InnoGrid2020+

The European Research & Development Dissemination Seminar

23 - 24 February 2012

AFTER project

A Framework for electrical power systems vulnerability identification, dEfense and Restoration

Electric Power System is a Continent-wide, very complex interconnected synchronous network

Electric power system is *increasingly vulnerable* to different threats (physical and functional)

Disturbances may propagate throughout the interconnection, eventually leading to significant interruption of service (blackouts)

This trend is expected to continue in the future, especially in the perspective of *Smart Grids.*

The future implementation of Smart Grids will further increase the importance of secure and reliable ICT.

Transmission System Operators (TSOs) are increasingly concerned about the resilience of *integrated Power & ICT* system with respect to *failures* caused by different kind of *threats* and, in particular, wide area multiple contingencies caused by

- *deliberate acts of terrorism, sabotage, criminal activity, malicious behaviour*
- *accidents, natural disasters, negligence of the operators*

TSOs need a jointly-agreed, practical methodology to

- evaluate the global operational risk,
- control the risk and
- guarantee an adequate security level for the interconnected network

Research organisations

RSE (Ricerca Sistema Energetico), SINTEF, ENEA, Università degli Studi di Genova, UCD Dublin, City University London, JRC Institute for Energy (European Commission)

Industries

ALSTOM, SIEMENS

Stakeholders

CEPS a.s., Terna, elia

Advisory group

ELIA (Belgium), *Svenska Kraftnät (Sweden)*, *RTE (France)*, *Energinet (Denmark)*, *STATNETT (Norway)*, *Tennet (The Netherlands)*, *TERNA (Italy)*, *Red Electrica de Espana (Spain)*, *Vattenfall Europe Transmission (Germany)*

Assessment framework and tools to identify vulnerabilities of energy grids and energy plants, and to protect them against cascading effects

O1. Define and develop a framework for risk and vulnerability assessment for power and ICT systems considering both natural and man-made (Power System and ICT) failures

O2. Introduce innovative defence plan concepts and techniques to manage multiple contingencies, and assessment methodologies to evaluate their effectiveness

O3. Develop innovative restorative control by designing a framework to support the restoration stages of the integrated power system

(1) Methodologies and tools for global vulnerability and risk assessment of electrical power system considering the relevant ICT systems

Operation: support operators in power system monitoring and supervision to identify high risk system operating conditions, enabling preventive actions (e.g. generation redispatching)

Operational planning: support operators in power system operational planning (day ahead to some days ahead); identify forecasted system operating conditions (also resulting from market rules) presenting high risk, thus allowing to call for preventive actions (e.g. generation rescheduling)

Planning: support planners in analysing the risk level associated to forecasted development scenarios.

(2) New defence plan concepts and defence plan design support

Planning: support engineers in global defence plan design. By means of the proposed risk assessment tool, planners can assess (off-line and on-line as an operator guide): the new defence plan concepts proposed within the Project and the effectiveness of different defence plan solutions (architectures, settings, etc.) in reducing operational risk.

(3) Restoration support

Planning: planners can assess the effectiveness of different restoration solutions

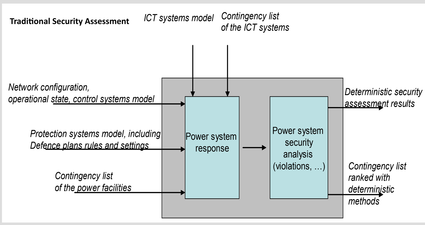
Operations (restoration): operators can be supported in the restoration process in identifying the best restoration actions.

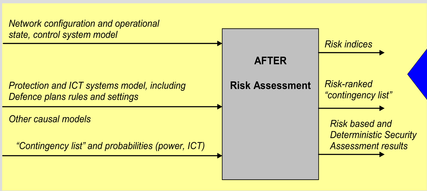
AFTER:

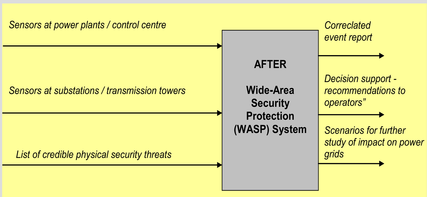
- will analyse the vulnerabilities of the different parts of the network and
- will provide tools to limit the impact of accidents/attacks on these networks

Expected impact:

- significant improvement in *the security and resilience* of complex interconnected energy networks

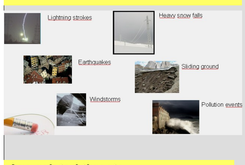




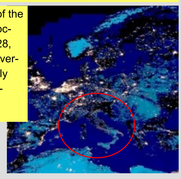


Vulnerability—Threats include wide area multiple contingencies caused by equipment and/or subsystems malfunctions, negligence of the operators, deliberate acts of terrorism, sabotage, criminal activity, malicious behaviour, accidents, and natural disasters.

Natural threats



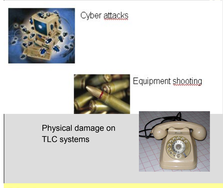
A satellite view of the blackout which occurred on Sept 28, 2003 at 4 am covering the entire Italy and some neighbouring areas.



Age-related threats

Some of the practical effects of the windstorm in December 1999 which affected an important portion of the Central-West part of the European electrical

Intentional threats



Some of the practical effects of the unexpected exceptional snowfall in Canada on December 17, 2007, causing the damage of tens of 765 kV poles and a major blackout .

Natural and man induced events and phenomena cannot be fully controlled

FROM *Security Assessment*

TO *Risk assessment and contingency planning*

N-1 security against a credible set of contingencies

Vulnerability to events of substantial risk

"sequence of dependent failures of individual components that successively weakens the power system" (IEEE)

- *Power/ICT contingencies*
- *Wide area events*
- *Cascading failures*
- *Large blackouts*

Vulnerability / Risk assessment

Current practices for the evaluation of security are based on purely deterministic N-1 criteria

Expressing security in terms of risk considering in particular wide area multiple contingencies would convey a better insight into security problems.

Current practices investigate the electrical power system ability to provide electricity when subjected to the failure of single components (N-1 security), without considering major accident and without considering the ICT aspects, thus lacking proper integration between the two

The integrated view of power and ICT security in terms of risk would convey a deeper insight into security problems.

Contingency planning

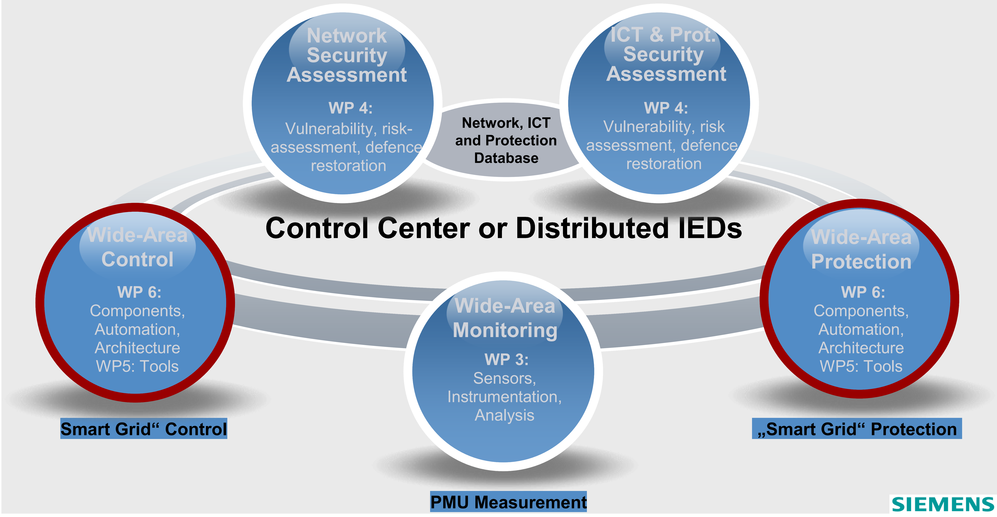
- **Calls for the set-up of - integrated - *global defence strategies* to handle high impact multiple contingencies and consequent cascading process**
- **The focus of the proposed *defense system* is to address issues related to cascading events, as opposed to the single or double contingency events as in the traditional approach**

Defence plans

- **Operate in critical situations, when the system is about to undergo a disruption process**
- **Require high dependability**

Operational Grid Compliance
e.g. entso-e

Operational Protection Compliance
e.g. DSOs, City Utilities



SIEMENS

T