EPS Software Engineering AG
Pestalozzistrasse 27
CH-9501 WIL (SG)
+41 (0)71 914 40 50
info@eps.ch
www.eps.ch
www.ispen.ch

Software Engineering AG

Intercompro AG

ISPEN / OCD

Instant **S**ecurity **P**robing of **El**ectrical **N**etworks
Online **C**ontingency **D**iagnosis

by Intercompro.

Intercompro, lead by Dr. Ingemund Nordanlycke, has designed network simulation and modelling software for more than 30 years. Its newest package represents a further breakthrough in both performance and accuracy:

It is a true real-time contingency diagnosis software!

A lot of organisations have spend man-years into software for secure network operations using *n-1* contingency analysis. However, mostly they are of little help for the dispatcher. They consider only the online network, fail to find converging solutions, do not model phase shifting transfomers correctly and are too slow for fast emerging contingencies. Read more about ISPEN/OCD.

ISPEN / OCD
Monitoring the State of Security

Introduction

To guarantee high security of supply it is essential for you to know the current state of security. ISPEN/OCD is a real-time contingency diagnosis software and enables you to monitor the state of security.

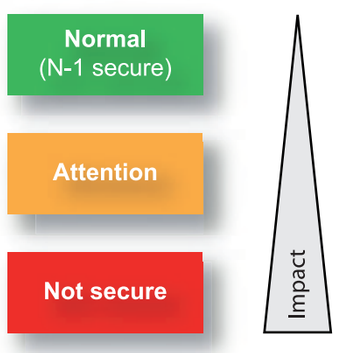
What does Security Mean?

The security of a power system refers to the degree of risk in its ability to survive imminent disturbances without interruption of customer service (security of supply).

Transmission networks are prone to outages and as a consequence to overloads. In the extreme, these can lead to instabilities and blackouts.

How Secure is Your Power Network?

Most time your network is in a normal state. However, this does not mean that the network is secure. If it is possible to simulate predefined outages and then calculate the power flow of this network, it is possible to inform you about the security state.



Green means that an outage of one element will not cause an overload. **Yellow** means that one or more branches exceed the first loading threshold. Moreover, in this case there exists a risk of cascading overloads. **Red** means that one or more branches exceed the second loading threshold and that they could automatically be switched off. Moreover, in this case there exists a risk of cascading overloads.

Online Contingency Diagnosis with OCD

ISPEN/OCD is an online contingency diagnosis tool giving you accurate informations about the state of security in a few seconds. ISPEN/OCD is a real-time security monitor. ISPEN/OCD is designed as an add-on for SCADA/EMS systems and thus can easily be integrated in your environment without extending or modifying it.

Unique features of ISPEN/OCD are:

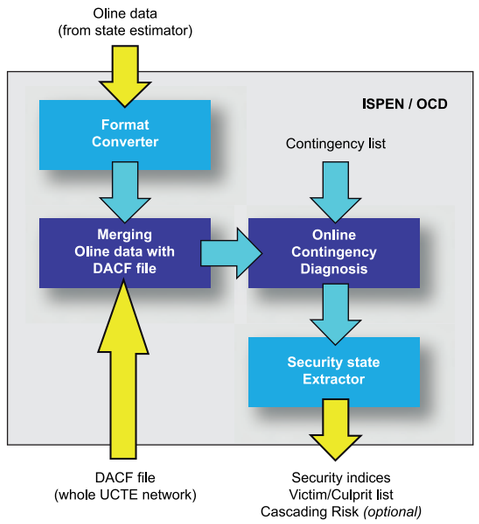
- High-performance algorithms
- High accuracy of the results
- Online diagnosis
- Short cycle time (minimum: 1 minute)
- Flat ASCII files as input and output
- Simple integration in your SCADA/EMS system
- Appropriate for networks with high transit of power
- Evaluation of cascading risk
- Accurate models of the elements (e.g. 3-port model for complex 3-winding transformer)

Principle of ISPEN/OCD

In order to get accurate results ISPEN/OCD merges your online data (from state estimator) with models or forecasts of the external surrounding network consisting of the whole UCTE network (e.g. DACF file).

This merged network is the base case of the contingency diagnosis. For every case listed in a user defined contingency list, the contingency state is now simulated.

The results calculated are condensed to a set of security indices for immediate evaluation.



Contingency List

The contingency list processed by ISPEN/OCD can be composed by a combination of single and/or multiple outage cases.

Examples:

- n-1 _ Single branch outage
- g-1 _ Outage of generation
- l-1 _ Outage of loads
- b-1 _ Outage of bus bars
- n-k _ Outage of parallel branches or a group of branches

Security State as Output

One of the outputs of ISPEN/OCD is a file containing the security indices, indicating the current security state:

1. Maximum loading [%]
2. # of objects with load > 100%
3. # of objects with load > 120%
4. # of object with re-closure angle > 100%
5. Maximum re-closure angle [°]
6. # of isolated injections
7. # of network splits
8. # of cases not solved

ISPEN/OCD provides a further output, the victim/culprit list, comprising the most affected objects and the causers of the overload condition.

Performance

The response time of ISPEN/OCD for a list of 1'600 cases with 7'000 nodes and 9'000 branches is calculated in 20 seconds on a PC (average values).

Integration in Your Existing System

ISPEN/OCD can be integrated in your existing system without modifying it. ISPEN/OCD only uses flat ASCII files as input - online data from state estimator and DACF file. Its results are written to text files, too, and can be visualized in your SCADA/EMS system or in a stand-alone tool.

Options

Optionally, ISPEN/OCD can detect cascading failures.

Applications with ISPEN/OCD

- Security monitoring
- Security monitoring with forecasting for the next hours
- Congestion Management
- Evaluation of cascading risk

Platforms

ISPEN/OCD runs on computers with standard operating systems (Windows 2003 Server & XP, Linux and VMS)

EPS Software Engineering AG
Pestalozzistrasse 27
CH-9501 WIL (SG)
+41 (0)71 914 40 50
info@eps.ch
www.eps.ch