- ***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?***

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.

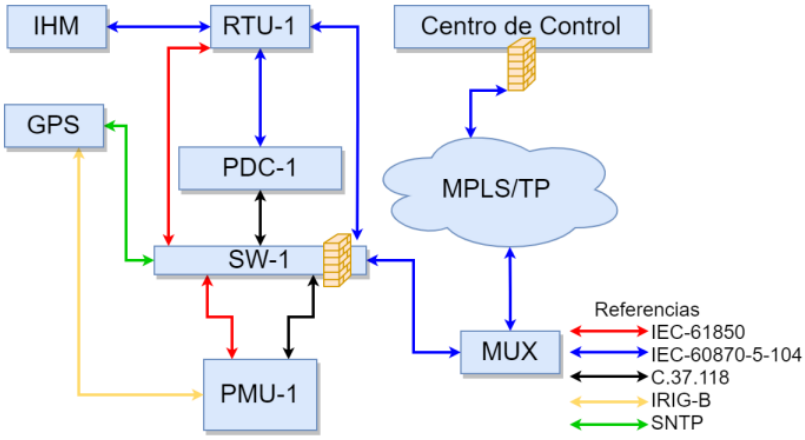
iv) application control to only allow Application Service Data Unit types of the IEC-104 protocol implemented in ECCANDE.

v) integration of PMUs, PDCs, and RTUs with the operating technology network device monitoring system to identify lost devices and/or communication[1]; and

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

An illustrative block diagram of the WAMPAC architecture is presented below, where the main firewalls, switches, and the control center where the monitoring of incidents is performed are highlighted.

Although simple, this architectural structure allows us to meet the involved teams' main safety requirements.



1. In its first stage, the devices' status and communication links based on devices' messages were considered, and services are being/planned to be incorporated gradually.

   Despite the ECCANDE experience, at the Itaipu powerplant, activities are being developed to provide adequate levels of cyber-security, including the installation of a console in the operation room, for providing alarms of devices and processes (including EMS applications), the development and deployment of a specific code and the planning and design of a system for monitoring devices and processes.

   Up to date, a comprehensive, holistic 61850 services monitoring process is a requirement to be fulfilled.