Adopting International Standards in Africa to Protect Critical Infrastructure

The digitally interconnected world has immense potential. Internet-based technologies are becoming an integral part of every critical infrastructure. The US Cybersecurity and Infrastructure Security Agency (CISA) defines critical infrastructure as assets, systems and networks, physical or virtual, that are deemed vital to nation-states, such that their compromise would have an enervating effect on security, public health or safety.[1] Examples of critical infrastructure include electricity generation and distribution systems, water and waste management systems, defense industries, and transport and traffic control systems. Traditionally, these systems operated in isolation, using mainly legacy proprietary software. The change to the use of Internet technology in critical infrastructure has many benefits, but it also entails risk and a host of vulnerabilities.

Adversaries with ever-increasing sophistication, determination and motivation see a great deal of opportunities to exploit vulnerabilities associated with the use of Internet-based technology in critical infrastructure control systems. Combating these threats and ensuring the resilience of Internet-enabled systems requires a systematic approach and robust cybersecurity standards. Cyberthreats targeted at critical infrastructure and the magnitude of the risk and the consequences of security breaches highlight why the adoption of International Society of Automation/International Electrotechnical Commission (ISA/IEC) standards could complement the initiatives already undertaken on the continent and help achieve a coherent approach and a baseline level of cybersecurity in Africa.[2]

Although these standards were predominantly developed for the industrial process sector, they have since been applied to building automation, medical devices and transportation sectors.[3]

Critical Infrastructure Adversaries

Adversaries targeting critical infrastructure are increasingly nation-states with the resources and the motivation to inflict damage on these assets. According to the ISA, the impact of these threats includes:

- Compromised national security
- Health, safety and environmental damage, including loss of life
- Unavailability of critical services
- Negative publicity
- Loss of public trust
- Theft of data

Attacks on critical infrastructure are becoming more oriented toward destroying assets rather than

```
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

Patrick Katuruza, CISA, ACS CP, CISSP, ISA/IEC 62443
Is a lead technical auditor (industrial controls systems) at Morison Menon Consulting and Advisory. He has extensive experience in industrial automation control systems (IACS) cybersecurity assurance and consulting.

> IN MOST AFRICAN COUNTRIES, GOVERNMENTS AND REGULATORS HAVE INSUFFICIENT FINANCIAL AND OTHER RESOURCES TO DEVELOP COMPREHENSIVE INFORMATION SECURITY STANDARDS.

making money.[4] Several cyberattacks involving critical national infrastructure illustrate the gravity of these threats and the magnitude of their potential impact:

- **Stuxnet**—This malware was first discovered in January 2010 at the Iranian Nantaz nuclear facility. Believed to have been in development since at least 2005, Stuxnet targets supervisory control and data acquisition (SCADA) systems and is thought to be responsible for damaging centrifuges used in uranium enrichment. Stuxnet has been dubbed the world's first digital weapon.[5]
- **Shamoon**—This virus was discovered in 2012. The first attack was newsworthy due to its destructive nature and the cost of restoring systems. Shamoon can spread from one infected machine to others on the network. The virus can compile a list of files from specific locations on the system, upload them to the attacker and erase them. It can also overwrite the boot records of the infected machine, effectively making it unusable. Adversaries used Shamoon to wipe data from 30,000 computer workstations at Saudi Aramco, and it is believed that a different version of the virus was used against Qatar's Ras Gas.[6] Generally, attacks of this nature keep recurring at slightly different levels of sophistication.
- **Ransomware attack at Norsk Hydro**—On 19 March 2019, Hydro, a global player in the mining and metals sector, was hit by an extensive cyberattack that affected all business operations. Although the extent of the damage to these operations differed, the cost of the attack was estimated to be somewhere between US$46 million and US$52 million.[7]
- **Life Healthcare security breach**—Life Healthcare is a healthcare provider with operations in South Africa and Botswana. On 9 June 2020, the organization reported that it had been hit by a cyberattack. The attack impacted admissions systems, business processing systems and email servers. Although no technical details were made available to the public on how the attack was launched, the case highlights the threats posed by cyberattacks on critical infrastructure on the African continent.[8]

Combating Threats in Africa

Given the significance of the threats and the magnitude of the impact of cybersecurity breaches, it is imperative that African countries strengthen their abilities to prevent, detect and respond to such incidents. These capabilities can be developed through a consistent, credible and coherent set of standards implemented holistically, with other strategic initiatives such as training and awareness.

Although some governments in African nations are starting to develop legislative frameworks related to cybercrime and cyberthreats, most African countries do not have national cybersecurity standards to guide their efforts in protecting nationally significant information networks and systems. According to a report by the International Telecommunications Union (ITU), only eight of 44 African countries have standards or frameworks for cybersecurity implementations. African countries that have made strides in developing and adopting standards include Kenya, Mauritius, Rwanda and South Africa.[9]

The development of standards can be a long process, taking years in some cases. This process requires significant investments in money, time and expertise. In most African countries, governments and regulators have insufficient financial and other resources to develop comprehensive information security standards. Therefore, the adoption of ISA/IEC 62443 standards can help governments and private-sector enterprises by providing security baselines and reference frameworks at a much lower cost.

The African continent has undergone significant knowledge loss as skilled professionals, including information security personnel, have migrated overseas in search of better working conditions. A

2016 research study by the Department of Electrical and Computer Engineering at Carnegie Mellon University Africa (Kigali, Rwanda) found that there are approximately 7,000 qualified information security professionals for the entire continent's population of 1.34 billion.[10] Countries in Africa can leverage ISA standards to bridge the skills gap as guidelines are developed, drawing on the consensus and expertise of practitioners from all over the world. ISA/IEC standards have been adopted widely across the world. The United Nations Economic Commission for Europe (UNECE) confirmed that ISA/IEC standards will be integrated in the Common Regulatory Framework on Cybersecurity (CRF). The CRF serves as an official UN policy position statement for Europe. The CRF serves to establish a common legislative basis for cybersecurity practices within the EU trade markets.[11] ISA/IEC 62443 standards have been adopted in Asia, Europe, Latin America, the Middle East and North America. In the Middle East, countries such as Qatar have used the standards to develop their own national AI industrial control systems security standards.[12]

> “THE ISA/IEC 62443 FAMILY OF STANDARDS CAN HELP ORGANIZATIONS DEVELOP ROBUST CSMS, AS THEY OFFER MORE GRANULAR GUIDELINES AS COMPARED TO OTHER STANDARDS ON CYBERSECURITY.”

Recently, a group of 40 enterprises from across the globe (ISA Global Cybersecurity Alliance) came together to increase industrial cybersecurity awareness and readiness by developing and implementing best practices from ISA 62443 standards. These enterprises include KPMG, Honeywell, Johnson Controls, Rockwell Automation and Schneider Electric.[13]

Benefits of ISA/IEC Standards

ISA/IEC standards provide a flexible framework that can be applied in a wide range of industrial control system (ICS) environments, regardless of the technology used. These standards also address current and future information security vulnerabilities. There are other standards, such as International Organization for Standardization (ISO) 27000, that address various aspects of cybersecurity; however, these standards have not been designed to address the safety, integrity, reliability and security of industrial automation control systems (IACSs). This is mainly because the consequences of a successful cyberattack on an IACS are principally different. The key implications of a successful cyberattack on IT systems is generally financial and privacy loss due to information disclosure. Conversely, the implications for an IACS may also include loss of life or health, damage to the environment, or loss of product integrity.[14]

The ISA/IEC 62443 family of standards can help organizations develop robust cybersecurity management systems (CSMS), as they offer more granular guidelines as compared to other standards on cybersecurity. ISA/IEC 62443-3-3 System Security Requirements and Security Levels sets out detailed guidelines for defining systems security requirements and security levels. It defines the following seven IACS foundational security requirements:

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

For each of these IACS security requirements, the standard defines three security levels: target security level, achieved security level and capability security level. Organizations can leverage the standard to evaluate their existing security posture, define target security levels for each foundational security requirement and assess the security capability of their technology deployments throughout their life cycles.

Another key benefit of adopting ISA 62443 standards is that controls imbedded in the documents can be mapped to other frameworks, such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This is important for entities that have adopted the CSF for their IT systems and 62443 for operational technology environments. The ability to map key controls eliminates unnecessary duplication while demonstrating compliance with both standards and frameworks.

ISA standards provide a common taxonomy and language for product suppliers. Africa has experienced a proliferation of various ICS devices from vendors in China, Europe and the United States. Considering the global reach of supply chains and the differences in technology providers' standards, African countries can benefit by embracing standards such as ISA 62443-4-1 *Secure Product Development Life Cycle*,[15] because many countries have not yet set stringent specifications for devices used in their critical infrastructures. The ISA/IEC 62443-4-1 standard can be used by organizations in developing invitations to tender (ITT) documents, developing vendor technical evaluation criteria for IACS tenders and assessing bids.

Conclusion

The risk of cyberattacks on critical infrastructure is increasing exponentially with advances in operational technologies. The intensity of the threats and the consequences of security breaches have far-reaching ramifications for organizations and the communities that depend on those organizations. IACS cybersecurity practitioners should advocate for the adoption and holistic implementation of critical infrastructure cybersecurity standards such as ISA/IEC standards, along with other initiatives such as awareness and training to help organizations build resilience.

Endnotes

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," *https://www.cisa.gov/critical-infrastructure-sectors*

[2] International Society of Automation (ISA), "ISA Standards," *https://www.isa.org/standards-and-publications/isa-standards*

[3] International Society of Automation (ISA) Global Cybersecurity Alliance, *Quick Start Guide: An Overview of ISA/IEC 62443 Standards*, June 2020, *https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf?utm_campaign=ISAGCA%20Communications&utm_medium=email&_hsmi=85876950&_hsenc=p2ANqtz-8EWeH7LBuH_w4FPYDqssxo0DFrM1GMh6zf0DFZSJ7dbscZt3q8oaUO_Td0c7cttSGvb5QDZqZxdW5ZFKZTqYr25jb6eDZItoisg6rQjkwX3TXpo4M&utm_content=85876950&utm_source=hs_automation*

[4] Lohrmann, D.; "How Vulnerable Is Critical Infrastructure to a Cyberattack?" Government Technology, 23 October 2020, *https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-vulnerable-is-critical-infrastructure-to-a-cyberattack.html*

[5] Zetter, K.; "Countdown to Zero-Day Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014, *https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/*

[6] Brewster, T.; "Warnings as Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry," *Forbes*, 13 December 2018, *https://www.forbes.com/sites/thomasbrewster/2018/12/13/warnings-as-destructive-shamoon-cyber-attacks-hit-middle-east-energy-industry/?sh=828d2323e0fd*

[7] Hydro, "Cyber-Attack on Hydro," 2019, *https://www.hydro.com/en/media/on-the-agenda/cyber-attack/*

[8] Reuters, "South Africa's Life Healthcare Hit by Cyber Attack," 9 June 2020, *https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY*

[9] International Telecommunication Union (ITU), *Global Cybersecurity Index 2017: Africa Report*, Switzerland, 2017, *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_GCIv2_report.pdf*

[10] Adomoko, K.; N. Mohamed; A. A. Garba; M. Saint; "Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index," *SSRN Electronic Journal*, 2018

[11] Intrado Global Newswire, "United Nations Commission to Integrate ISA Standards Into Cybersecurity Regulatory Framework," 8 January 2019, *https://www.globenews*

wire.com/news-release/2019/01/08/1682362/0/en/United-Nations-commission-to-integrate-ISA-standards-into-cybersecurity-regulatory-framework.html

[12] Qatar National Information Assurance, *Qatar National ICS Security Standard*, Qatar, January 2013, *https://www.motc.gov.qa/sites/default/files/documents/National%20Industrial%20Control%20Systems%20Security%20Standard-English.pdf*

[13] Basset, R.; “Cybersecurity Standards Hit Their Stride,” International Society of Automation, *InTech*, November–December 2020, *https://www.isa.org/intech-home/2020/november-december-2020/columns/cybersecurity-standards-hit-their-stride*

[14] *Op cit* ISA Standards

[15] Arampatzis, A.; “What Is the ISA/IEC 62443 Framework?” *The State of Security*, 10 September 2019, *https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/*