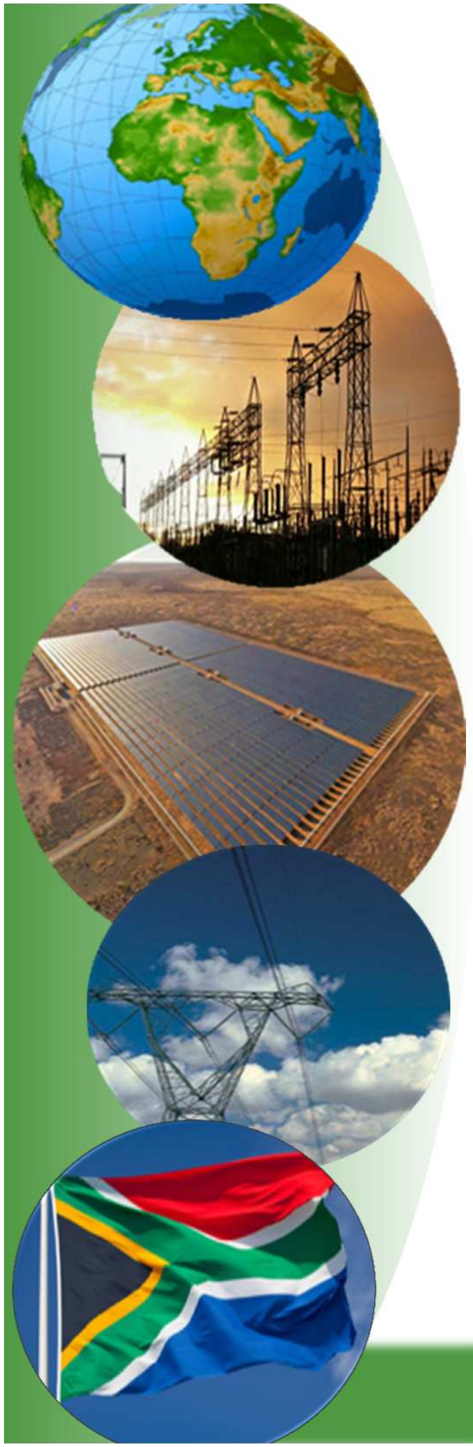


Network and Data Security Strategy of the Electric Power System

Matthew Taljaard
Eskom

Paper number 11.04
Session number 11
16 November 2017

The Future of the Electric Power Utility (EPU) Network

Interconnectivity

The future of the utility network revolves around IT/OT Collaboration

Opportunity

- Share Physical Transport Infrastructure
- Shared Resources
- Centralized approach
- Smarter Grid

Risk

- Cybersecurity – no longer OT is in isolation.
- Dependency – dependent on other areas of the business.

Therefore, can interconnectivity improve cybersecurity?

Four Key Areas for Interconnectivity

Operational Technology (OT)

Technology used to control, monitor and operate the electrical grid.

Information Technology (IT)

Technology used for business information processing.

Internal EPU Telecommunication

Provisions internal telecommunications for the EPU.

Integrated Security Operations Centre (ISOC)

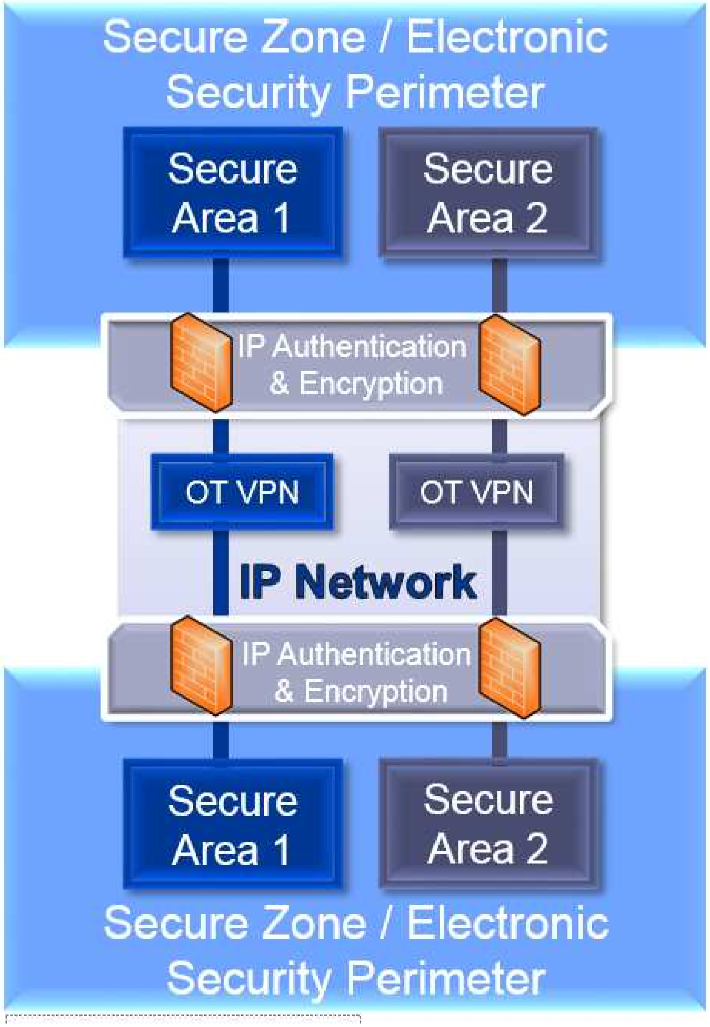
Cyber and Physical Security for the whole of business.

Secure Areas

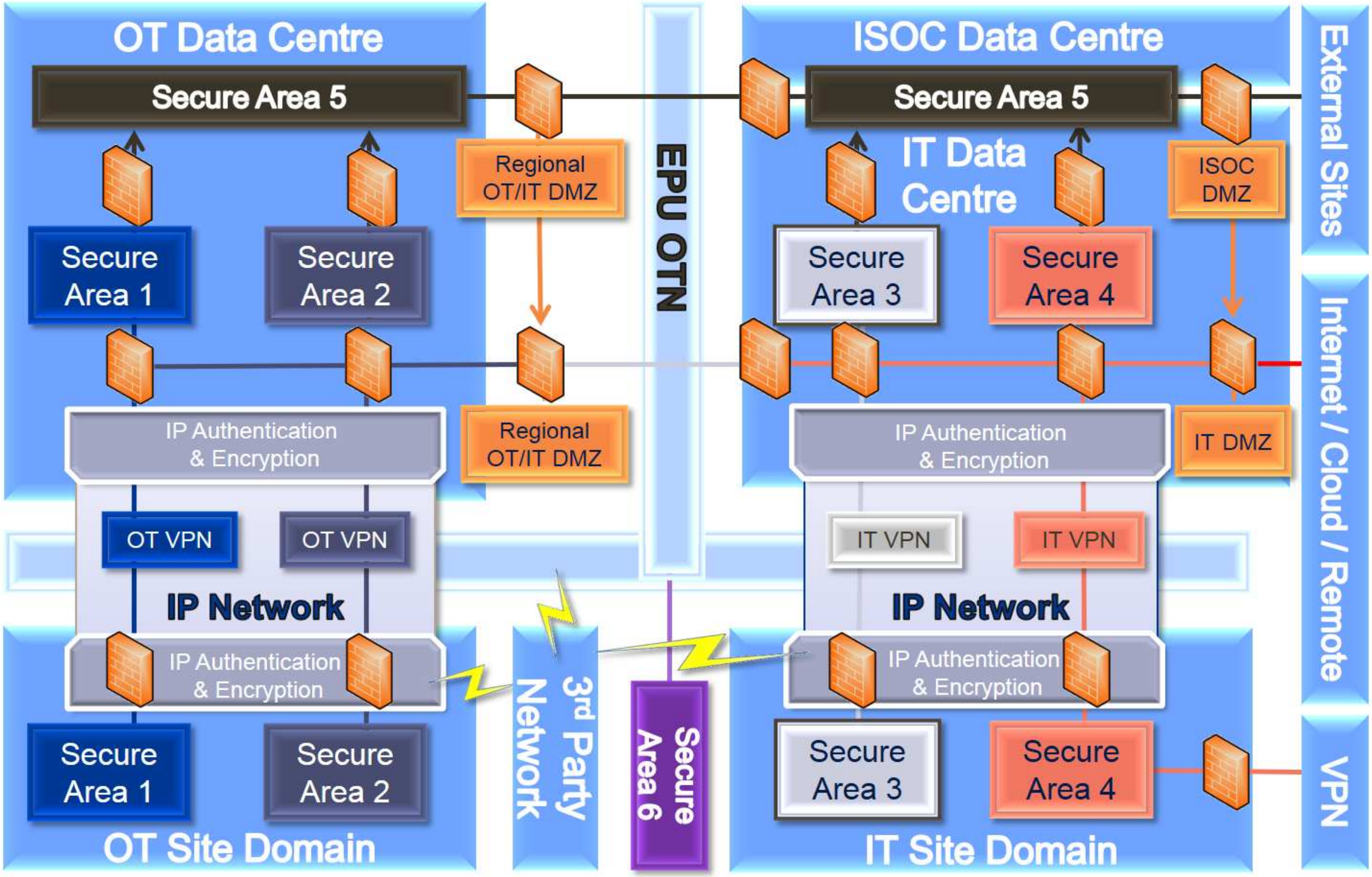
- A secure area is a term used to secure a service both on site and in transport.

- Secure areas are setup in a manner that prevents propagation of a threat from one secure area to the next.

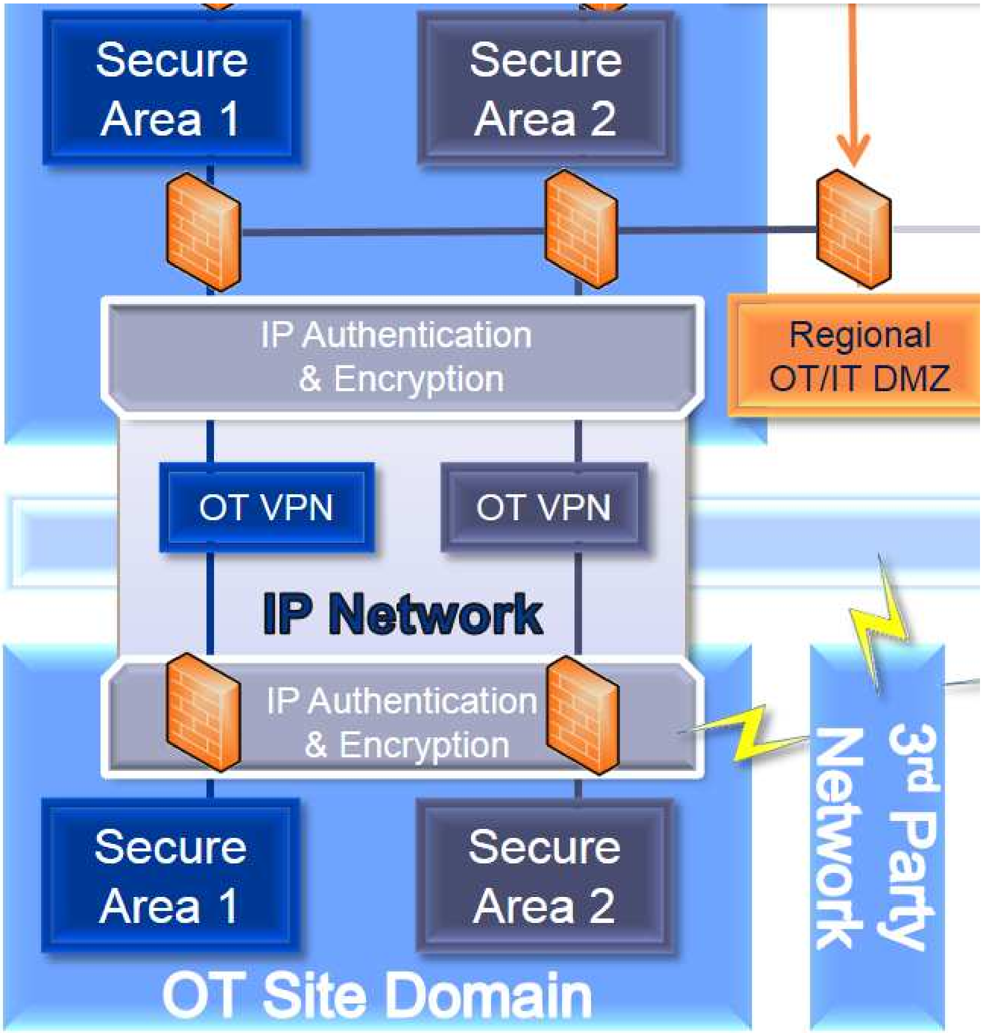
- Segregation can be accomplished by:
  1. Physical insulation
  2. Protocol insulation
  3. Firewall insulation


Secure Zone / Electronic Security Perimeter
Secure Area 1
Secure Area 2
IP Authentication & Encryption
OT VPN
OT VPN
IP Network
IP Authentication & Encryption
Secure Area 1
Secure Area 2
Secure Zone / Electronic Security Perimeter

The Information and Data Security Strategy of an Interconnected EPU Network

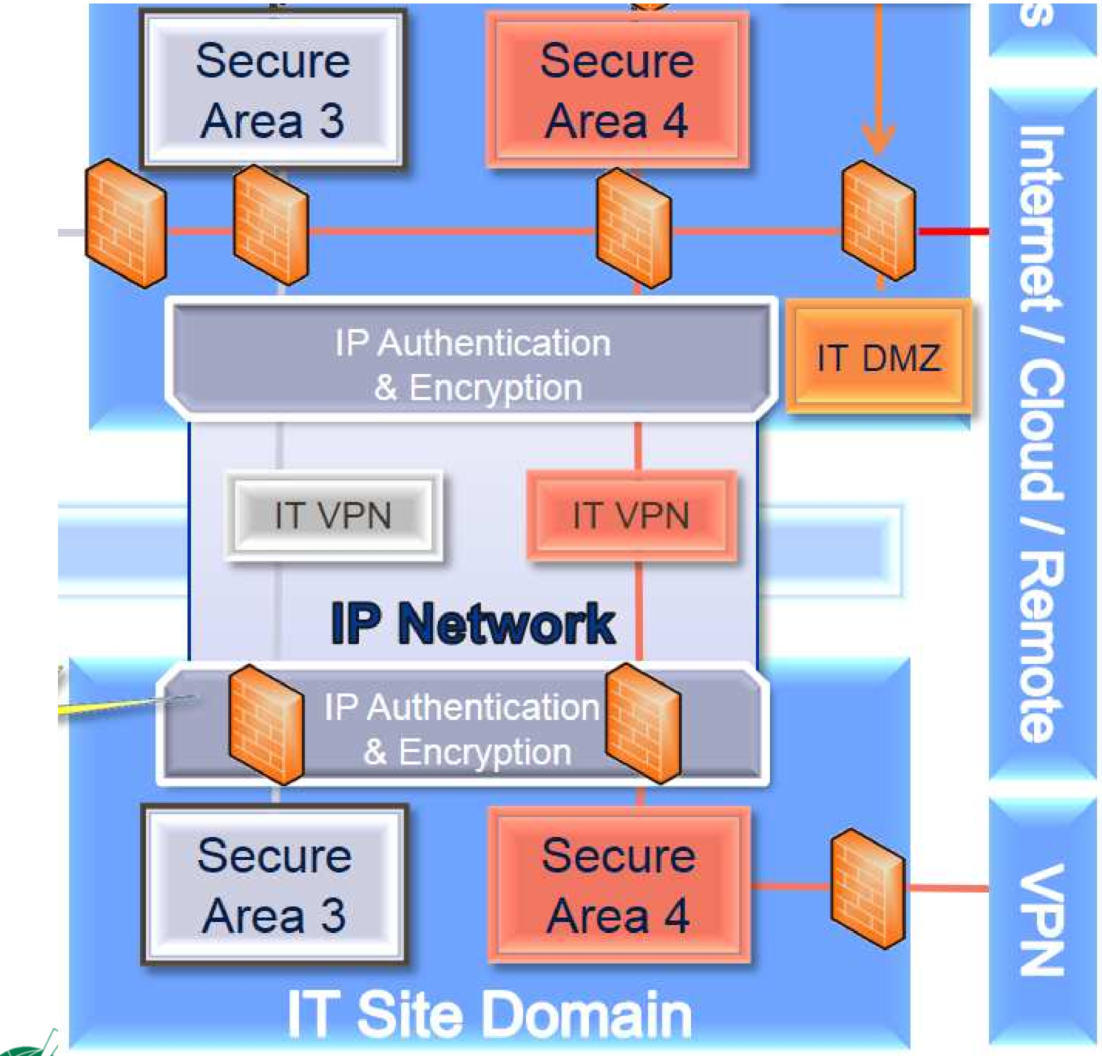


OT Secure Areas



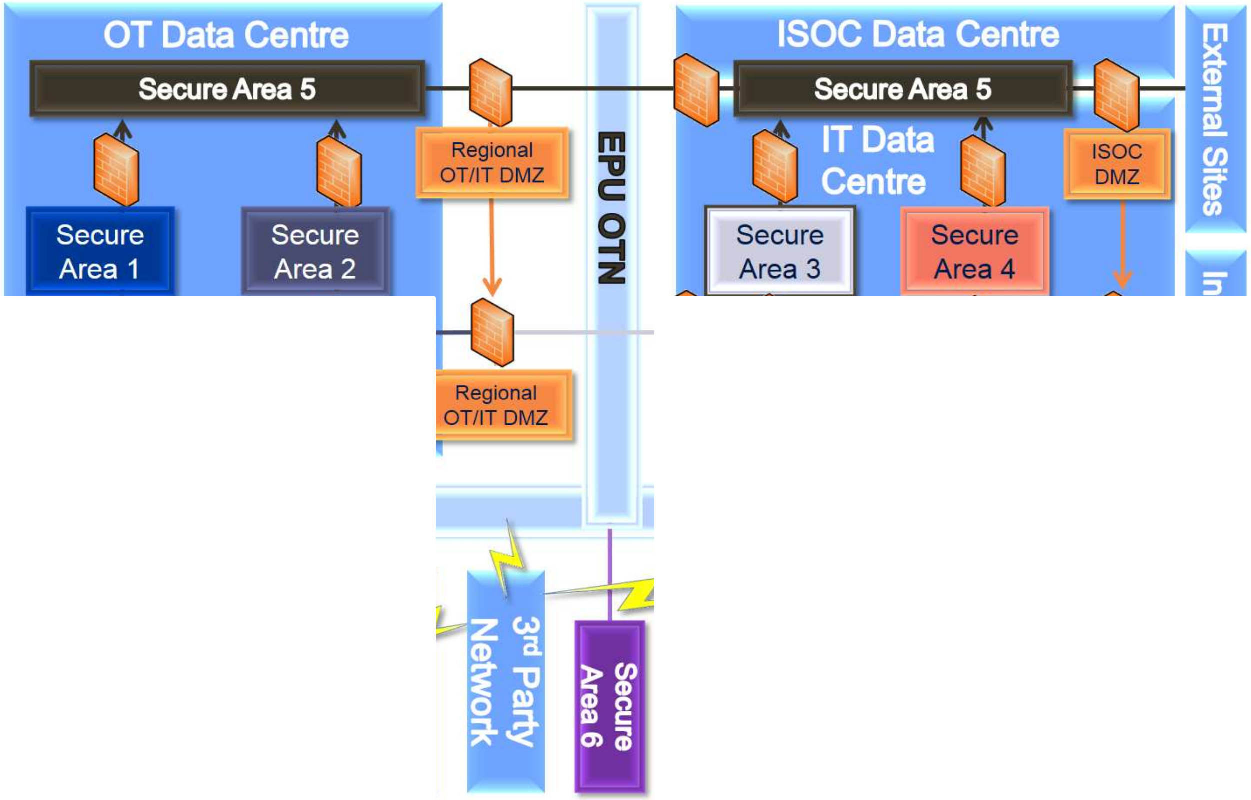
- Secure Area 1 – Critical
- Secure Area 2 – Non-Critical
- Secure communications over shared transport infrastructure.
- Authentication and encryption provided by either the internal EPU telecoms or the customer themselves.
- Regional DMZ to share data between secure areas.
- 3rd party telecommunication services are used when required.

IT Secure Areas



- Secure Area 3 – Production
- Secure Area 4 – Enterprise
- Secure communications over shared transport infrastructure.
- Authentication and encryption provided by either the internal EPU telecoms or the site themselves.
- Single logical entry point into the business for Cloud / Internet / Remote Access.
- Site-to-site VPN for bandwidth management.

ISOC & External Secure Areas



- Secure Area 5 – ISOC
- Secure Area 6 – External
- Secure communications over shared transport infrastructure.
- “External Sites” are for collaboration of combating security threats. E.g. Cyber Response Committees, Government organizations.
- Secure area 6 for external networks that connect on the transport network. E.g. selling of fiber.

Thank You

Presenter: Matthew Taljaard

Email: TaljaaMM@Eskom.co.za