Enhancing the Backup of Power Network Substations Control Systems through Version Control

István DÉNES

Automation Department - Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, Bécsi út 96, 1037 Budapest, Hungary

Accenture ISS Kft, Lechner Ödön fasor 10/B Budapest, Hungary,

i.denes@accenture.com

Sándor SEMPERGER

Automation Department - Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, Bécsi út 96, 1037 Budapest, Hungary

semperger.sandor@uni-obuda.hu

Abstract: *Power networks substation control systems (substation IACS) are special, from cyber security point of view. As part of the critical infrastructure, the availability requirements of substation IACS are high. Business interruption, caused by security incidents, will have severe consequences nationwide. Protecting substation IACS is becoming more than just the financial interest of the power distribution company, it is under present political situation also a matter of state security. The research uses the terminology and follows the recommendations of ISA 62443 , in particular ISA 62443-3-3. It expresses security maturity, both present and targeted, in Security Levels (see Fig 1, definition of security levels of ISA 62443). This research analyses particularly the backup system of substation IACS. It gives a view of present security maturity of those backup systems, recommends a new level of security based on recent and expected security incidents, and offers a solution for introducing enhancements through application of a Version Control System as an automated solution for backups. In comparison to other similar research on substation automation system security, it elaborates the use of Version Control Systems from the point of view of increasing Security Level of Substation IACS backups, considering the relevant Security Requirement according to ISA/ENSI 62443. The NIS2 EU directive on critical infrastructure security also urges improvement of backup systems of substation IACS. As power distribution organizations will be declared, as essential entities according to NIS 2, the OT security controls will need enhancement.*

Keywords: Cyber Security, Industry Automation and control System (IACS), Backup and Restore, Security Level (SL), Version Control

1 Introduction

Power distribution companies are cost sensitive, the operation and maintenance costs of a substation need to be kept low; therefore, the headcount of personnel of substations is constantly under pressure to be reduced. The limited availability of trained resources is another driver of reducing headcount in the industry: the gap between the demand and availability of trained and experienced automation experts is getting wider. For these reasons, substations today need to be operated, maintained with constantly decreasing headcount- both in numbers and seniority. Operation and maintenance works are done by experts of decreasing seniority, education, and experience. Also, a constantly increasing part of that work is outsourced to subcontractors and vendors -this is also a challenge, since their access authentications increase the surface of cyber-attacks.

Another challenge is the limitation of downtime. Security requirements, such as patching, backup, updates, monitoring need to be done without effect on business process. These challenges drive the digitalization of the industry. There is a growing demand for conducting operation and maintenance remotely. Also, an increasing part of those processes are to be covered with automatic solutions. Due to this, there is an increasing number of TCP/IP connected assets on substations and a good part of them can be accessed remotely.

Digitalization helped to solve the headcount issue and to maintain the costs of operation and maintenance, but it increased security vulnerability. One of the new vulnerabilities is increased maturity itself: a simple relay or voltage switch cannot be a subject of a cyberattack, but intelligent ones are a target. The second vulnerability is remote access- once they are accessible to operators and maintenance personnel, they can be accessible also to threat actors.

Since substations are in most cases unmanned, they are exposed to physical access of cyber security threat actors. Recent research also show that Power networks are becoming desirable targets of cyber security threat actors. According to 2022 S&P Global Energy Security Sentinel [2], there were 25 known cyberattacks on energy sector in the years from 2020 to 2022, and more than half of those, 13 were in 2022 alone. This shows an increase in the likelihood of initiation of a cyberattack against power networks. The motivation of threat actors is also increasing, and their means are getting more sophisticated due to increasing political strains globally. Speaking on the language of ISA 62443, we need to increase the Security Level (SL) of IACS assets, (ISA-ENSI 62443-1-1, 2007, Security for industrial automation and control systems, Edition 1.0 2007 Part 1-1 Terminology, Concepts and Models chapter 5.10.2.2 SL (Target)Target Security Level, [4])

For the above reasons, the security controls of a substation IACS need to be enhanced on all Foundational Requirements of ISA 62443.

The security of a substation IACS can be increased either by decreasing the likelihood of a successful attack or through decreasing the possible impact of a security incident through, for instance, a more advanced backup system.

The premise of this paper is that the security level of substation IACS backup [1] can be increased through the use of a version Control System (VCS) and we elaborate that improvement herein.

2 Description of the Challenge

2.1 Security Maturity of Power Network Substation IACS now

The security maturity of Power Distribution Substation IACS today is typically low: using the terminology of ISA 62443, their security level is in most cases on SL2: they are protected against threat actors of low motivation with little resources, having no IACS specific knowledge. (See Fig 1., definition of Security Level 2)

As stated in the paper (A Holistic Approach - How to Achieve the State-of-art in Cyber security.[6]) "The high exposure to cybernetic risks is due to the fact that these systems have a relatively low level of protection maturity".

To increase that level of security, we need a business case: according to ISA 62443 standard, "Establishing a business rationale is essential for an organization to maintain management buy-in to an appropriate level of investment for the IACS cyber security program". (ANSI/ISA 62443-2-1 (99.02.01)-2009 4.2.2 Element: Business rationale [8]).

Figure 1
Security levels of ISA 62443. Source:[18]

2.2 Game changer milestones in power distribution security

As we have seen, power distribution security today is generally on a security level of SL2, which protects against threat actors of low motivation, simple means and no IACS specific knowledge.

Recent events show however, that power distribution is becoming a target of international terrorism and might be attacked even by nations, possessing over sophisticated means.

The first game changer event was the 2013 physical attack on transformers in Metcalf, CA, [14] which, though not a cyber-attack, raised awareness on power distribution security in general. Not long after Metcalf attack, in 2015 the first known cyber-attack against a power distribution network was carried out [15], blacking out a whole region in Ukraine. This latter attack, impacting 250000 customers of the Ivano-Frankovsk region, was probably the first complex attack on a critical infrastructure:

On 23. December 2015 the command over the SCADA of Ivano-Frankovsk power distribution hub was taken over, using Black energy 3 to compromise credentials of the system- the operators of the SCADA could actually see the manipulated moves of the attackers on the screen. The effect of the attack was increased through compromise of serial-ethernet converter of sensors and a TDOS attack on customer hotlines.

However, the attack did not raise risk awareness of power distribution companies significantly, as it was made on a site with extremely low maturity of protections. The paper "recommendations of an analysis of the attack" [10] let us believe that on the site even the basic protections were missing. For instance, as we understand from the recommendations of the paper, there were no backup made on the site at all: "Use backup and recovery tools to take digital images from a few of the systems in the supervisory environment such as Human Machine Interfaces (HMI) and data historian systems every 6-12 months." This clearly shows that the site was operating without even basic protections of backup and restore, as described in Foundational Requirements 7 (FR7): Resource Availability of the ISA 62443 [1]. Using the terminology of ISA 62443-3-3, the Security Level of the site was zero (see fig.1). This low maturity of the impacted Ukrainian site made power distribution companies believe that their higher, Security Level 2 protection is sufficient to protect themselves from a threat actor, like the one which attacked the Ivano-Frankovsk site.

Ever since, power distribution in Ukraine is subject of international cyber warfare [16]. Recent trends [17] show that threat actors of attacks against critical infrastructure are supported increasingly by governmental and quasi-governmental organizations, allowing them more sophisticated means, and giving them higher motivation.

2.3 Targeted Security Level of Power Network Substation IACS

As we will see in this chapter, based on the definition of security levels of ISA 62443 (Fig1), the acceptable target security level of high voltage substation IACS under present circumstances is minimum SL3. To justify this increase of SL, we will address three components of SL through analysis of cyber-attacks of near past: sophistication of means, IACS specific knowledge and motivation.

Sophisticated Means

The attacks, listed in the 2022 S&P Global Energy Security Sentinel [2] against Power Distribution architecture clearly show that the means used by threat actors are getting more sophisticated as in the past. The Ivano Frankovsk attack invoked use of Black Energy 3 [13], the same time RS 232-ethernet converters were attacked and the customer support call center was subject to a Denial-of-Service attack. This well coordinated, complicated action cannot be considered as “misuse by simple means” of SL2

IACS Specific Knowledge

One of reasons of increasing Security Requirement of backup systems of substation IACS to SL 3 is that, as it has been stated in literature, in contrast to natural disasters with random behavior, malicious cyberattacks, designed by well-equipped and knowledgeable adversaries, are often tailored to create specific severe damage to power systems [9]. This tendency implies that threat actors have increasing knowledge about the business processes of power distribution, and they also have specific knowledge about the IACS of substations.

Motivation increased from low to moderate.

As cyber-attacks are funded increasingly by governmental and semi-governmental organizations, increasing funds allow a significant increase in motivation of threat actors. We can no longer speak about low motivation [16][17].

Substations are usually on unmanned sites on remote locations (P1402/D11, Jun 2021 - IEEE Draft Guide for Physical Security of Electric Power Substations, IEEE). Since they are easy to access physically, and the consequences of security incidents are high, they are becoming a desired target of threat actors (see Fig. 2). And, as we have seen, these substations are expected to be attacked in future with higher motivation, using more sophisticated means and having more resources. Even now we see an increasing number of cyber incidents [2] which are justifying the increased costs of security controls.

Figure 2
A 500 kV Transformer substation in China. Source:[19]

We have found reasons to increase security level of substation IACS to SL 3 (prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation,) from the today generally used level 2 (prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, and low motivation ISA-ENSI 62443-3-3, 2013, chapter A.3.2.5 [1]). This demand to increase security level of substation IACS is consequently setting also higher expectation for the backup solution of their control systems.

This paper elaborates the concept of introducing VCS, to meet those higher expectations of SL3.

2.4 Backup systems in Power Distribution Substations today

As we concluded in chapter 2.1, the maturity of substation IACS backup systems are today typically on SL 2- this means, according to ISA 62443-3-3 [1], they meet only the basic requirements of backup, which means, they have the capability of making backups of user level and system level information without affecting normal plant operations- but the enhanced requirements, like automation, verification and monitoring are not met.

This means, the only requirement those backup systems meet, is that it shall be possible anytime to make either full image, differential or incremental backup manually about information which is needed for restoring the control system to a known good state. This is done without overloading the process network or other resources.

As we have seen in the introduction, this is far more than what Ivano Frankovsk power distribution had in time of the attack [10]: contrary to most substation IACS, there were not even manual backup functions driven by established formal processes. The backup files were not available at the time of the attack and the control system could not be restored to a known good state after the security incident.

But even the standard ISA 62443 requirements of backup, which were far from being fulfilled in Ivano Frankowski during the attack, have two weaknesses:

1. Since it has only manual backup, the reliability of backup depends on the quality of formal process and the discipline and awareness of the staff.
2. It allows no verification of backup process and of backup files, which can easily lead to unintentional latent mistakes or intentional manipulation of backup files or process. Without capability of verification, we cannot trust that we will have all the files necessary to restore the control system to a known good state.

3 Meeting the Challenge

3.1 About security level 3 of backup systems

To increase the security level of a backup system to SL3, we need to meet the following enhancements according to ISA 62443-3-3, 11.5:

Backup verification

"The control system shall provide the capability to verify the reliability of backup mechanism" (ISA 62443-3-3, 11.5.3, (1))

In other words, we need a process and solution of validating the capability of restoring the control system to a known good state.

Backup automation

"The control system shall provide the capability to automate the backup function based on a configurable frequency". (ISA 62443-3-3, 11.5.3, (1))

This means backups shall be made without human interaction automatically, triggered both by changes and by configured time.

Backup Monitoring

To increase the security Level of backup system to SL 3, it is recommended to have a monitoring function.

> "Information required for post incident forensic activity realizes the function to detect the legitimacy of the data to be backed up, operators and the data to be recovered so the system can effectively promote the confidentiality by preventing the operators backing up data to illegal destination and restoring data to illegal target machine. (Research and Implementation of a Data Backup and Recovery System for Important Business Areas" [5])

3.2 Version Control as backup

A feasible way of covering all the required and recommended enhancements is the using a Version Control Systems (VCS) as a solution for automated backups. VCS were originally used by OT software developers. "A Version Control System, also known as a Revision Control System or Source Control System, is required when developing projects above a few hundred lines of code or where more than one developer needs to collaborate on a project." (The History of Version Control, NB Ruparelia - ACM SIGSOFT Software Engineering Notes, 2010) [3].

It is a relatively new approach to use VCS as a cyber security system of IACS on level 1 (Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), bay controllers) and level 2 (Supervisory Control and Data Acquisition, (SCADA), Distributed Control Systems, (DCS) of the Purdue model. One of the first extensive uses of VCS for shopfloor anomaly detection was in automotive industry. In" Detection of Anomalous Values within TIA Project Data History for Industrial Control Systems." [11] a solution is described, where a VCS is used for detecting changes to the data, caused either by infiltrated attacks, or by unintentional or malicious changes made by employees, who have direct access to the machines.

The advantages of VCS as backup solution of control systems are:

- Most VCS enable backup of PLCs - conventional systems cannot do that
- During backup of SCADA, DCS solutions, most VCS detect variables and manage them properly
- VCS allow continuous monitoring for unwanted or latent changes

We also need to mention that VCS as backup solution has some significant disadvantages, like:

- High cost: apart from the significant license costs of VCS, for the backup of PLCs you need a development environment for each type of PLC in scope
- None of the VCSs support all type of PLCs, SCADAs and DCS
- VCS will not support custom made solutions
- Encryption: most VCS don't support encryption of backup files in rest

- The installation, operation and maintenance of VCS systems need senior resources

Taking in consideration above listed advantages and disadvantages, the decision for a VCS based automatic backup system the following aspects need to be considered:

- Size of the site: automatic backup is more feasible on sites of considerable size- number of assets exceeding 100.
- OT landscape shall be considered: are PLCs, SCADAs, DCS supported by the VCS
- Can we compensate the lack of encryption with other controls of security, like, for instance, physical security

Apart from above aspects, if the site is owned by an essential organization according to local transposition of NIS 2, it also need to be checked, if the local transposition of NIS 2 require specifically an automatic backup solution.

One of the first applications of VCS for security related anomaly detection were not without reason in automotive industry: the high number of PLCs with a relatively homogenous vendor background is an optimal environment for the use of VCS.

VCS in such cases acts as a combination of an automatic backup and a File Integrity Monitoring System: it makes periodically (every minute even, if needed) backups of OT assets, and compares the new backup with the last good version. If difference detected, it gives an alarm.

4 Proposed example of version control application in a substation

In the given example a substation IACS backup is covered with a Versiondog system. The reason of choosing it was its capacity to backup and restore all PLCs, SCADAs and network devices of the site.

4.1 What is VCS

Some control components, like in our example, WinCC Scada and S7 300 PLCs, have native support of most VCS. This means, their incremental, differential, or full image backups, version control and restore functions can be done without programming, only configuration of backup strategy and frequency shall be done.

Most network devices, common in substation environment, are natively supported by most VCS.

For substation Intelligent Electronic Devices (IED), the backup of configuration and version control can be done as text files, since they are usually Linux based. But since their configuration in most cases is not changing, VCS can be used for periodic refresh from static configuration files stored in VCS.

An important function of VCS is monitoring. Actions taken, like manual backup, restore or refresh of an asset, change in backup frequency or any other parameters will be logged. And logged data can be sent to a Security Incident and Event Monitoring (SIEM) system for further analysis.

VCS stores backup files in our example on a server locally. It supports no encryption of backup files and no external storage. However, it supports integration to most common automatic backup systems, like Acronis. If encryption or external storage of backup files is a requirement, this integration capability can cover that.

4.2 The use of VCS in our example

In our proposed example (Fig 3.) the substation IACS consists of a SCADA system (WIN CC Classic), network devices, Substation IEDs (protection Relays) and PLCs. They are all interconnected through a substation LAN.

VCS is hosted locally on a physical server which is connected to substation LAN. All backups are stored locally on the server. A VCS client is connected to the same substation LAN. There is no integration to other backup systems, as encryption of backup files or external storage in our case is not a requirement. The proposed backup strategy for the asset types are the following:

4.2.1 WIN CC SCADA

WIN CC Classic SCADA is natively supported by most VCSs. Full image and incremental backups are supported usually with configurable frequency. New versions are compared to previous versions. The VCS client gets an alert in case difference is detected. In case no difference detected, the old version will be overwritten. It is advised, depending on infrastructure capacity, to make a full image backup of SCADA server at least weekly, and incremental backup daily.

4.2.2 Network devices

The Hirschmann network devices, used in our example, are natively supported by the chosen VCS. Settings are advised to be backed up after any change done and at least weekly.

4.2.3 Substation IEDs (protection Relays)

For the configuration backup and restore of IED devices a Linux plug in of the VCS is used. Backup and Restore is done through SSH. Version Control is based on the strategy of text file comparison. Substation IEDs are advised to be backed up with every change but refreshed at least weekly.

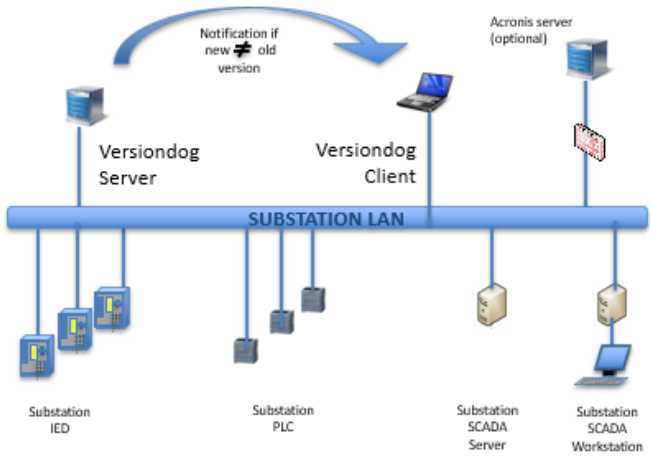

Figure 3
A possible architecture of using version control on a substation. Source: authors

4.2.4 PLCs

Siemens PLCs are natively supported by most VCS - for this, of course, the programming environment needs to be provided. PLCs are advised to be backed up with every change but at least daily.

5 Conclusions

Recent threat intelligence shows that the security level of power network HV substations IACS, which is today typically on level 2, shall be raised to level 3: (Prevent the unauthorized disclosure of information to an entity actively searching for it, using sophisticated means with moderate resources, IACS specific skills and moderate motivation)

The business case behind this aim is validated through evidence of having in past years attacks on power distribution sites by threat actors having IACS specific knowledge and sophisticated means. Recent political developments leave unfortunately no doubt that in mid-terms attacks against power network substation IACS will increase both in numbers and sophistication.

Speaking specifically of their backup systems, for increasing the security level in substation IACS, an optimal solution is offered, through the use of VCS. A VCS offers a low TCO solution, to meet all of the basic and most recommended enhancement requirements of Security Level 3 [1].

5.1 Automated backup

The chosen VMS meets basic enhancement requirement of offering configurable automated backups entirely. ([1], chapter 11.5.1: VCS, when configured properly, provide the capability of conducting backups of user level and system level information without affecting normal plant operations. [12])

5.2 Verification of backups

The offered solution meets basic enhancement requirement of offering automated verification of backups entirely.

([1], chapter 11.5.3: Version control provides the capability of verification of the reliability of backup mechanism through automatic comparison of new backups with previous versions [12])

5.3 Monitoring of backup events

The offered solution meets supplement Guidance on the monitoring of automated backup solution entirely.

([1], chapter 11.5.2: Version Control provides the capability of providing information required for post incident forensic activity, as all actions taken with backup system are logged and made available for SIEM [12])

5.4 Encryption of backups

The offered solution partially meets Supplement Guidance on encryption

([1], chapter 11.5.2: according to this supplement guidance, encryption of backup information is not a requirement of security level 3 but the capability shall be available in case backup data contain confidential information. Version Control System alone will not offer capability of encrypting backup information but the offered solution can be integrated with conventional backup systems, like Acronis [12] which offer encryption of data in rest).

The findings of this paper are, that in the future, it is feasible to increase the security levels of power network substations and improve the resilience of power distribution, against cyber-attacks, through the use of Version Control Systems (VCS), as automated backup systems.

References

[1] ISA/ ANSI-62443-3 3-2013, Security for industrial automation and control systems, Edition 1.0 2020-06 Part 3 3 System Security Requirements and Security Levels

[2] 2022 S&P Global Energy Security Sentinel https://www.spglobal.com/energy/en/news-research/latest-news/electric-power/101022-energy-security-sentinel-cyberattacks-surge-in-2022-as-hackers-target-commodities

[3] Marc J. Rochkind: A Retrospective on the Source Code Control System. IEEE Transactions on Software Engineering, 25 January 2025, https://ieeexplore.ieee.org/abstract/document/10821013

[4] ISA-ENSI 62443-1-1, Security for industrial automation and control systems, Edition 1.0 2007 Part 1 1 Terminology, Concepts and Models

[5] Jianping Zhan, Hongmin Li: Research and Implementation of a Data Backup and Recovery System for Important Business Areas., IEEE Xplore, 26-27 August 2017, https://ieeexplore.ieee.org/abstract/document/8048193

[6] André Luis Franceschett, Paulo R.A. de Souza, Fábio L. Pereira de Barros,: A Holistic Approach - How to Achieve the State-of-art in Cyber security for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard, IEEE PES Smart Grid initiative, 2019 https://ieeexplore.ieee.org/abstract/document/8895368

[7] P1402/D11, Jun 2021 - IEEE Draft Guide for Physical Security of Electric Power Substations, IEEE

[8] ANSI/ISA 62443-2-1 (99.02.01)-2009

[9] Abolfozl Rahiminejad, Jordan Plotnek, Ribal Attalah, Marc-Andre Dubois,: A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations. JEPE 2023, https://www.researchgate.net/publication/363916148_A_resilience-based_recovery_scheme_for_smart_grid_restoration_following_cyberattacks_to_substations

[10] Robert M. Lee, SANS Michael J. Assante, Tim Conway, SANS, Analysis of the Cyber Attack on the Ukrainian Power Grid, E-ISAC, 2016, http://www.sherpain.net/SW_upload_file/SW_qna/a615bde86d160330091226.pdf (downloaded: 15. December 2025)

[11] Laura Hartmann, Steffen Wendzel: Detection of Anomalous Values within TIA Project Data History for Industrial Control Systems. ACM Digital library, November 2021, https://dl.acm.org/doi/abs/10.1145/3487405.3487662(viewed: 15. December 2025)

[12] Jon Westfall: Basics of Backups and Version Control, Springer Nature, April 2021. https://link.springer.com/chapter/10.1007/978-1-4842-6966-4_6 (accessed: 15. December 2025)

[13] Marcus Geiger, Michael Masuch: An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems, 2020, IEEE, https://scholar.google.com/scholar?hl=hu&as_sdt=0%2C5&q=Marcus+Geiger%2C+Michael+Masuch%3A+An+Analysis+of+Black+Energy+3%2C+Crashoverride%2C+and+Trisis%2C+Three+Malware+Approaches+Targeting+Operational+Technology+Systems%2C+2020%2C+IEEE&btnG=, (downloaded: 15. December 2025)

[14] Paul W. Parfomak: Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations, Congressional Research Service, 2014, https://www.congress.gov/crs-product/R43604 (downloaded: 16. December 2025)

[15] Tereza Pultarova: Cyber security - Ukraine grid hack is wake-up call for network operators, Engineering and Technology, (Volume: 11, February 2016), https://ieeexplore.ieee.org/abstract/document/7592621 (downloaded: 16. December 2025)

[16] Dimitrios Serpanos, Theodoros Komninos: The Cyberwarfare in Ukraine, July 2022, Computer, (Volume: 55, Issue: 7, July 2022) https://ieeexplore.ieee.org/abstract/document/9810126 (downloaded: 17. December 2025)

[17] Tejasvi Alladi, Vinay Chamola, Sherali Zeadally: Industrial Control Systems: Cyberattack trends and countermeasures, Computer Communications, Volume 155, 1 April 2020, Pages 1-8 https://www.sciencedirect.com/science/article/abs/pii/S0140366419319991 (downloaded: 19. December 2025)

[18] Fatiha Djebbar et al: A Comparative Analysis of Industrial Cybersecurity Standards, In: IEEE Access, January 2023. https://scholar.google.com/scholar?hl=hu&as_sdt=0%2C5&q=Fatiha+Djebbar+et+al%3A+A+Comparative+Analysis+of+Industrial+Cybersecurity+Standards&btnG= (downloaded: 23. December 2025)

[19] Wang Ruoting: CSG Completes Its First 500kV Transformer Substation with Unmanned Operation, Inspection System, http://en.sasac.gov.cn/2020/10/02/c_10743.htm, (downloaded: 22. December 2025)