Paris Session
2022

cigre
For power system expertise

Contribution of strategies for cybersecurity in modern protection systems

B5 Protection & *Automation PS 3 / Integration of intelligence on substations / Question 3.06 – What are your experience to monitoring IEC 61850 based and how you secure the operation of critical infrastructure and respond to incidents?*

Jonas Pesente / Brazil

ITAIPU

What are your experience to monitoring IEC 61850 based and how you secure the operation of critical infrastructure and respond to incidents?

A: Regarding IT security, four types of probable attacks were considered in the project: Denial of Service, Man in The Middle, Delay, and Sniffing.

The preventive actions taken were:

i) protection with new generation firewalls;

ii) implementation of a restrictive policy up to the application layer of the OSI reference model, denying all types of unnecessary services and including anti-malware;

iii) incorporation of detection and prevention of IPS/IDS intruders on all inbound and outbound connections to ECCANDE;

What are your experience to monitoring IEC 61850 based and how you secure the operation of critical infrastructure and respond to incidents?

iv) application control to only allow Application Service Data Unit types of the IEC-104 protocol implemented in ECCANDE;

v) integration of PMUs, PDCs, and RTUs with the operating technology network device monitoring system to identify lost devices and/or communication; and

vi) implementing an event management system and security information as a preventive tool and reacting to the attacks.