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° PS2

A Monitoring Architecture for Smart Grid Cyber Security

G. DONDOSSOLA, R. TERRUGGIA
Ricerca sul Sistema Energetico – RSE spa
Italy
{Giovanna.Dondossola, Roberta.Terruggia}@rse-web.it

The new Smart Grid landscape requires the development of new ICT (Information and Communication Technology) enabled functionalities or the reshaping of the existing ones. The global control strategies of the power grid need information coming from internal, but also external, entities, and the consequent establishment of new data exchanges. For this reason the cyber security of the involved communications becomes a key aspect determining the correct operation of the power grid. The security issues need to be addressed in order to guarantee the availability, integrity and confidentiality of the essential information exchanges.

The cyber security of the smart grid comprises several requirements to be analysed and addressed by suitable countermeasures: in this paper the focus is on the use of the monitoring infrastructure as an instrument to support the response capabilities to ICT anomalies and to increase the system resilience. The traditional preventive measures (e.g. network segregation, access control, authentication, end to end data encryption) can be enforced by a smart monitoring infrastructure able to identify existing vulnerabilities before they are exploited by targeted attacks. Moreover the correlation of the monitoring data can provide relevant alerts about on-going attacks. The paper investigates the capability of the real time monitoring to highlight vulnerabilities and timely respond to the residual risks not covered by the preventive measures applied in the system.

The smart monitoring can be performed implementing and configuring a Network and Application Security Monitoring platform where several monitoring agents are installed in key control infrastructure points at communication and IED devices, in order to observe and correlate not only the ICT aspects as the traditional monitoring frameworks, but also power control communication specific events addressing for example the objects defined in the IEC 62351-7 standard. The smart platform allows analysing in detail the key role of the monitoring in the attack prevention, detection and effect mitigation. The monitoring information coming from different kind of devices (communication components as well as power grid IEDs) need to be collected and analysed by a central system (Figure 1) correlating data at different stack layers in order to recognise the type of occurring anomaly.

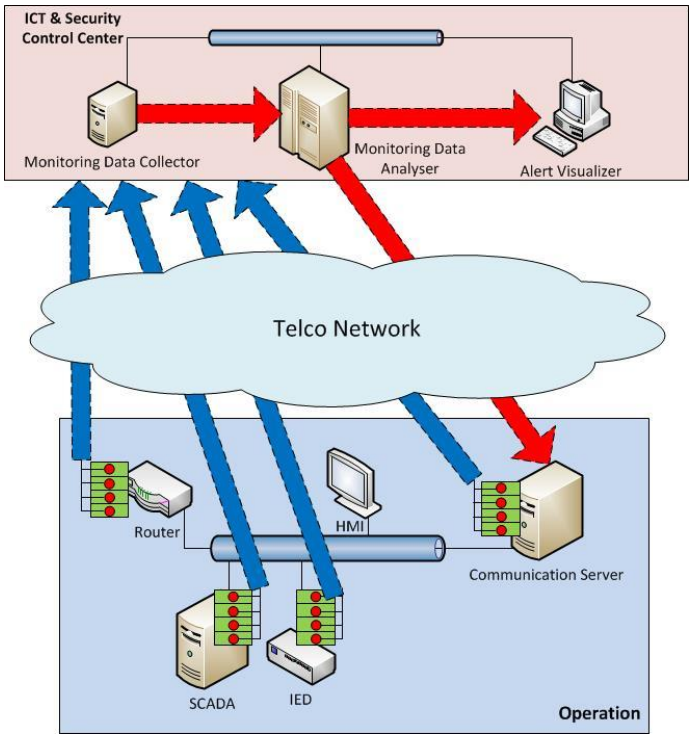

Figure 1 – Smart Monitoring Infrastructure Layout

The alerts coming from the analysis of collected data can reveal the existence of vulnerabilities or give an indication that a given attack is active. In the first case the data are used in order to identify potential threats and address possible corrective actions. In the case of active attacks, the alerts allow performing automatic or manual recovery activities. Moreover it is possible to consider the outcomes of the monitoring data analysis as an important source of information for the setup of power control actions aligned with both the power and ICT infrastructure status.

The assessment of the security monitoring functionality described above is carried out by the setup of a lab platform implementing the ICT components of the smart grid domain with different standard communication modules: in this paper the focus is on the communications between a DSO (Distribution System Operator) primary substation and third party DER (Distributed Energy Resources) sites, required for the optimization of the medium voltage grid management in presence of renewable generation. These communications are implemented by MMS (Manufacturing Message Specification) information flows, compliant with the IEC 61850 data model and communication profile, and secured in compliance with the IEC 62351 T-profile. The lab platform deploys the monitoring infrastructure implementing the monitoring agents (related to ICT and IED objects) that provide data to the Security Control Center via standard protocols (i.e. SNMP, Syslog). Here the information coming from the agents are collected, correlated and analysed. The capability of the lab platform to achieve the security requirements is demonstrated by means of some meaningful attack scenarios.