GROUP REF. : B5-PS3
COUNTRY : Russia
PREF. SUBJECT : 3.7
REGISTRATION NUMBER : 10377
QUESTION N° :3.06

Dmitry Yasko, Oleg Fedorov
JSC «System Operator of the United Power System», JSC «RTSoft»
Russia

Implementation of Protection Operation Analysis and Fault Management System Based on Fault Data Aggregation and Detailed Digital Simulation

Question 3.06: What are your experiences to monitoring of IEC 61850 based PCAS and how you secure the operation of critical infrastructure and respond to the incidents?

System Operator of Russia (SO UPS) has initiated development of new "Protection Operation Analysis and Fault Management System" (POA FMS).
Input information for POA FMS is received from different sources such as SCADA and devices (IED, PCAS) with digital fault recording functions having different communication protocols including IEC 61850.

The following data types (discrete signals, SCADA analog values, fault recording files and Comtrade, text logs, calculated values from transients and short circuits simulation) are aggregated and are used for automation of fault event analysis and evaluation of protection devices/functions operation.
The algorithms work independent from data collection protocol types (with or w/o IEC 61850). It was done in microservice architecture design where separate module is responsible for preprocessing of IEC61850 messages. COMTRADE files and PCAS settings values are retrieved into POA FMS algorithms through developed API. Data input from different protocols (SOAP, FTPS, IECx104) and even manual upload are preprocessed into REST API.
All components of POA FMS, deployed on the servers of System Operator of UPS, has successfully passed through numerous tests during 1 year to verify all functionality.
The analysis using this method is predictive one and enables detection of hidden failures in PCAS, such as:

- errors in settings values (configuration parameters) and in operation of measuring functional blocks of the protection that can include:
  - incorrect settings group;
  - non-conformance of actual settings values stored in device with confirmed (etalon) configuration requirement;
  - errors in implementation of the measuring functional blocks or logic part of the protection;
- errors or failures in secondary (measurement) circuits of protection devices;
- incorrect operation during transients conditions (incorrect protection operation in time-domain dynamic).

Use of POA FMS enables achieving the following effects:

- automated collection and analysis of fault data that reduces time required for further follow-up actions and restoration planning in the grid;
- detection of hidden failures and incorrect settings of protection devices that contributes into enhancement on overall power system reliability.

POA FMS was designed in SO UPS to receive initial data from external servers of power utilities. To meet cybersecurity requirements were used traditional separation of communication networks through DMZ and equipped with firewalls. Neither control signals coming from POA FMS to any power utilities nor any control commands to equipment are used in the architecture. The System is not part of critical infrastructure like substation automation or telecontrol communication links. Data flows are read only and are having single direction – to the POA FMS (like in data diode).
The system itself has RBAC role-based access and identification and authorization functions by default.
This solution has no additional costs in deployment projects when scaling POA FMS in the System Operator for new control centers.