Network and Data Security Strategy of the Electric Power System

Matthew Taljaard
PTM&C Telecommunication Technology and Support,
Eskom, Group Technology, Power Delivery Engineering.
Johannesburg, South Africa
TaljaaMM@eskom.co.za

***Abstract*— 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 center and how it can integrate with the above mentioned environments is also addressed.**

***Index Terms*-- Cybersecurity; Operational Technology; Information Technology; Integrated Security Operating Centre; Secure Area; Electric Power Utility; Information and Communication Technology; Smart Grid.**

I. INTRODUCTION *(HEADING 1)*

The operational network of the electric power utility (EPU) [1] is no longer in isolation from the rest of the organizational 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.

II. THE FOUR KEY ROLE PLAYERS

The EPUs are now challenged to co-exist with the four role-players, namely:

A. Operational Technology (OT)

The network which control, monitor and operate the power grid.

B. Information Technlogy (IT)

The network which describes the entire spectrum of technologies used for enterprise information

C. Integrated Security Operations Centre (ISOC) [2]

The network which provides security for the entire business.

D. Internal EPU Telecommunications

The internal wide area network (WAN) for the EPU.

III. CO-EXISTANCE

Co-existing is a challenge as 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 internal OT customers such as generation, transmission and distribution sites. The internal EPU WAN can extend telecommunications to the business as a whole. Therefore, OT, IT and ISOC can be 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

IV. SECURE AREAS

A secure area [4] is a term used to secure a service both on site and in transport. Secure areas are setup in a manner that prevents propagation of a threat from one secure area to the next. It is important to plan for when a security compromise occurs as prevention alone is no longer sufficient. Secure areas encourage utilities to identify where services belong in their network and that they are correctly segregated.

Segregation of secure areas can be accomplished in the following ways [4]:

A. Physical Insulation

No physical access and access is granted on request. The industry is moving away from this method, but still viable for most critical cyber assets [5].

B. *Protocol Insulation*

A different protocol is used to prevent communication form leaving the network until a converter is applied.

C. *Firewall Insulation*

Creating a barrier with rule sets to control flow of communications between secure areas.

Traditional zoning such as an electronic security perimeter [5] or secure zone [6], stop at the site. This leaves the data to flow over an "untrusted network", regardless if that telecommunications network is internal to the business. The purpose of the secure area is to extend the security over the telecommunications portion required by the service. Therefore, the security of the data life cycle is maintained throughout the secure area. If an internal EPU network is used as the telecommunications, the term "untrusted network" could be removed as now the telecommunications is provided to meet the attributes of the secure area. A summary is shown in figure 1 below.

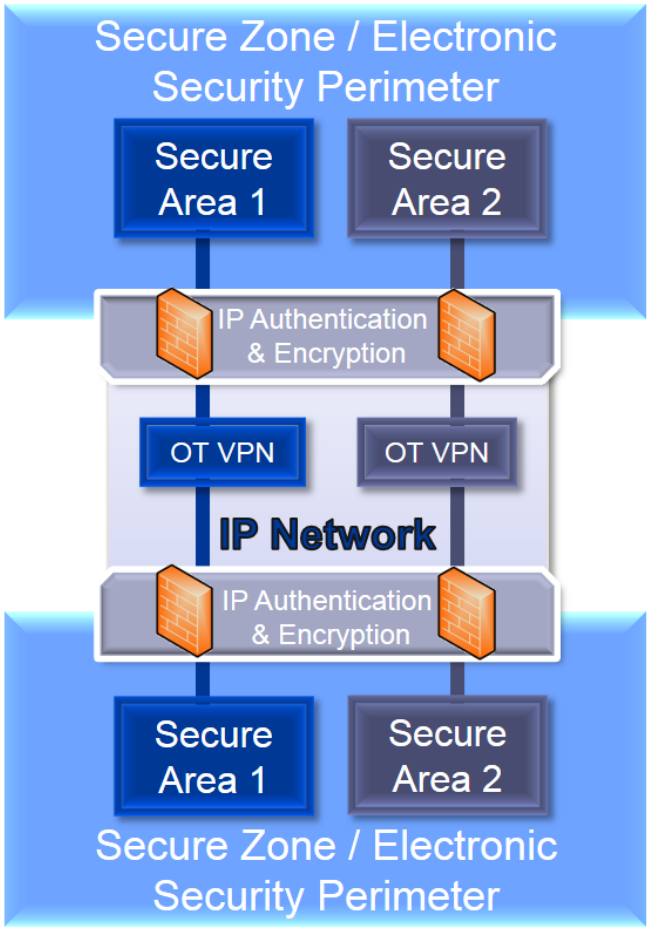

Figure 1. Example secure areas with regards to Secure Zones and Electron Security Perimeters.

V. Network and Data Security Strategy of the Electric Power System

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

Figure 3 below 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 attributes to the business. The OT area is recommended to be divided into two secure areas, namely:

A. *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 in a critical and/or real time manner.

B. *Secure Area 2 – Non-Critical OT Services*

Secure Area 2 is dedicated to services that support the OT environment. A loss of this service will not crucially result in the control, monitor or operation of the power grid.

Connection leaving a secure area will go to a demilitarized zone (DMZ) and separating internally to OT reduces the risks of propagation through the OT site.

All data entering or leaving the OT environment should do so via a centralized or regionally centralized 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 below.

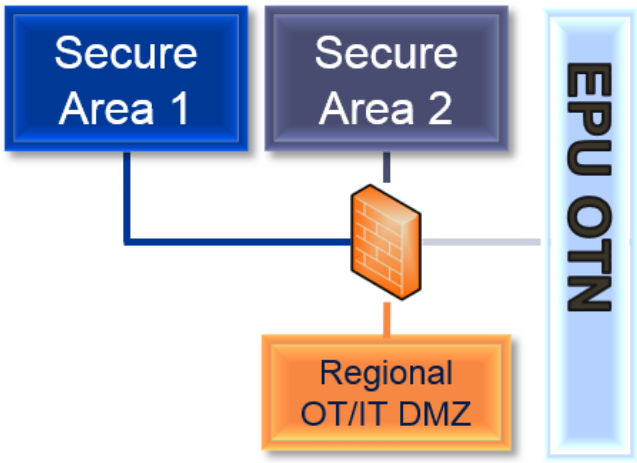

Figure 2. Logical Connection of the OT Secure Areas

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.

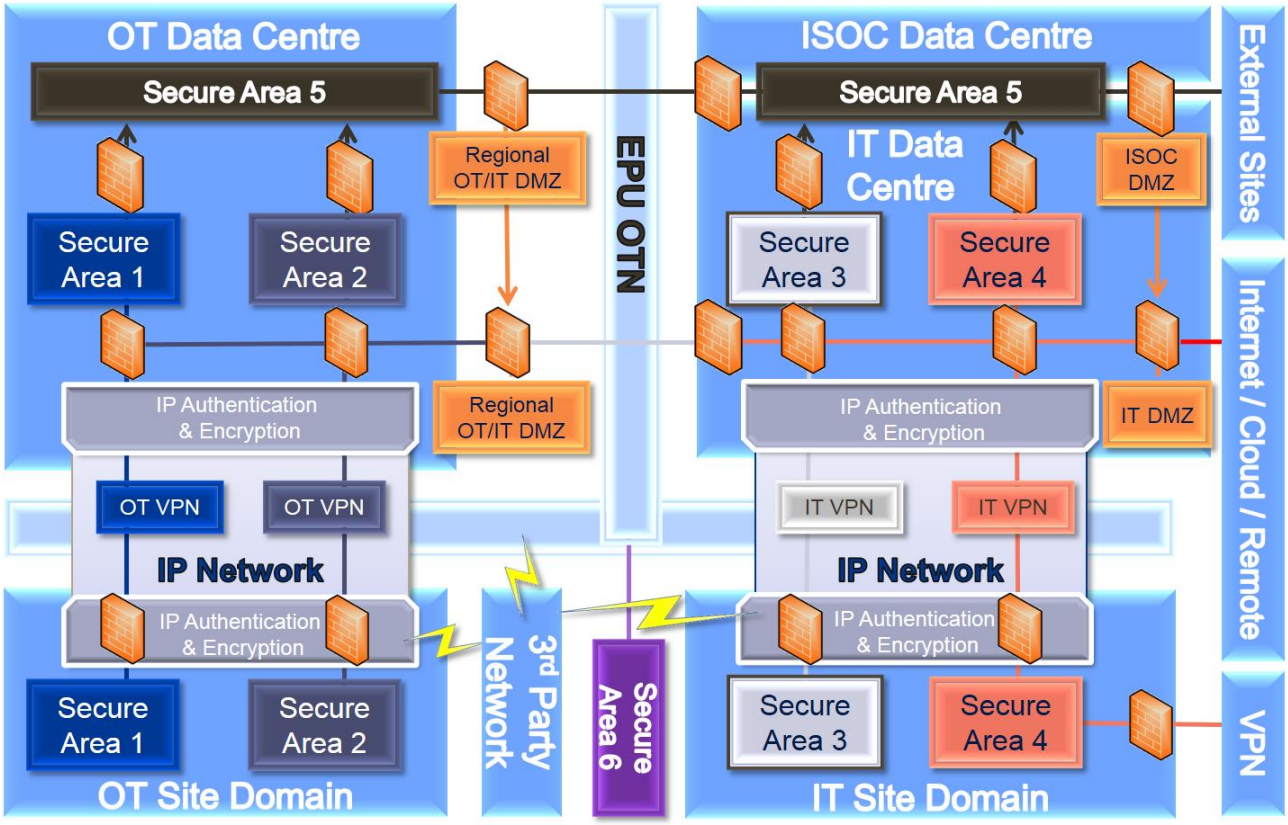

Figure 3. The Data Security Strategy of the Electric Power System

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

C. Secure Area 3 – Operational Enterprise Services

Dedicated for services hosted by 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.

D. Secure Area 3 – Enterprise Services

Dedicated to enterprise services maintained by IT that have no impact to OT operations. Enterprise services will follow IT governance.

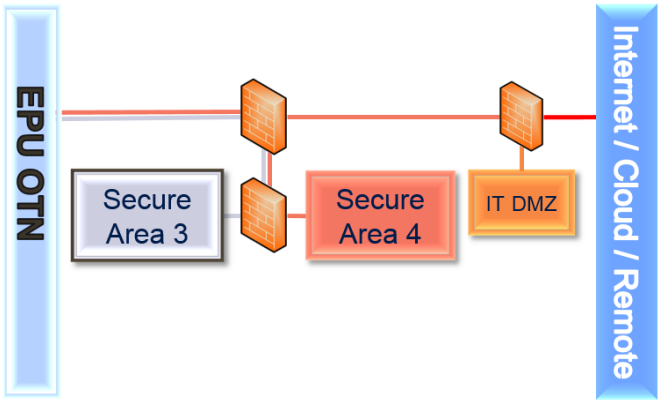

Figure 4 Logical Connection of the IT Secure Areas

Figure 4 above 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 EPU OTN to connect sites with logical separation. IT sites can use site-to-site Virtual Private Networks (VPN) services to assist with bandwidth management internal to the business.

Breaking out of the utility should be done at a single logical point. Internet, cloud, remote access, and other such external connections should pass through IT's security systems before progressing to the correct secure area. In this situation, IT security is assisting the rest of the business in security as part of a defense-in-depth [7] approach.

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 organization, or be a separate division.

E. Secure Area 5 – Security

Secure Area 5 is dedicated to services controlled by ISOC. In this setup, certain cybersecurity services are provided to the whole organization.

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:

- Agreed upon commitments with Cyber Response Committees.
- Government organizations

F. Secure Area 6 – External Services

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 [8][9]. Similar to IT, services that reside in Secure Area 6 will share the same physical transport infrastructure but be logically separated.

VI. Share Physical Transport Infrastructure

The secure areas are shown to traverse the internal EPU Optical Transport Network (OTN). The internal EPU WAN is comprised of a shared physical transport infrastructure with physically separate Internet Protocol (IP) Networks such as a Multiprotocol Label Switching (MPLS) network. Where the internal EPU 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. 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

Utilities in the transmission environment can lay their own fiber via methods such as overhead optical ground wire. This usually becomes part of the internal EPU OTN 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 [10]. This initial excess bandwidth on an internal EPU OTN could therefore be serviced to external 3rd parties as a return on capital expense.

VII. Conclusion

The strategy when applied together, culminates into a defense-in-depth approach. As data moves to a higher secure area, there must be permissions that allow the data to traverse further in the network. The strategy also give motivation for hosting and maintaining an internal WAN and highlighting the possibility of a shared OTN 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 cybersecurity 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 grid.

References

[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] North American Electric Reliability Corporation critical infrastructure protection, "CIP-005-3 Cyber Security – Electronic Security Perimeter", 2013.

[6] SABS Standards Division, SANS 62443-2-1:2016 "Part 2-1: Establishing an Industrial Automation and Control System Security Program", Pretoria, June 2016.

[7] SANS Institute InfoSec Reading Room, "Defense In Depth", 200. [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525 [Accessed 22 August 2017].

[8] 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.

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

[10] 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].