CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS3 – Developing Secure and Reliable ICT Systems Infrastructure

Network and Data Security Architecture of the Electric Power System

M. TALJAARD
Eskom
South Africa
TaljaaMM@eskom.co.za

The operational network that supports the energy production of a power company is no longer in isolation form the rest of the network and the systems that support the business. The technology move to a more interconnected network to increase business intelligence and productivity has exposed operational networks to cyber threats that previous were not a risk.

Energy power systems now face the challenge of co-existing two networks namely:

1. The Operational Technology (OT) network which operates, monitors and controls the power grid and;
2. The Information Technology (IT) network which provides business information solutions.

OT and IT have different personnel, priorities, policies and technology. Collaboration is recommended for financial and practical purposes; however, the question is where collaboration can exist and what vulnerabilities are introduced?

The technology move has not only introduced the merging of networks, but also the protocols used inside a system. Traditionally, OT networks used serial based non-routable protocols (e.g. DNP3, X.25, etc.) that operate on layer 2 of the open Systems Interconnectivity (OSI) model. These systems are now moving to routable IP and Ethernet based systems that can operate at layer 3 (IEC61850, TCP/IP, etc.). This increases the vulnerabilities to the system from an external source.

It becomes clear that a converged and interconnected network between OT and IT is the future of the electric power system.

The paper with therefore look at:

1. Network and data security of an interconnected network between OT and IT.
2. How policies and priorities require development with collaboration and synergy of all connecting networks.
3. The responsibilities of data and user accounts along with threats to the organisation.

4. Types of segregation that provide control over data and access to data.
5. When breaches are detected, how will threats be contained and prevented from traversing the electric power network?