PowerFactory Users' Conference and Future Networks Technical Seminar

DIgSILENT Pacific & The University of Sydney

5-6 September 2013, Sydney Harbour Marriott Hotel

Some Issues in deployment of Future Networks

Ashok Manglick
Director, Manglick & Associates

Contents

- ***Future Networks (*or SmartGrid)**
- **Some Issues in Deployment of Future Networks**
  - Integration of diverse generation sources
  - Security of Future Networks
  - Security, handling and protection of data
  - Integration of new IT with ET
  - Standards for Future Networks
  - Regulation of Future Networks
- **Concluding remarks**

Future Networks (or SmartGrid)

- **The term "SmartGrid" –**
  - **stroke of marketing genius,**
  - **discourages legitimate criticisms and concerns,**
  - **no one really knows what it means**
  - **Not something you can point to, its an evolutionary process**

- **IEC – *"The electrical network is composed of a high number of very distributed nodes that are highly coupled and operating in real time. .. Figuring out where intelligence needs to be added is very complex. The Smart Grid implementation has already started and 33will continue to be implemented as an "evolution"."***

Future Networks (or SmartGrid)

- **Institute of Engineering & Technology + European Regulators Group for Electricity & Gas**

"Smart Grid will cost efficiently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety."

[But what about the networks? 3

This is exactly what the current grid does.]

Future Networks (or SmartGrid)

- **IEEE** – " *The "Smart Grid" has come to describe a next generation electrical power system that is typified by the increased use of communication and information technology in the generation, delivery and consumption of electrical energy."*

- Hence, **Future Networks** is a more accurate description and a preferable term to describe the next generation grid

Integration of diverse generation sources

- Without debating the impact of GHG and Global Warming which may or may not be real, generating sources will become more and more diverse
- Most of them will be renewables such as wind, solar and EV
- There are two reasons for the push to connect them to the grid:
  - *They reduce GHG*
  - *They cannot deliver acceptable level of reliability or continuity of supply in stand alone systems so need back up from the grid*

    [Customers used to seeing the lights come on at the push of a button 24/7]

Integration of diverse generation sources

- **Main issues in integrating these generating sources:**
  - *Intermittency - cannot be controlled like conventional generators, so need to provide back up from the grid and/or storage – both costly, who pays?*
  - *Increased unpredictability in size and direction of power flows in the network*
  - *Lack of inertia which is necessary to stabilise the grid*

Integration of diverse generation sources

- **Main issues in integrating these generating sources (cont'd):**
  - *No reactive power support necessary for voltage level and control – again who pays for the remedial measures*
  - *No support in terms of synchronising torque or damping torque following a contingency*
  - *In general best sites for PV and Wind are at large distances from existing transmission lines –*

    Who pays for the connection costs?

    And who is responsible for acquiring easements?

Security of Future Networks

- **As noted, main developments will be in IT & Communications**
- Communication and control of the grid and dispatch of generating sources using web based portals and applications (Apps)
- Convergence of protection and substation control into intelligent systems capable of remote control and setting
- At the consumer end, Smart phone based apps allowing remote control of devices inside the house to take advantage of dynamic pricing (not time of use pricing)

Security of Future Networks

- Each communication link is susceptible to external infiltration – cyber attack
- Need to ensure security of these new communication pathways
- First need to develop measures for detecting and protecting against cyber attacks
- Secondly, securing the grid in case of a successful penetration

Security of Future Networks

- Traditional grid is operated to be secure after a single contingency and at least partially secure after two successive contingencies
- With Future Networks, there will be a very high level of integration in control and operation of the entire chain G-T-D-C
- It is highly likely that one cyber attack or a single systemic failure will take out multiple critical elements and lead to catastrophic failure making continued secure operation of the grid less tenable

Security of Future Networks

- Such cyber attack can be initiated at any point in the G-T-D-C chain, including malware introduced into so called Smart Meters
- Compromised software controlling the hardware may result in Denial of Service (DoS) from an otherwise healthy hardware
- This could potentially cripple the whole grid
- Need to devise protective and remedial measures

Security, handling & protection of Data

- Future Networks will have Smart Meters, remote and automatic access and control of myriad of devices owned by different parties across the entire G-T-D-C chain
- There will be huge amount of data collected by various parties
- And, there will be many parties wanting access to this data for commercial gain
- Data security, handling and protection become critical while ensuring legitimate access to data
- Need strong legislative framework to ensure the privacy and security of data

Integration of IT with ET

- New IT & Communications systems are not simple high level patch up of IT infrastructure on to existing or new electro-technical (ET) devices such as lines, substations and generators
- In the Future Networks, each electro-technical (ET) device will be simultaneously an electro-technical (ET) device as well as a node with local intelligence
- Some examples of local intelligence are integrated protection and control in a substation, digital and remotely programmable PSSs, dynamic line rating integrated with FACTS devices

Integration of IT with ET

- Second issue relates to entirely different life spans of IT & ET
- IT systems have a typical life span of 3-5 years compared to 30-40 years for ET devices such as lines, transformers etc.
- We need to integrate these two very different systems which can be controlled and updated coherently with no or little downtime

Standards for Future Networks

- New IT & Communications systems are not simple high level patch up of IT infrastructure on to existing or new electro-technical (ET) devices such as lines, substations and generators
- In the Future Networks, each electro-technical (ET) device will be simultaneously an electro-technical (ET) device as well as a node with local intelligence
- Some examples of local intelligence are integrated protection and control in a substation, digital and remotely programmable PSSs, dynamic line rating integrated with FACTS devices

Standards for Future Networks

- Standards for Future Networks are being developed by:
  - National Institute for Standards and Technology (NIST), USA
  - International Electrotechnical Commission (IEC), Europe
  - Indian Standards Institute (ISI), India
  - Japan Standards Association (JSA), Japan
  - Standards Australia (SA), Australia
- Standards Australia and Department of Resources, Energy & Tourism has published a “Australian Standards for Smart Grids – Standards Roadmap”, June 2012

Standards for Future Networks

- **Some areas to be covered by standards :**
  - Data security protocols
  - Communication protocols
  - Electromagnetic compatibility
  - Interconnection protocols
  - Smart Grid vocabulary
  - EV connectivity to grid
  - Home automation
  - Transmission of information & data
- **IEC considers that around 100 standards are needed to cover most aspects of Smart Grid**

Regulation of Future Networks

- **Regulatory framework requires significant changes to address governance and economic regulation of Future Networks**
- **For example:**
  - In Future Networks, issues caused by one entity will require remedial measures to be implemented in another entity's system
  - For example, renewables will require installation of equipment to provide reactive support and may require additional capacity to deal with intermittency – who pays ?
  - Need for remote access and control of substation or generating unit may require retrofitting or in extreme case whole rebuilt of a substation

Regulation of Future Networks

- Technical requirements for connection of distributed generation
- Recognition of capex spent on upgrading control systems, control centres purely to accommodate Future Networks
- Recognition of life spans of IT systems
- Increased vulnerability of network and its elements due to cyber attacks and consequent impact on service levels

Concluding remarks

- Future Networks is a evolutionary process
- They will have a high level of IT, communications technology and very high level of automation in the entire G-T-D-C chain
- However I think a **FULLY** automated grid with no provision for human intervention will be a nightmare – one unforeseen contingency and its gone - automatically
- Future Networks will be far more complex, more susceptible to cyber attacks
- There are a number of issues we need to address to successfully transition to more automated and connected Future Networks

Thank you

- Ashok.manglick@gmail.com