on connection to servers (Malicious/ Accidental insiders) • Data manipulation through software (supply chain attack)
	Confidentiality	• Backdoor access on vendor device (supply chain attack)
Relay Controllers	Integrity	• Adverse effects on connection to servers (Malicious/ Accidental insiders) • Data manipulation through software (supply chain attack)
	Confidentiality	• Backdoor access on vendor device (supply chain attack)

[6] Time Synchronization in the Electric Power System naspi, North American Synchrophasor Initiative | March 2017

Attack vectors can be roughly divided into three categories: Vectors in **communication mediums**, in **underlying protocols** used and on **substation devices** themselves.

a) Attack vectors can be roughly divided into three categories: Vectors in **communication mediums**, in **underlying protocols** used and on **substation devices** themselves. Attack scenarios on modern over-the-air communication mediums mostly involve attacks against availability, with the most prominent ones being jamming through malicious node interference and rogue base stations, as well as man-in-the-middle integrity and confidentiality attacks. Confidentiality attacks on legacy systems are also possible through eavesdropping with voltage detectors over cable, although these attacks are known to generate too much noise on the tampered line.

b) Attack vectors also exist on the numerous protocols that can be used for transmitting data. Industrial protocols (such as DNP3, MODBUS etc.) can be implemented in various ways. Some implementations utilize connections over TCP or UDP. These implementations are subject to threats common in IT networks in general, e.g. IP spoofing, TCP session hijacking, Man-In-The-Middle, and RST/ FIN attacks. Concerning industrial protocols themselves, some availability attacks exist, namely network Denial of Service (DoS) and/ or jamming of measurement packets by deletion of packets. Integrity attacks focus mostly on packet insertion or packet replay attacks to introduce offsets and data mismatch in magnitude of seconds. Confidentiality attacks on protocols include eavesdropping of commands and measurements over protocol implementations. In some cases, eavesdropping can also be executed over encrypted MODBUS traffic[7].

c) Some attack vectors are related to the devices used in substations. Attacking the integrity of GPS signals can affect PMU measurements and cause an increasing phase angle difference, able to divert decision controls and trigger load shedding or otherwise affect system executions[8]. Such attacks are considered sophisticated, since they require Software Defined Radio (SDR) and radio frequency (RF) devices, on-site close proximity to the PMUs and partial knowledge of device functionality. Attacking solely the availability of time-sensitive measurements is an easier task in comparison; e.g. jamming. GPS unavailability will potentially trigger fall-back to other sources (oscillators). Devices can then also synchronize to spoofed time signals and insert an incorrect stream of time-stamps. Other device attacks at the substation include wire cuts between the GPS receiver and the PMU and/ or manipulation of control loop packets at the slave. This can result in incorrect estimation measurements and potential drifting of measurements over time. Delaying the slave clock can cause an offset of μs, which escalates in the order of mrad in the synchrophasor estimation.

PMUs at the substation can convert GPS signals into various protocols (such as NTP or PTP) for further use within the substation or even use other sources for NTP time measurements. Similar attacks on packet crafting affect all NTP protocol/ server implementations. Replay attacks on network time packets can affect measurement data integrity. The master server will seem to announce the wrong time and will affect both sync and response packets. NTP has been used to manipulate logs and change the time on computer systems, thus altering the sequence of events. When clocks are not synchronized, distributors have a much harder time

[7] Tsalis, N., Stergiopoulos, G., Bitsikas, E., Gritzalis, D., & Apostolopoulos, T. K.. Side Channel Attacks over Encrypted TCP/IP Modbus Reveal Functionality Leaks. In the 15th International Conference on Security and Cryptography (SECRYPT 2018), ICETE (2) (pp. 219-229).
[8] Konstantinou, Charalambos, et al. "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment." IET Cyber-Physical Systems: Theory & Applications 2.4 (2017): 180-187.

performing data correlation across disparate systems for automation of processes. Using NTP or PTP protocols and servers can result in constant measurement biases if multiple, independent sources are not used. Optimally, the IEEE C37.118 requirement of 1μs accuracy can be met through GPS signals[9]. Backdoor access on vendor devices and integrity attack through software are also considered a possible attack vector, where the attacker can take control of measurements and affect decision making at the distribution layer.

2.2.3. Impact analysis

Impact of potential attacks varies according to the attack vector, system specifications and the type of services that is being affected. Modern implementations that utilize PMUs to automate load balancing and monitor for system failures for decision support, exhibit higher impact than traditional and legacy systems due to the increased level of automation. The most important technical errors that can be introduced through the aforementioned attacks can be summarised as follows:

- Inaccurate monitoring and control functions of PMU-based load and grid stability;
- Erroneous or overly delayed timing data in NTP-based stations can be discarded from the operator and, if the number of dropped packets increases, power grid balancing may be less effective and trustworthy;
- Overflow of timing data can result in buffer overloads from too many time-stamps for the same instant for the same channel and PMU. This can lead to system unavailability;
- Incoherent timing data about time and grid condition will produce incorrect results and leap second events; and
- Man-in-the-middle or spoofing attacks lead to erroneous estimations and incorrect phase angle computations, which in turn can cause an unnecessary generator trip.

Potential failures can cause varying levels of impact. Effects can vary based on system specifications and devices used and can range from simple miscalculations on substation power data that can be mitigated through error checks, to area blackouts. In automated grids that utilize PMUs, the introduction of false measurements (either by accident or on purpose) can possibly trigger control actions and even cause grid instability[10].

All the attack scenarios of this dependency were circulated to subject matter experts from the public and private sector, including telecommunications and energy experts and other stakeholders. The following table depicts the likelihood and impact for each scenario based on the average of the given answers of the relevant stakeholders.

Table 6: Impact and likelihood of attack scenarios

	ATTACK SCENARIOS	IMPACT	PROBABILITY
Communication mediums	**Physical attacks** (e.g. on Cellular network/ Fixed Line)	Moderate	Highly likely
	Network Attacks (e.g. on 4G/ LTE/ Cellular network)	Moderate	Likely

[9] Time Synchronization in the Electric Power System, Report, NASPI Time Synchronization Task Force, The North American Synchrophasor Initiative, March 2017
[10] Jiang, X., Zhang, Z., Harding, B.J., et al.: 'Spoofing GPS receiver clock offset of phasor measurement units', IEEE Trans. Power Syst., 2013, 28, (3), pp. 3253–3262

	ATTACK SCENARIOS	IMPACT	PROBABILITY
Communication Protocols	**Network Attacks** (e.g. on DNP3, IEC 61850, Modbus protocols)	Severe	Moderate
Sensors and devices	**Integrity attacks** (e.g. on PMU, NTP/ PTP server)	Severe	Likely
	Availability attacks (e.g. on PMU)	Moderate	Likely
	Supply chain attacks (e.g. on PMU, Industrial and Relay controllers)	Severe	Highly likely
	Delay attacks (e.g. on NTP/ PTP server)	Moderate	Unlikely
	Malicious/ Accidental insiders (e.g. on Industrial controllers)	Moderate	Likely

2.3. SECURITY GOOD PRACTICES

Transmission as well as distribution operators need to implement specific security measures in order to protect systems in a power grid, especially when automation is widely used (e.g. in smart grids). Good practices and relevant security measures are broken down into separate groups, allowing a more focused approach on different technologies and devices.

Most widely known measures relevant to network security also apply to IT networks in power grids. Also, we should note that, apart from the scenario specific measures, common organisational security measures such as security governance models, security policies and procedures, standards and certifications, training and awareness-raising, risk management, audits and assessments and contractual clauses, also apply to the power sector.

Technical measures specific to technologies presented in the aforementioned scenarios include, among others, device and configuration management, network monitoring, patching and updating, network segmentation and authentication, and network security (certificates, protocol configuration etc.).

The NTP protocol measures synchronisation distance from primary time sources using Stratum levels. Stratum 0 devices (like GPS clocks) are usually used as a reference clock (or synchronisation source) for a Stratum time server[11]. Some best practices concerning NTP servers and their underlying protocol are listed below[8,12].

[11] Mills D., et al, RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification, Internet Engineering Task Force (IETF), ISSN:2070-1721 (2010)
[12] Snoke T., Best Practices for NTP Services, Carnegie Mellon University, Software Engineering Institute, https://insights.sei.cmu.edu/sei_blog/2017/04/best-practices-for-ntp-services.html

Table 7: Technical good practices based on scenario technologies

Technical good practices	
Category	**Good Practice**

Phasor Measurement Units (PMU)	• Establish an Electronic Security Perimeter
	• Minimize number of electronic access points
	• Utilize network segregation for PMUs and substation LAN
	• Firewalls with white list (deny by default)
	• PDC provides a security layer
	  ○ Users access PDC not PMUs
	  ○ Security upgrades occur at PDC rather than a PMUs
	• Take into account IEEE C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems
	• Implement IPSEC on substation gateway device
	• Anti-spoofing and anti-jamming for PMU at the hardware level. Some devices have built-in anti-jamming devices with 99min lock
	  ○ Blocks software defined radio (SDR) to overtake GPS signal

Transport layer (TCP/ UDP)	• Secure data streaming from PMUs to the industrial controller • Close unnecessary ports • One-way, whitelisting firewall rules • Hide PMU IP addresses • Disable command frames • Encrypted VPN connections • Avoid remote bidirectional connections and employ SSH when needed
NTP/ PTP server and protocol	• Use multiple Stratum 0 devices to correlate time to NTP servers • Protect the NTP protocol with multiple paths between master and slave clocks • Hide primary NTP servers and only allow secondary systems to access them for querying information remotely (if necessary) • Utilize access control lists (ACLs) as well as a firewall to filter connections to NTP servers • Whitelist commands and systems able to issue commands to the NTP server. Do not allow public queries • Standardize systems to UTC time to facilitate data correlation • Consider the use of cryptography for sensitive data

Table 8: Generic applicable good practices

Generic good practices	
Category	**Good Practice**
Dynamic network segmentation and use of firewalls	Separate critical parts of the network from non-critical parts. For instance, it is recommended to separate PMU and IAC devices from other IT systems in substation equipment. In general, it needs to be evaluated if the benefits of connecting a specific device to the network outweigh the risks.
Use of multiple time sources	Using multiple source for time information lowers the risk of unavailability (and sometimes

Generic good practices	
Category	**Good Practice**
	integrity) attacks. Various sources include: Internal, local clocks, GNSS/ GPS, NTP servers, Optical Transport Networks (OTN) over telecom networks, etc.
Check that the alternative time sources work	Checks should be conducted on regular intervals to verify that all used time sources are up and running. Additionally, utilize more than one time signal sources so as to increase the accuracy and availability, e.g. GPS and NTP or GPS and DCF77/ radio.
Antivirus and antimalware software	IT systems should run antimalware and anti-spam software to detect and remove or quarantine malicious software.
Device configuration and management	Utilize ICS-based asset inventories to ensure a sound understanding of the grid's systems and their components. Such inventories also allow changing configurations and creating and evaluating logs of system events.
Apply patching and updating procedures	Regular patching and updating of software and devices are essential to avoid the exploitation of known vulnerabilities as well as to ensure the detection of attacks using know paths.
Encrypt data	It needs to be evaluated if the use of encryption is necessary to protect critical processes and decision making, especially at the distribution layer. If so, cryptography must be used following international standards.
Protect remote connections and systems	Remote connections to substation systems need to be adequately protected with strong access control, authentication mechanisms and relevant network security measures.
Assess the risk	The understanding and management of risk are key issues for the electric sector organizations. Therefore, a harmonised risk methodology across the organizations is recommended.
Information sharing	Ensure the implementation of effective information sharing models between the sectors.
Prioritization of energy supply	Discussing and prioritising supply of services (based on network topology). More specifically: • ensure energy supply to critical Telco location; and • ensure communication services to critical locations (substation control centre).

GPS timing can be secured using a multi-layered approach. Anti-jamming and anti-spoofing mechanisms can protect the antenna, while software assurance can provide similar anti-jamming as well as anti-spoofing measures to device components. Assurance through product integration and installation can also aid in securing timing functionalities, through proper use and configuration of devices and oscillators[13].

[13] Kevin M. Skey, Responsible Use of GPS for Critical Infrastructure, Homeland Security Systems Engineering and Development Institute (HSSEDI), 6 December 2017

Table 10: Summary of the power sector dependency attack scenario

POWER SECTOR DEPENDENCY ON TELECOMMUNICATIONS	
Threat types	• Unintentional (interference, out-of-band emissions, natural phenomena etc.) • Intentional (Jamming, spoofing, packet crafting)
Description	The power grid automation utilizes time synchronization in the following areas[14]: (i) Transmission and distribution; (ii) Real-time data acquisition and analysis from GPS and PMUs e.g. power balancing (iii) Real-time process control of equipment like circuit breakers and relays, e.g. differential protection; and (iv) Fault recording for fault and performance analysis.
Assets affected (Telecommunications and positioning services)	The assets primarily affected by cyber-attacks in our scenario include: • Network Time Protocol, Precision Time Protocol and relevant communication protocols. • Various telemetry equipment and components • Underlying telecommunication lines, e.g. fixed lines, LTE - 4G equipment etc.. • GPS embedded location modules.
Assets affected (Energy sector)	The assets primarily depended on the telecommunications provider assets that are affected include: • PMU, Circuit breakers, Relays; • GNSS, GPS Antenna/ Antenna Diplexer; • Industrial Automation Controllers (IACs) • SCADAs; • Data processing modules and servers
Criticality	Incorrect timing, either introduced by failures or malicious actions can cause numerous issues during data analysis: • Inaccurate monitoring and control functions of PMU-based load and grid stability. • Erroneous or overly delayed timing data in NTP-based stations can be discarded from the operator and, if the number of dropped packets increases, power grid balancing may be less effective and trustworthy. • Overflow of timing data can result to buffer overloads from too many time-stamps for the same instant for the same channel and PMU. This can lead to system unavailability. • Incoherent timing data about time and grid condition will produce incorrect results and leap second events. • Man-in-the-middle or spoofing attacks lead to erroneous estimations and incorrect phase angle computations, which in turn can cause an unnecessary generator trip. Such attacks can result to monetary loss, grid imbalance and even power outages. They can also produce “false interpretations of grid conditions and inappropriate control actions”[4]. Unrecorded oscillations can lead to equipment failure and contribute to large-scale blackout.

[14] https://electrical-engineering-portal.com/time-synchronization-substation-automation

POWER SECTOR DEPENDENCY ON TELECOMMUNICATIONS	
Good practices	• Resilience: Timing sources and technology must ensure high availability in the event of loss of time synchronisation from one or more substations. • Security: Ensure the integrity of input sources and synchronisation data. • Accuracy: Need for identification of data corruption, both at GPS and network levels. • Use of alternate timing sources. • Adhere to relevant standards (e.g. IEEE C37.118.1-2011)
Challenges and gaps	• Challenge 1 – Lack of built-in anti-jamming components • Challenge 2 – Need to defend against rogue base stations and spoofing attacks • Challenge 3 – Lack of network security measures for protecting data transmission • Challenge 4 – Low pace of standardisation • Challenge 5 – Lack of high resilience and automated detection of errors:

3. CHALLENGES AND RECOMMENDATIONS

Identifying good practices per technology used leads to the identification of open security issues in the synchronisation of the aforementioned systems. Enhancing security in the near future equals mitigating the risks introduced by modern technologies, automation and the geographical disparity between power substations. The most important challenges for modern power stations as well as the future work can be summarised as follows:

Challenge 1: **Lack of built-in anti-jamming components**

Recommendation: Vendors should design modern devices for substation automation (including GPS receivers) with security in mind. Built-in anti-jamming components such as lockouts for extended periods of time, dynamic reconfiguration etc. are necessary to mitigate risks from close-proximity jamming attacks.

Challenge 2: Need to defend against rogue base stations and spoofing attacks

Recommendation: Operators should establish electronic perimeters and implementing measures against spoofing attacks, such as signal processing techniques are necessary to protect substation synchronisation. Vendors and operators should utilize technologies to detect and correct measurement data against spoofing attacks; primarily for GPS timestamps. They should also apply mandatory security patches for lifetime on sensors/ devices.

Challenge 3: Lack of network security measures for protecting data transmission

Recommendation: Operators should always implement basic measures for substations in order to protecting underlying networks and protocols, such as network segregation, filtering and access rules. Firewalls and industrial controllers acting as intermediate filters should be in place in all substations. Grid automation also needs to incorporate control checks on functional.

Challenge 4: Low pace of standardisation

Recommendation: Current certifications and standards are not up to speed with the rate of adoption of automation in modern smart grids. Vendors should design modern devices used for automation in a way that meets universally accepted requirements and implements selected security measures through proper standardisation procedures. This will aid in creating a normalised security level across power grids in the entire EU while supporting new technologies.

Challenge 5: Lack of high resilience and automated detection of errors

Recommendation: Transmission and distribution layers are beginning to automate load balancing and monitoring of power grids through real-time PMU measurements. This automation needs adequate monitoring processes. Operators must adopt tools and procedures that will enhance power grid's resilience against malformed and/ or injected data that can affect decision making in modern smart grids. Data validation should be implemented in mission-critical processes.

4. BIBLIOGRAPHY

Time Synchronization in the Electric Power System, Report, NASPI Time Synchronization Task Force, The North American Synchrophasor Initiative, March 2017.

Konstantinou, Charalambos, et al. "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment." IET Cyber-Physical Systems: Theory & Applications 2.4 (2017): 180-187.

Novosel, Damir, Miroslav M. Begovic, and Vahid Madani. "Shedding light on blackouts." IEEE Power and Energy Magazine 2.1 (2004): 32-43.

Tsalis, N., Stergiopoulos, G., Bitsikas, E., Gritzalis, D., & Apostolopoulos, T. K.. Side Channel Attacks over Encrypted TCP/IP Modbus Reveal Functionality Leaks. In the 15th International Conference on Security and Cryptography (SECRYPT 2018), ICETE (2) (pp. 219-229).

Jiang, X., Zhang, Z., Harding, B.J., et al.: 'Spoofing GPS receiver clock offset of phasor measurement units', IEEE Trans. Power Syst., 2013, 28, (3), pp. 3253–3262

Mills D., et al, RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification, Internet Engineering Task Force (IETF), ISSN:2070-1721 (2010)

Snoke T., Best Practices for NTP Services, Carnegie Mellon University, Software Engineering Institute, https://insights.sei.cmu.edu/sei_blog/2017/04/best-practices-for-ntp-services.html

Kevin M. Skey, Responsible Use of GPS for Critical Infrastructure, Homeland Security Systems Engineering and Development Institute (HSSEDI), 6 December 2017

Edvard, Protocols applied for time synchronization in a digital substation automation, Electrical Engineering Portal (2018) https://electrical-engineering-portal.com/time-synchronization-substation-automation

TP-03-20-283-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-344-5
DOI 10.2824/496449