Study Committee D2

Information Systems and Telecommunication

Paper D2_104_2014

SECURITY OF COMMUNICATIONS IN VOLTAGE CONTROL FOR GRIDS CONNECTING DER: IMPACT ANALYSIS AND ANOMALOUS BEHAVIOURS

G. Dondossola, R. Terruggia

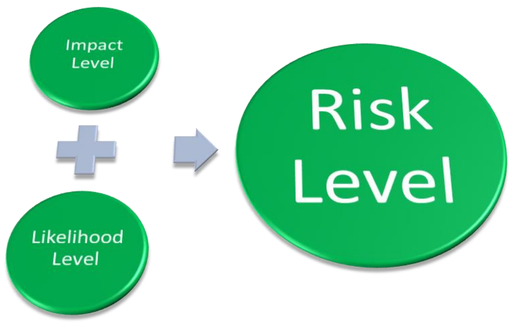
Ricerca Sistema Energetico – RSE spa

Motivation

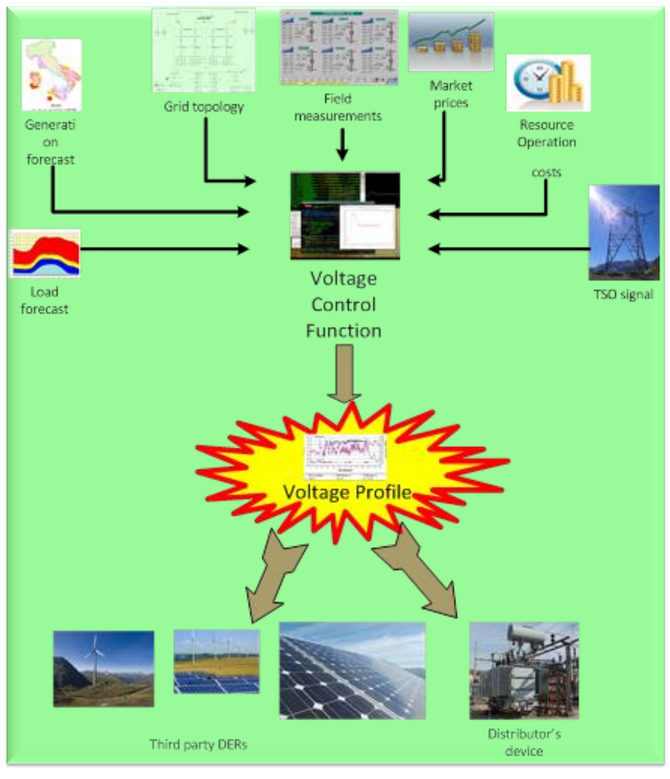
- How to identify Cyber Risks of Smart Grid architectures
- European Mandate E/490 on Smart Grid Standardization
- CEN/CENELEC/ETSI Smart Grid Coordination Group SG-CG
    - WG Smart Grid Information Security - SGIS
- Apply and evaluate the SGIS approach to the Risk Analysis of Smart Grid Use Cases

Method/Approach

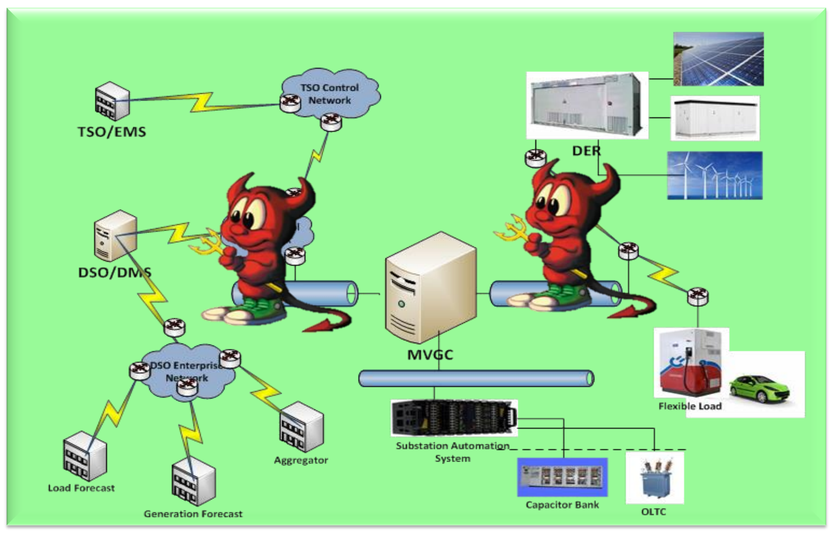
Voltage Control in MV Grids with DERs Use Case	• Actors • Information Flows
Risk Assessment	• Impact Levels, Likelihood Levels • Risk Levels
Security Standards	• Security Requirements • Security Solutions
Policies	• Logical Interfaces



Objects of investigation

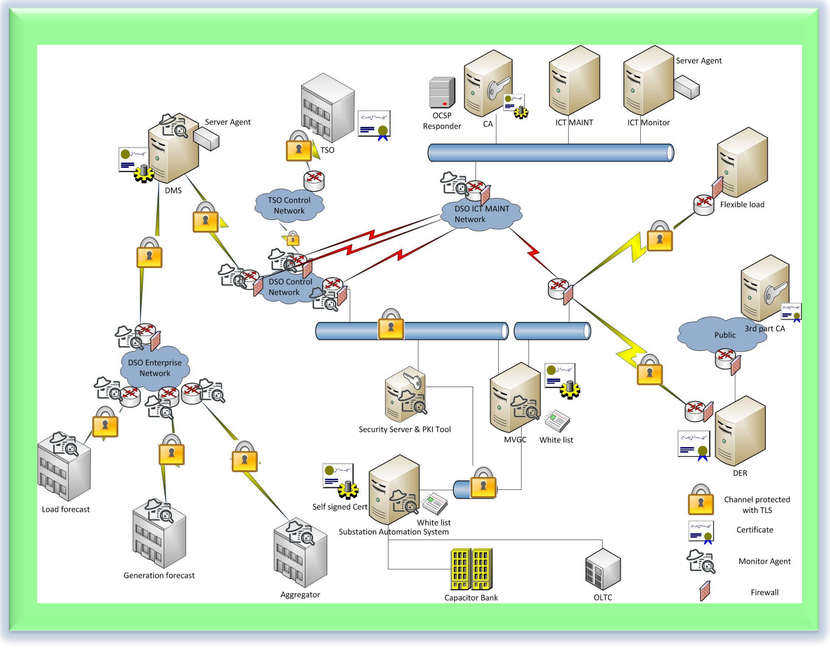


Experimental setup & analysis results



Discussion

- By applying the SGIS matrix to the Voltage Control security analysis, High and Critial Risk Levels are associated to the use case information assets
- Resulting Risk Levels may support the selection of adequate protections from ongoing security standards



Conclusion

- Risk analysis of Smart Grid use cases requires modeling their detailed architecture, message sequencing and attack scenarios, and instantiate them over benchmark grid data and control network topologies
- Qualitative methods allow deriving rough risk levels of information assets providing indications of the required security measures
- Quantified risk levels, possible only with the support of modeling tools, would allow evaluating security measures

SMARTC2NET

SoES Security of Energy Systems

INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

Conseil International des Grands Réseaux Électriques

http://www.cigre.org