8TH SOUTHERN AFRICA REGIONAL CONFERENCE

14 - 17 NOVEMBER 2017

"**Electricity Supply to Africa and Developing Economies …. Challenges and opportunities."**

Preferential Topic: No.3 – Planning for the Future in Uncertain Times

Network and Data Security Strategy of the Electric Power System

M Taljaard

Eskom

South Africa

Summary

This paper discusses the strategy of interconnecting the Operational Technology Environment and Information Technology Environment with a focus of cybersecurity for an electric power utility. This paper introduces the concept of "secure areas" and how these can be used to prevent the propagation of cybersecurity threats and allow co-existence with other networks. The concept of an overarching integrated security operating centre and how it can integrate with the above mentioned environments is also addressed.

Keywords

Cybersecurity; Operational Technology; Information Technology; Integrated Security Operating Centre; Secure Area; Electric Power Utility; Information and Communication Technology; Smart Grid

The operational network of the electric power utility (EPU) [1] (Ericsson, 2007) is no longer in isolation from the rest of the organisational network and the systems the support the business. The technological move to an interconnected network is necessary. Interconnectivity promotes both business intelligence and financial gains. The biggest concern for the operational network however, is the cybersecurity of this new interconnected network.

The EPU's are now challenged to co-exist with four role-players, namely:

1. Operational Technology (OT) network which monitor and operate the power grid;
2. Information Technology (IT) network which describe the entire spectrum of technologies used for corporate information and;
3. Integrated Security Operations Centre (ISOC) [2] (Electric Power Research Institute, 2013) network which monitor the cybersecurity and physical security of the entire business.
4. Internal EPU Telecommunications which provide the internal Wide Area Network (WAN) telecommunications for the EPU.

Co-existing is a challenge because OT has priorities that are in order of Availability, Integrity and Confidentiality where IT and Security has the reverse in order of Confidentiality, Integrity and Availability [3]. OT therefore accepts cybersecurity as a lower priority to the availability of the system and interconnecting current systems in their current state is a dangerous risk. The requirement on availability required by OT can encourage an EPU to host their own internal WAN.

The internal EPU WAN is seen as a highly available but untrusted network for the EPU that should provide telecommunications to the business as a whole. Therefore, OT, IT and ISOC are seen as customers. If OT was to use an IT hosted system for OT operations, there would be an expectation of high availability. However, IT's top priority is Confidentiality and this will affect the expected availability for OT operations.

A strategy is therefore required on how ISOC, IT, Internal EPU Telecommunications and OT will co-exist taking cybersecurity into the design.

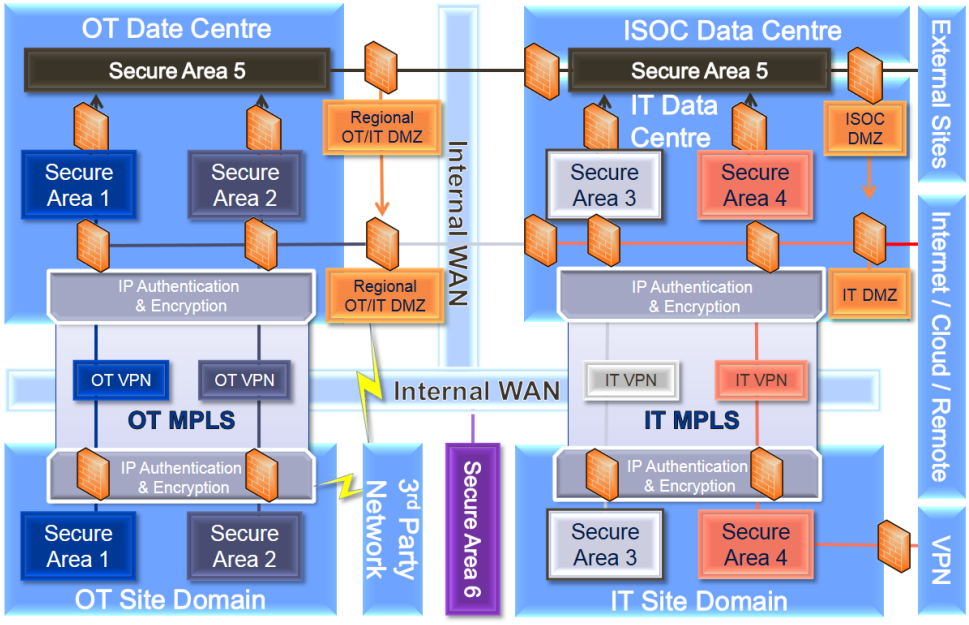

Figure 1 : The Information Security Strategy of an Interconnected EPU Network

Figure 1 shows the combined view of an interconnected EPU network strategy. The network has multiple secure areas [4] that separate the data on the network based on their criticality to the business. The secure areas are separated and accomplished through a security insulation technique. This could be done by using:

1. Physical Insulation – No physical access and access is granted on request.
2. Protocol Insulation – Using a different protocol to prevent communication from leaving the area until a convert is used.
3. Firewall Insulation – Creating a barrier with rule sets to control flow of communications between secure areas.

Secure Areas from a cybersecurity perspective are intended to prevent cyber threats from propagating from one secure area, to the next. The OT area is recommended to be divided into two Secure Areas namely:

Secure Area 1 – Critical OT Services: Secure Area 1 is dedicated to services that directly impact the control, monitoring and operations of the power system.

Secure Area 2 – Non-Critical OT Services: Secure Area 2 is dedicated to services that support the OT.

It is likely there will be connections leaving Secure Area 2 to a Demilitarized Zone (DMZ) and separating internally to OT reduces the risks of critical services from being compromised.

The secure areas are shown to traverse the internal WAN. The internal WAN is comprised of a shared physical transport infrastructure with physically separate Multiprotocol Label Switching (MPLS) networks.

Where the internal WAN is not available, a 3rd party network is utilized. The drawbacks of using a 3rd party network for OT services are that availability and latency for OT services are at risk and cybersecurity must be provided by OT sites. If an internal WAN is used, it is possible that cybersecurity can be provided as a service to OT sites. This is an advantage as many OT sites in utilities have legacy equipment that most likely will not support current cybersecurity requirements.

At a minimum should provide logical separation of the services in their respective secure areas. For an internal WAN, it is plausible for services to share the same physical transport infrastructure and be separated logically while maintaining a low cybersecurity risk.

All data entering or leaving the OT environment should do so via a centralised or regionally centralised DMZ. Any data going to Secure Area 1 does not go through Secure Area 2 first. All secure areas are separate. This is shown in Figure 2.

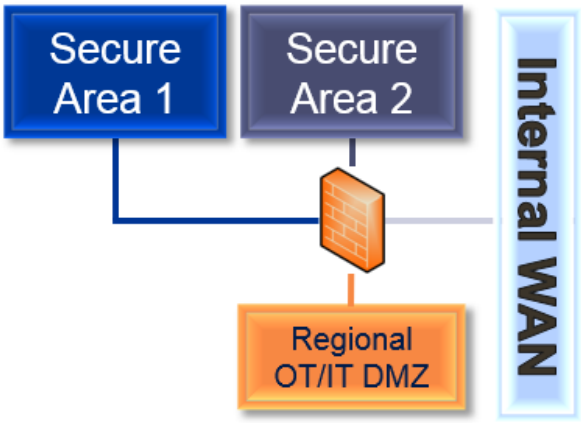

Figure 2 : Logical Connection of Secure Area 1, Secure Area 2, Regional OT/IT DMZ and Internal WAN

Having data flow through a central point makes it easier to control data in an environment. This is because only one central point requires the extensive perimeter security, both hardware and human resources, for that environment.

The 3rd party network is available for connections which is not available by the internal WAN. It can either break in at the central DMZ or be treated as a remote access connection.

The IT Environment can be split into 2 secure areas, namely:

1. Secure Area 3 – Operational Enterprise Services: dedicated for services hosted IT for OT operations. The reliance for OT on IT makes this a requirement that OT hosted services on It systems be segregated from the rest of the IT enterprise network. An agreed upon IT/OT governance will be required for services residing in this secure area.
2. Secure Area 4 – Enterprise Services: dedicated to enterprise services maintained by IT that have no impact to OT operations. Enterprise services will follow IT governance and OT will have no influence to these systems.

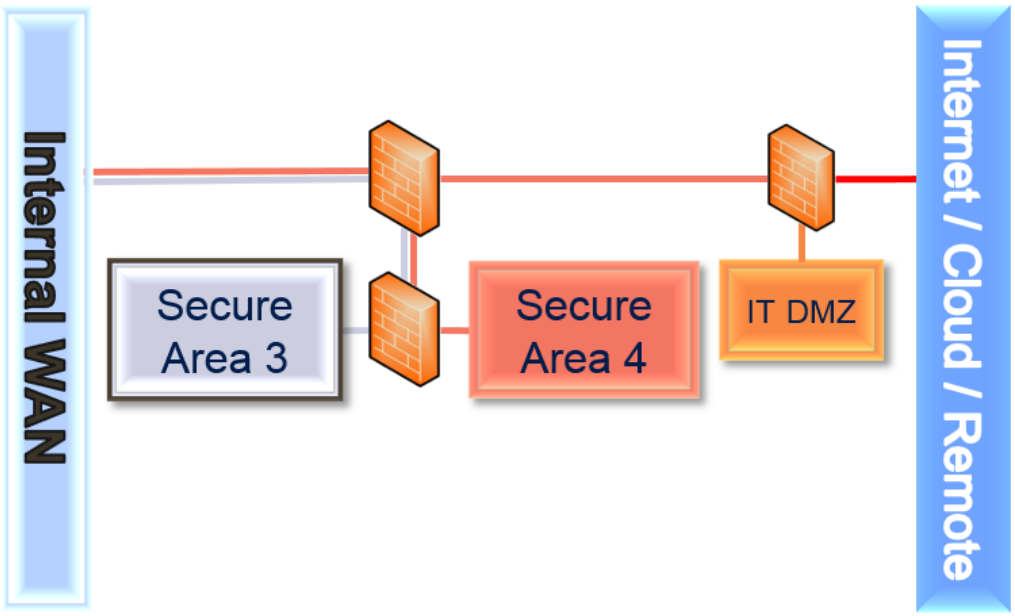

Figure 3: Logical Connection of the IT Secure Areas

Figure 3 shows the logical connection of the IT secure area. Any external connection must first pass through the IT DMZ before heading to its designated secure area, similar to the OT secure areas.

Similar to the OT secure areas, the IT secure areas will be segregated in transmission between sites. IT can use the existing internal WAN to connect sites with logical separate. IT sites can use 3rd party DSL services to connect sites that are not supported by the internal WAN.

The Secure Areas 1 and 2 and Secure Areas 3 and 4 focus on OT and IT respectively in protecting services in those environments. There is however, a lack of visibility of the overall cybersecurity of the business. Therefore, there is a requirement to have an area that monitors cybersecurity globally for the business.

“Security” has been made into a separate entity, similar to IT and OT, to establish the concept. It is possible that Security can be absorbed into either the IT or the OT environment, depending on the existing organisation, or be a separate division.

Secure Area 5 – Security: Secure Area 5 is dedicated to services controlled by ISOC. Secure Area 5 will reside in both IT and OT environments. Security incidents will be fed from Secure Area 1-4 to Secure Area 5 directly. This information will have a high data classification sensitivity rating. Declassified information from Secure Area 5 will be shared back to the secure areas via their respective DMZ. This declassified information can be used to update system owners on how the threat occurred and what preventative measures can be implemented.

Security Area 5 also could have communication to external sites. These sites are used in the collaboration of combating cyber threats which include but not limited to:

1. Agreed upon commitments with Cyber Response Committees.
2. Government organisations

Utilities in the transmission environment can lay their own fibre via methods such as overhead optical ground wire. This usually becomes part of the internal WAN mentioned in the above strategy. These lines are laid with ample bandwidth to sustain the growing bandwidth requirements of technologies expected in the utility environment [5]. This initial excess bandwidth on an internal WAN could therefore be serviced to external 3rd parties. In order for external 3rd party telecommunications can be provided, a separate secure area is required.

Secure Area 6 – External Service: Secure Area 6 is dedicated for external services that traverse the shared physical transport infrastructure of the internal WAN. An electric power utility network could provide telecommunications along with power as part of the future smart grid strategy [6][7].

Similar to IT, services that reside in Secure Area 6 will share the same physical transport infrastructure but be logically separated.

The strategy when applied together, culminates into a defence in depth approach. As data moves to a higher secure area, there must be permission that allow the data to traverse further in the network.

The strategy also give motivation for hosting and maintaining an internal WAN and gives confidence in the reliance of OT to use IT host services by means of Secure Area 3.

In the event that a breach occurs, only the affected secure area will be vulnerable and the cyber security threat should be contained in the secure area. For example, if the corporate network residing in Secure Area 4 was breach. The IT hosted OT services will not be impacted due to the secure area preventing the breach from propagating.

The added addition of an overarching security division to monitor threats throughout the business is a step in countering the cybersecurity threats of tomorrow for the power system.

BIBLIOGRAPHY

[1] Ericsson, G. N. (2007). Toward a Framework for Managing Information Security for an Electric Power Utility - CIGRE Experiences. *IEEE Transactions on Power Delivery, Vol 22, No. 3*, 1-9.

[2] Electric Power Research Institute. (2013). *Guidelines for Planning an Integrated Security Operations Center.* California.

[3] W. A. (2016). IT vs OT Security: A Time to Consider a Change in CIA to Include Resilience. *49th Hawaii International Conference on System Sciences.* Hawaii.

[4] B. W. S. Z. Yongli Zhu, "The Analysis and Design of Network and Information Security of Electric Power Systems," in *2005 IEEE/PES Transmission and Distribution Conference & Exhibition*, Asia and Pacific Dalian, China, 2005.

[5] Akamai, "Akamai's State of the Internet," 2016. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-connectivity-report.pdf. [Accessed 27 April 2017].

[6] J. Van Ooteghem, B. Lannoo, S. Verbrugge, D. Colle, M. Pickavet, P. Demeester, "Can a Synergetic Cooperation Between Telecom and Utility Network Providers Lead to a Faster Rollout of Fibre to the Home Networks?," in *IEEE*, Belgium, 2011.

[7] L. Jianming, Z. Bingzhen, Z. Zichao, "The Smart Grid Multi-Utility Services Platform Based on Power Fiber to the Home," in *IEEE*, China, 2011.