Smart Energy Management System for the Complex Operational Environment

Chen-Ching Liu
Professor of Power Systems
University College Dublin
National University of Ireland, Dublin
The operating state of a power system is **SECURE** if no disturbance in the next contingency list leads to an emergency operating condition and is **INSECURE** otherwise.

- Needs a list of ‘next contingencies’
- N-1 or N-2 security criteria
Traditional EMS Security Functions

- MEASUREMENTS
  - FILTERING
  - STATE ESTIMATION
- NETWORK TOPOLOGY
- SECURITY MONITORING
- EMERGENCY CONTROL
- LOAD FORECAST UPDATE
- EXTERNAL EQUIVALENT UPDATE
- CONTINGENCY EVALUATION
- ON-LINE LOAD FLOW

Data Acquisition And Processing

Security Analysis

EXIT
PREVENTIVE CONTROL
Alarm Processing

yes

Security analysis
Energy transactions

Preventive controls
Maintenance actions

no

Normal?

Fault / malfunction diagnosis

Remedial controls
Emergency controls
System restoration

Current Technologies

Limitations
Current Operating Environment

• Electricity markets
• More interconnections
• Slow increase in load
• Aging and weakened transmission infrastructures
• New information and communications technologies
Future Operational Environment

- High level penetration of wind power and other renewable sources
- Demand side participation
- Electric vehicles
- “Smart grids”
Smart Energy Management System

- DGs, renewable sources, demand side controls
- Handling system faults / malfunctions
- Dealing with cascading failures
- Wide area control and protection
- System restoration capabilities
- Dealing with cyber security threats
ALARM ANALYSIS / DIAGNOSIS
SYSTEM ARCHITECTURE

Data format information
Message/Data Interpreter
Data format information
Generalized preprocessor
Preprocessed Data
Analyze

Alarm Analysis

SER
Relay
DFR
EMS
The other devices

Data & Information
ALARMS AND HYPOTHESES

**Fault No. 1:**
- **Hypothesis No. 1**
- **At:** 12-08-98 23:10:27-000

*Line No. 1 between Baggio-Turbigo ST*
*Status: Permanent fault on phase F4*
*Hypothesis Index = 1*

No relay or breaker malfunction is found.

**Fault No. 2:**
- **Hypothesis No. 1**
- **At:** 12-08-98 23:10:36-000

*Line No. 1 between Baggio-Lacchiarello*
*Status: Permanent fault on phase F4*
*Hypothesis Index = 1*
Wind Generation Curtailment to Alleviate Transmission Overload

- Overload reduction by curtailing wind farm generation.
- Achieved by continuous monitoring and control of wind farms using SCADA.
- Curtailment decision made by operator if required for system security.
- Curtailment amount determined by linear optimization.
- Wind farm will curtail the output to the given set point.
Curtailment Procedure

1. Prepare List of prior outage events
   \{n-1-1 or n-2\} (offline)

2. Monitor critical contingency (n-1 and n-2)

3. Linear optimization determines wind generation set points

4. In case of n-2 implement Step 5. In case of n-1 wait for second contingency to occur.

5. Send new MW set point to wind farms

6. Outage cleared, signal generator to come back to normal
N-K Tripping Determination Method

Voltage is the key to determine the wind farm tripping status.

Find the voltages at fault instant, zone 1 clearing and (zone 2 clearing) at wind farm buses during the fault.

This determines which wind farm can be tripped during the fault.
Tool to identify vulnerable operating conditions of power systems

A practical index for on-line vulnerability assessment using wide-area measurement systems
Patterns of Cascaded Events

Basic patterns of cascaded events:

- Line Tripping due to Overloading
- Generator Tripping due to Over-Excitation
- Line Tripping due to Loss of Synchronism
- Generator Tripping due to Abnormal Voltage and Frequency System Condition
- Under-Frequency/Voltage Load Shedding

An effective way to prevent cascaded events:

Specifying the basic patterns of cascaded events and exploring how these patterns can be incorporated into sequences
Impedances Obtained by Power Flow and Time Domain Simulation

Post-Contingency Impedance Obtained by Power Flow Does Not Coincide with Impedance Obtained by Time-Domain Dynamic Simulations
Contingency evaluation performed on line every several minutes

Contingency Evaluation

<table>
<thead>
<tr>
<th>Case</th>
<th>Relay</th>
<th>Status</th>
<th>Contingency Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>Secure</td>
<td>3 phase fault at bus 1</td>
</tr>
<tr>
<td>2</td>
<td>Zone 3</td>
<td>Insecure</td>
<td>3 phase fault at bus 2</td>
</tr>
<tr>
<td>..</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>N/A</td>
<td>Secure</td>
<td>3 phase fault at bus N</td>
</tr>
</tbody>
</table>

Fuzzy Inference System (FIS) developed using off line time domain simulations
Power System Restoration

• Primarily manual work by system operators and restoration planners
• Off line restoration planning
• Little progress has been made on system restoration on-line decision support tools
• Little progress in system restoration R&D over the last decade
System Restoration Capabilities

- Status assessment of the grid
- Maximizing generation capabilities with the available black start resources
- Scheduling of tasks and resources during system restoration
- Establishing transmission capability and paths while meeting operating constraints
- Picking up load while meeting operating constraints and load requirements
Sequence of NBS units
• Serve Load in Island
• Establish Transmission Grid
Synchronize Electrical Islands
Evolved through generations

- Monolithic
- Distributed
- Networked
Escalating Cybersecurity Factors

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Constraints on use of existing security technologies and practices
- Insecure remote connections
- Widespread availability of technical information about control systems
Direct DoS/DDoS Attacks

Attacker compromises attack machine (the master).

The master installs attack code on slave machines, also called (zombies).

Slaves are instructed to flood the victim with packets holding spoofed IPs
Cyber Systems in Power Infrastructure
Enhancing Cybersecurity of SCADA

Anomaly Detection
- Output Anomaly Detection
  - Heterogeneous Correlation
    - Correlate Logs from Substations and Control Center
    - Correlate the Different Type of Logs from Control Centers
  - Homogeneous Correlation
    - Correlate Security Event Logs
    - Correlate System Event Logs
    - Correlate File Integrity Logs

Real-Time Monitoring
- Gather Information
  - Cyber Aspects
    - Security Logs
    - System Event Logs
    - File Integrity Logs
  - Physical Aspects
    - Critical Alarms
    - System Health Messages

Impact Analysis
- Formulate a Hypothesis
- What-if Scenarios Based on Current Network Conditions
  - Cause
  - Effect

Mitigation Strategies
- Preventive / Remedial Actions
- Decision Making
  - Prevention
  - Remedial
    - Cyber System
      - Change the Roles of User Privileges
      - Suspend Suspicious Users
    - Power System
      - Relieve the Overloaded Lines
      - Correct Voltage Problems
For Further Information