WHITE PAPER

A Systematic Approach to Checking Cybersecurity for Critical Infrastructures Including IEC-61850 Power Substations That Conform to ISA / IEC 62443

Felipe Sabino Costa
Moxa Brazil Tecnologia.
São Paulo, SP

ABSTRACT

Although cybersecurity has already been discussed for many years, it is only recently that proper attention has been given to cybersecurity in industrial environments, including manufacturing and power generation. This is partly due to the increasing number of cyberthreats in industrial environments and also due to the fact that automation systems are expanding. Within this context, a number of standards have been discussed, among them ISA / IEC 62443, which is often used in critical infrastructures. When trying to secure network assets, a long and often complex list of configurations have to be performed, to ensure industrial control systems have the appropriate cyberprotection. This paper will present a systematic and automatic approach to those security configurations, with a focus on network assets, which aim to decrease the probability of implementing incorrect or incomplete configurations that can occur when configurations are performed manually.

INTRODUCTION

In recent years, there has been an increasing number of cyberattacks on critical industrial sectors/infrastructures including energy, water treatment, hospitals, and transportation. As all of these sectors require electricity, power generation is vital for the sovereignty of any country, which unfortunately makes it one of the priority targets of cyberattacks (ICS-CERT, 2017).

The implementation of cybersecurity should take a holistic approach, encompassing the pillars that IEC lists as: 'People, processes and technologies', where each aspect has equal priority and relevance (IEC, 2018). This paper will focus on the technical aspect of cybersecurity and the technologies that can be utilized to secure network infrastructure assets. A systematic and automatic configuration approach will be proposed to help avoid human error by verifying the existing functionalities of each device connected to a given network, in accordance with IEC 62443 section 4 for security level 2 'two' (SL-2) (IEC 62443-4-2).

THE NORMATIVE APPROACH

Recent studies have shown that the best approach to protect critical infrastructures, from a regulatory perspective, is by using a hybrid adoption of standards (vertical and horizontal). Horizontal standards are characterized by a broader and more flexible spectrum, such as ISA / IEC 62443, and can be applied to a wide variety of critical infrastructures. The vertical standards focus on a specific sector, such as NERC CIP, for the electrical sector (IEC, 2018). This recommendation is based on the fact that applying both types of standards brings greater

Released on May 15, 2020

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 57 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®

procedural robustness to the overall cybersecurity solution. As each normative system focuses on the more specific parts of their standards, their approaches tend to complement each other rather than oppose, bringing a highly multifocal approach to the process.

As different companies have different levels of maturity regarding their implementation of cybersecurity (ARC, 2019), it is challenging to recommend a singular approach that fits all of them. But it is reasonable to start the normative process structure with the horizontal standards and then complement them with the vertical standards that are specific to each sector. Neither approach is more efficient than the other, but both are equally necessary and complementary (IEC, 2018).

Based on this approach, we intend to present the ISA / IEC 62443 set of standards hereinafter referred to as 'standard' as an applicable cybersecurity guide to any critical industrial process. Included in section 4 of the standard are lists of good practices and requirements to which components must adhere. There are different levels of complexity defined by different 'security levels', which detail the level of resilience the components would be able to offer in the event of a cyberattack.

Each security level has a clear definition of the skills, motivations, intentions, and resources that the level is able to protect. Assuming that the standard already presents best practices for predetermined levels, the automatic security verification system presented in this paper, is based on the parameters elaborated by it. Security level 2 "two" (SL-2) was defined as the minimum requirement for critical infrastructure, and is capable of handling the simplest and most common intrusion attempts including brute force, network scanning, and weak authentication, among others, by associating these features with a graphical interface.

Additionally, more sophisticated attacks, considered as higher levels (levels 3 and 4 that represent 'terrorism' and 'nation attacks' respectively), require a much greater combination of resources (software and hardware) as well as a much longer development time.

THE IMPORTANCE OF SYSTEMATIZATION

The use of a systematic and mainly automatic approach to implement configurations is essential to ensure uniformity and, more importantly, a consistent and reliable repeatability of the configurations. This approach aims to reduce human interference during this process, as the human factor is considered a major cause of cyberincidents regardless of whether they are intentional or not (ICS-CERT, 2017).

Performing configurations automatically becomes even more important in repetitive activities, as human beings generally tend to make more mistakes on this type of process (Dekker, 2017). Thus, the aim is to ensure that manual configurations are performed only when absolutely necessary as this will significantly reduce the possibility of mistakes. Furthermore, the personnel that set the security of each device should have the correct technical ability to ensure the settings are performed appropriately. Ensuring personnel have the correct level of expertise will reduce the possibility of the configurations being performed inaccurately.

Further compounding this problem is the fact that vulnerabilities caused by human error are difficult to detect, because the detection often relies on the audit process that the company has implemented, which may not be 100% reliable. This type of problem tends to be exponentially greater if the audit processes are purely manual (Dekker, 2017). However, unfortunately, there is sometimes a deliberate attempt from an employee to sabotage a network. Whether it is performed by accident or on purpose, both are referred to as insider threats. (Adams, M; Makramalla, M, 2015) It is therefore crucial that the cybersecurity measures must also be able to identify and prevent those with malicious intent being able to disrupt normal operations.

It is important to give attention to not only the methodologies themselves, i.e. 'what to implement', but also to the way in which they are implemented, 'the how'. By taking a systematic and automatic approach to implement the configurations, these risks can be considerably reduced, which increases the reliability and security of the networks.

Although this paper presents many arguments that support implementing an automatic and systematic approach as opposed to an approach that relies solely on humans, it does not mean that humans should be removed from the process altogether. Instead, the idea is to find the optimum point of interaction between technology and humans.

THE REFERRAL LIST

The first section of the standard (IEC 62443-1-1) introduces seven fundamental requirements for cybersecurity which are: Identification and Authentication control, Use Control, System Integrity, Data Confidentiality, Restricted data flow, Timely response to events, and Resource Availability.

In addition, the standard also sets out some system requirements and suitability for each security level. Higher levels of security will require more features and configurations with high levels of complexity. Similarly, for lower levels, less features will be required. Therefore, the security levels (SLs) established by the standard must have their requirements implemented differently to achieve their objectives. Annex B of IEC 62443-3-3 shows a clear relationship between requirements and security levels, allowing the creation of a fully auditable list for each piece of equipment for each security level.

THE HUMAN FACTOR

A systematic configuration and verification system aims to defend automation systems against the types of threats defined by the standard, but it has other advantages as well.

As previously mentioned, an extremely important issue is how humans can introduce vulnerabilities to automation systems. The main vulnerabilities are as follows: Configuration process (execution only), decision-making process (cognitive decisions), and hybrid process (a combination of decisions and execution).

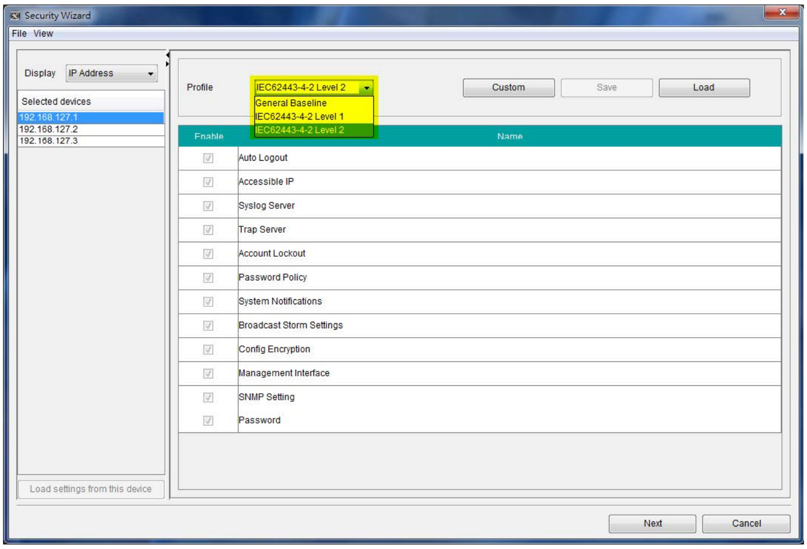
Decisions are necessary when implementing cybersecurity measures. Even neuroscience itself is unclear how decision-making processes and interactions occur within the human brain, but it is generally understood that performing processes of different complexity produce different intensities of effort within the human brain (HR Heekeren et al., 2004). Therefore, all deployment of cybersecurity measures must also take into account the dynamics of the human brain in decision-making.

This paper will now briefly consider how humans interact with automation cybersecurity systems and consider the difficulties that can arise.

THE DECISION-MAKING LEVEL

Within the context of this paper, ‘decision-making’ means something that the standard leaves for an operator to choose. It often involves complex decisions that only the user is able to determine. In this sense, the systematic configuration and verification system should support the user, but does not decide on behalf of the user. It should assist the user to implement their decisions easily, without compromising or influencing their decision-making process.

An important concept introduced in IEC 62443-1 that requires decision-making is, security zones, where equipment within the same zone must be protected by the same ‘achieved security level’ (SL-A where ‘achieved’ denotes the protection of an asset or zone). However, this does not mean that all zones must have the same security level. For this reason, it is necessary to have the flexibility to allow lower or even customizable levels of security (see figure 1).



Display: IP Address

Selected devices
192.168.127.1
192.168.127.2
192.168.127.3

Profile: IEC62443-4-2 Level 2
General Baseline
IEC62443-4-2 Level 1
IEC62443-4-2 Level 2

Enable	Name
☑	Auto Logout
☑	Accessible IP
☑	Syslog Server
☑	Trap Server
☑	Account Lockout
☑	Password Policy
☑	System Notifications
☑	Broadcast Storm Settings
☑	Config Encryption
☑	Management Interface
☑	SNMP Setting
☑	Password

Figure 1. List of objective functionalities to be audited (Moxa, 2019)

The security level required for an asset or zone and the decision whether or not to apply specific security settings to an existing process is determined by the asset owner. The owner can measure and understand the applicability and impact of each configuration to the system.

It is essential to highlight that the implementation of these functionalities in a production system, even if recommended by the standard, must be evaluated through an appropriate risk assessment and its impact to the current system operation should be evaluated. The result of this is that no implementation is performed automatically without the user's consent.

SOFTWARE-AIDED IMPLEMENTATION

Compared to the decision-making process, the configuration process tends to be simpler, but as mentioned earlier, this process has other difficulties, such as the repeatability and complexity of certain types of configurations that can lead to human error. The configuration process mentioned in this paper is defined as the implementation of the technical policies and does not require any decision-making processes, only the execution tasks.

The list available in Annex B of IEC 62443-3-3 is the basis for the security verification system. It allows users to compare without subjectivity whether the audited equipment is correctly configured or not.

By conducting a network scan and comparing current settings with desired ones, deliberate or unintentional acts that compromise cybersecurity settings are resolved, ensuring uniform security within the zone. As zone security is defined by its weakest link, it is therefore of the utmost importance that all equipment in the same zone has the same protections.

Additionally, this feature assists an automatic system audit, where even if the user has made a mistake, a new audit can be performed quickly to find the vulnerability. In this respect, the ‘pillar of the process’ is critical, as it determines the duration of time that system audits should be performed. It is important to mention, that any verification or changing on production systems should be evaluated and tested prior to implementation.

Using Images Rather Than Lists

One of the most efficient ways to support the security checking process without compromising user judgment is to use graphical representations rather than lists to identify equipment on networks. It has been acknowledged for a long time that the human brain processes images and words differently (Potter, 1976) and that, despite having many similar cognitive processes, images and words end up having different processing times (Ganis G, Kutas M, Sereno Martin, 1996). In short, images are processed faster and are easier to recognize by the human brain. Therefore, using graphical representations helps quicken the identification of the security settings of each device, as shown in Figure 2.

Using Colors

The second point that we will consider is color differentiation to highlight different levels of security. The human brain can easily recognize different color tones (Engel S, Zhang X, Wandell B, 1997), which means that different colors can be used to offer the user a quick identification of the security status of each device and inform them of possible actions that have to be taken. Due to the importance of this, a color palette should be selected that ensures that color blind people can differentiate between the colors.

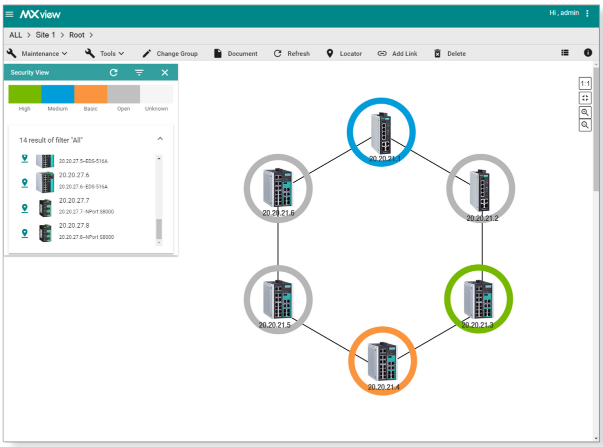
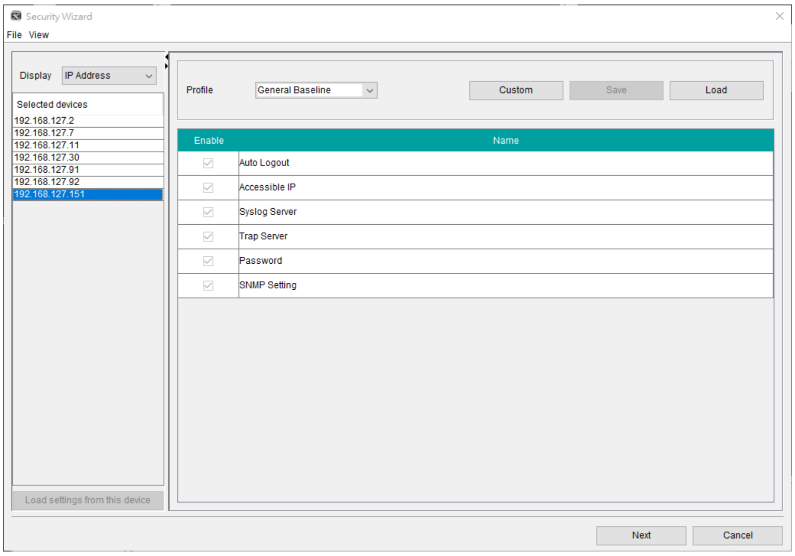


Figure 2. Graphical architecture with color system security status

CONFIGURATION LEVEL

When the security verification system scans and finds a mismatch between the settings recommended by the standard and the current ones deployed, the user will need to make a decision on how to proceed. If a mismatch is found, it is likely to be due to one of two reasons.

In the first scenario, the user identifies which suggestions can be implemented, authorizing the system to perform the update, assuming that the equipment is capable of performing the update, represented in figure 3.



Display: IP Address

Selected devices
192.168.127.2
192.168.127.7
192.168.127.11
192.168.127.30
192.168.127.91
192.168.127.92
192.168.127.151

Profile: General Baseline

Enable	Name
☑	Auto Logout
☑	Accessible IP
☑	Syslog Server
☑	Trap Server
☑	Password
☑	SNMP Setting

Figure 3. Checkboxes indicate which features are available/enabled (Moxa, 2019)

In the second scenario, when a mismatch is noted, the equipment does not have these features and capabilities. In this scenario a risk assessment should be performed to assess whether or not the system can remain with these vulnerabilities or whether there are measures to counteract them. Regardless of these scenarios, it is important that where possible, the user implements the required minimum security functionalities discussed by the standard so that the zone to which it belongs is secure.

CONCLUSION

It has been presented that systematic and automatic methods are more reliable especially compared to repetitive and manual processes, when performing cybersecurity settings. Because it is such a sensitive and important issue for industries, it is essential that all existing cybersecurity features are implemented correctly.

A security verification system should not be seen as the sole resource to ensure appropriate cybersecurity implementation, as cybersecurity is complex and requires a multifocal approach. However, a security verification system can assist those responsible for implementing cybersecurity by helping them to objectively implement the requirements recommended by the standard. This approach aims to avoid the problems that occur when there is too much reliance on humans performing the security settings.

REFERENCES

1. “Cybersecurity Maturity Model,” ARC, Advisory Group, 2019. https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model
2. “The Field Guide to Understanding 'Human Error',” Sidney Dekker, 2017. http://leonardo-in-flight.nl/PDF/FieldGuide%20to%20Human%20Error.PDF
3. “The Search for “Common Sense”: An Electrophysiological Study of the Comprehension of Words and Pictures in Reading,” Giorgio Ganis, Marta Kutas and Martin I. Sereno, 1996. http://www-cogsci.ucsd.edu/~coulson/cogs179/ganis96.pdf
4. “A general mechanism for perceptual decision-making in the human brain,” H. R. Heekeren et al, 2004. https://www.nature.com/articles/nature02966
5. “IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program,” International Electrotechnical Commission, 2010.
6. “IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers,” International Electrotechnical Commission, 2015.
7. “IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels,” International Electrotechnical Commission, 2013.
8. “IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements,” International Electrotechnical Commission, 2018.
9. “IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components,” International Electrotechnical Commission, 2019.
10. “IEC Cyber security Brochure overview,” International Electrotechnical Commission, 2018. https://www.iec.ch/cybersecurity/?ref=extfooter

11. "IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment," International Electrotechnical Commission, 2015.

12. "IEC TR 62443-3-1:2009 industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems," International Electrotechnical Commission, 2009.

13. "IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models," International Electrotechnical Commission, 2009.

14. "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," M Adams, M Makramalla, 2015. https://timreview.ca/article/861

15. "MXview 3.0 User's Manual," Moxa Inc., 2019. https://www.moxa.com/Moxa/media/PDIM/S100000150/moxa-mxview-series-manual-v1.1.pdf

16. "NCCIC. ICS-CERT Annual Assessment Report," US Department of Homeland Security CISA Cyber + Infrastructure, 2017. https://ics-cert.us-cert.gov/Other-Reports

17. "Short-term conceptual memory for pictures. Journal of Experimental Psychology: Human Learning and Memory, 2(5), 509-522," Mary C. Potter, 1976. https://psycnet.apa.org/record/1976-29232-001

18. "Colour tuning in human visual cortex measured with functional magnetic resonance imaging," Stephen Engel et al, 1997. http://invibe.net/biblio_database_dyva/woda/data/att/f903.file.pdf

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.