An Expert System for Preventing Emergencies in Power Systems

Mark Jyn-Huey Lim
School of Engineering
University of Tasmania
GPO Box 252-65 Hobart TAS 7001 AUSTRALIA
mjlim@utas.edu.au

Michael Negenevitsky
School of Engineering
University of Tasmania
GPO Box 252-65 Hobart TAS 7001 AUSTRALIA
Michael.Negnevitsky@utas.edu.au

Abstract

A Java-based prototype expert system is developed for advising system operators in a power system operations control centre on how to prevent selected emergency situations. The expert system is implemented on IBM PC's in the operations control centre of Transend Networks Pty Ltd in Tasmania. This paper discusses the methods used for solving power system contingencies and the development and implementation of the Java-based expert system. The case study also demonstrates how advice is presented to the system operators.

1. Introduction

In a power system operations control centre, a Supervisory Control and Data Acquisition (SCADA) system receives measurements from different equipment that make up the power system grid. The data received by the SCADA system is automatically analysed and the system operators are informed about the current status of the power system. Equipment failure, unexpected load demand variations or catastrophic events (eg. lightning strikes, bushfires) may drive the system into an emergency state of operation. In this state some transmission equipment (eg. power transmission lines, busses and transformers) may have their voltage limit or loading ratings violated. In such cases, to avoid a failure or damage of the system equipment as well as collapse of the entire system, the system operators must take some control actions to remove these violations.

However, making decisions on the appropriate control actions to return the power system to a normal state during emergency situations is a difficult task where useful tools of artificial intelligence can be applied [1]. In a power system operations control centre, a program called the Contingency Analyser, analyses data stored in the SCADA system and runs power flow simulations of different emergency situations to predict whether the power system would be able to cope with a given emergency. If the Contingency Analyser finds any voltage limits or loading violations' while running the power flow simulation, outputs a list of these violations informing a system operator of a possible problem if a particular emergency should occur. A flow diagram of the programs and their outputs is shown in Figure 1. It is then up to the system operator to decide on what type of preventative control actions to take to prevent the power system from reaching an emergency state of operation.

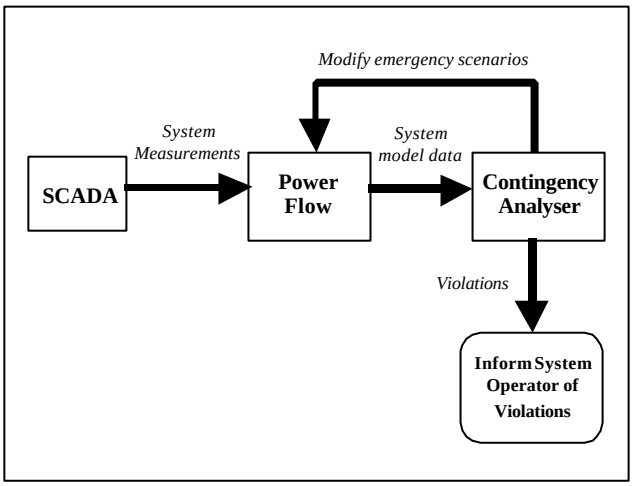

Figure 1. Flow diagram of power system operations control centre programs and their outputs.

Successful execution of these preventative control actions largely depends on an operator's skills and experience to recognise the problem and apply appropriate actions to solve it. System operators that have little experience in solving these types of problems often have great difficulty in deciding on the appropriate preventative control actions. The role of a prototype expert system in providing decision support for preventative control actions is described in this paper.

2. Power System Security Control

The type of control actions used by the system operators for preventative control is dependent on violations that are found by the Contingency Analyser. These violations can be divided into two types: bus voltage violations and equipment overloads.

Bus voltage violations occur when the voltage level on a bus is above or below specified limits. The allowance for variation in voltage level is usually ±5% of the bus rating. Control actions that can be applied to remove bus voltage violations are [2]:

- Adjusting generator excitors to change the voltage at the generation busbar.
- Adjusting in-phase transformer taps.
- Switching in-phase transformer taps.
- Switching on/off shunt reactive (capacitors/reactors) sources.
- Performing emergency load shedding at selected locations.
- Switching the transmission network.

For the case of equipment overloading, this occurs when the power flow through transmission equipment exceeds the equipment's loading rating. Power transmission equipment that can become overloaded includes transmission lines and transformers. Control actions that can be applied to remove such overloads are [3]:

- Provide full loading of the power stations and other power sources in the receiving part of the power system.
- Provide unloading of the power stations in the sending part of the power system.
- Adjust phase-shift transformers and switch capacitor banks and reactors.
- Transfer the load from one part of the system to another.
- Increase output of the active and reactive power of generators and synchronous compensators in the receiving part of the power system via their permissible short-term overloading.
- Adjust bus voltages in order to decrease the power demand.
- Curtail loads of the lowest priority.
- Switch off radial transmission lines.
- Perform emergency load shedding at selected locations.

However, determining which preventative control action to use is dependent on the effectiveness of a particular action. To determine the effectiveness of a particular action requires the use of network sensitivity methods [4].

3. Network Sensitivity Calculations

Network sensitivity methods are based on calculating a set of values (network sensitivity factors), which relate the sensitivity between a change in a control device and its effect on each element of the given power system. The control devices are generators, tap transformers, and shunt reactive sources. The elements affected by a change in the control devices are busses, transmission lines and transformers. It can be demonstrated that network sensitivity factors represent a fast way of determining the most effective control device for changing the bus voltage or power flow through transmission equipment [4].

Calculation of the network sensitivity factors takes the following form [4]:

$$\Delta C_k = C_k' - C_k^o \tag{1}$$

$$\Delta E_j = E_j' - E_j^o \tag{2}$$

$$S_{kj} = \Delta E_j / \Delta C_k \tag{3}$$

where:

- C_k^o is the original value for the control device C_k; C_k' is the value for control device C_k after a small change is applied; ΔC_k is the percentage change for control device C_k.
- E_j^o is the original value for element E_j; E_j' is the value for element E_j after a change is applied from control device C_k; ΔE_j is the percentage change for element E_j due to a small change applied from control device C_k.
- S_{kj} is the sensitivity factor relating the change in value for element E_j to a small change from control device C_k.

Using the above sensitivity factors, a sensitivity matrix is built. It relates the sensitivities between all control devices to all elements in the power system.

4. Expert System Development

The Java programming language was used to develop a prototype expert system. The preference for choosing Java rather than an expert system shell for developing the prototype expert system was Java's flexibility which allows the expert system better interaction with external programs and databases. The Java-based system also is better suited for on-line use.

4.1 Overview of the Expert System

The following diagram in Figure 2 shows an overview of how the expert system interacts with external programs in an operations control centre.

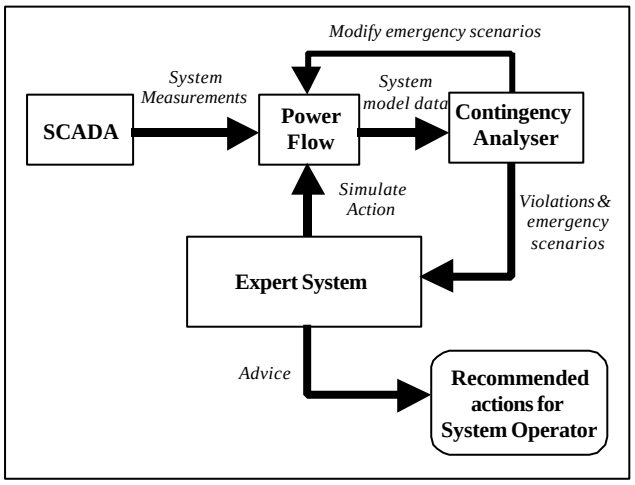

Figure 2. Diagram of interaction between external programs and the expert system.

4.2 External Programs

The Contingency Analyser is used in power system operations control centres to simulate different contingencies and inform the system operators of any violations resulting from the contingencies. The expert system is using the output of the Contingency Analyser to obtain the list of violations resulting from a simulated emergency situation. Contingency Analyser is also used by the expert system to rerun the emergency simulation after a corrective action has been applied.

The Power Flow program uses a model of the power system grid and performs calculations of power flow and bus voltages, based on a set of parameters of the power system elements. Power Flow is used by the expert system to calculate network sensitivity factors and to build up the network sensitivity matrix. It is also used by the expert system to simulate effects of a particular control action.

4.3 Database

The expert system for preventing emergencies interacts with a power system database. This database provides on-line data and is used for:

- Obtaining information on the type of emergency situations that is to be simulated.
- Checking on the violations given by the Contingency Analyser.
- Obtaining and changing the data computed by the Power Flow program.
- Obtaining information on voltage limits for busses and obtaining information on loading ratings for transmission lines and transformers.

4.4 Rule-base and Inference Engine

A rule-base is used for selecting the most appropriate control device from the network sensitivity matrix for a particular situation.

The expert system can be used in either off-line or on-line modes. In the off-line mode the inference engine performs the following steps (generating an advice – the first stage of the inference process):

- Allow the system operator to select an emergency situation being simulated by the Contingency Analyser.
- Check the database for violations generated by the Contingency Analyser for the selected emergency situation.
- If no violations are found, then stop the inference process. Otherwise select the most serious violation, based on the selection rules in the rule-base.
- Build a list of recommended actions, using rules from the rule-base and network sensitivity factors from the network sensitivity matrix.

- Calculate the effectiveness of each recommended control action by using the network sensitivity matrix.
- Sort the list of recommended actions based the effectiveness of each action and find the most effective control device.

After the inference engine selects the most serious violation and generates a list of recommended actions to deal with that violation, the system operator can then choose to simulate one of the recommended actions to see its effect. When the system operator chooses to simulate one of the recommended actions, the inference engine performs the following steps (control action simulation – the second stage of the inference process):

- Apply the selected control action to the database.
- Run Power Flow to predict the new state of the power system.
- Run Contingency Analyser to check for new violations.
- Check the database for violations generated by the Contingency Analyser after applying the selected control action.
- If there are no more violations, end the inference process. Otherwise do the first stage of the inference process again to select the most serious violation from the new list of violations and form a new list of recommended control actions.

After finishing the second stage of the inference process, the inference engine builds a list of control actions that have been simulated. The system operator can view this so that they have a complete record of the control actions that have been used.

The first and second stages of the inference process are repeated until either no violations occur or the system operator chooses to stop simulations.

4.5 User Interface

The screen dialogs shown in figures 5 to 8 show the graphical user interfaces that are presented to the system operators. Figure 5 shows the main screen interface that is shown to the system operator in off-line mode. This screen allows the system operator to view a list of contingency cases simulated by the Contingency Analyser and to select an emergency scenario to view the violations that would occur. When the system operator clicks on the "Advice..." button, the advice screen is displayed as shown in Figure 6, allowing the system operator to view advice on how to remove a violation for the selected contingency case. If the system operator wishes to view more information about a recommended control action, the system operator can select a recommended action from the list and click on the "More Information..." button. A dialog then appears as shown in Figure 7 revealing more detailed information about the selected control action.

Once the system operator has selected a recommended control action from the list in Figure 6, they can tell the expert system to simulate the effect of applying that control action by pressing the "Simulate Action" button. The expert system will then perform the simulation and refresh the advice dialog. If the system operator has requested the expert system to perform several control action simulations, a record of the actions previously simulated by the expert system can be displayed by clicking on the "Previously Simulated Actions..." button in the advice dialog. A dialog showing the list of control actions previously simulated by the expert system is then shown as in Figure 8.

5. Case Study

The prototype expert system is to be implemented on IBM personal computers in the Network Operations control centre of Transend Networks Pty Ltd, a Tasmanian company that manages and operates the electricity transmission system for Tasmania. The expert system's performance is tested on a part of the Tasmanian power transmission network, comprising of Sheffield, George Town, Hadspen and Palmerston substations. A diagram of the 220 kV network is shown in Figure 3.

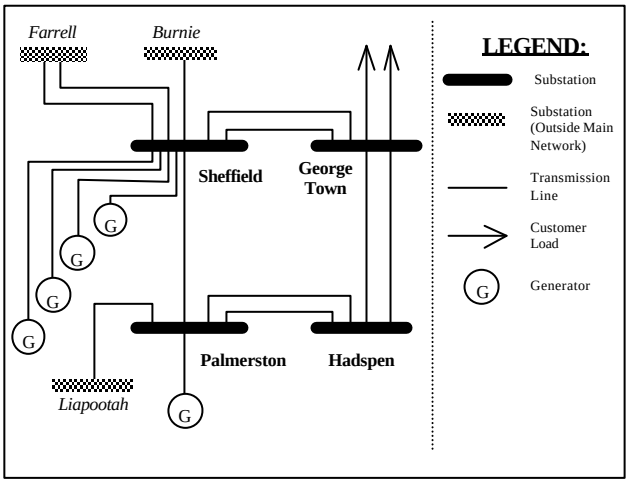

Figure 3. Diagram of the 220 kV network comprising of Sheffield, George Town, Hadspen and Palmerston substations.

The case study examines a contingency of two of the Sheffield-George Town transmission lines (i.e. the lines are disconnected from the rest of the power system). In this study, there is a large amount of power being produced by power stations on the west coast of Tasmania in comparison with the power produced by power stations in the south of the state. A diagram of the emergency situation is shown in Figure 4.

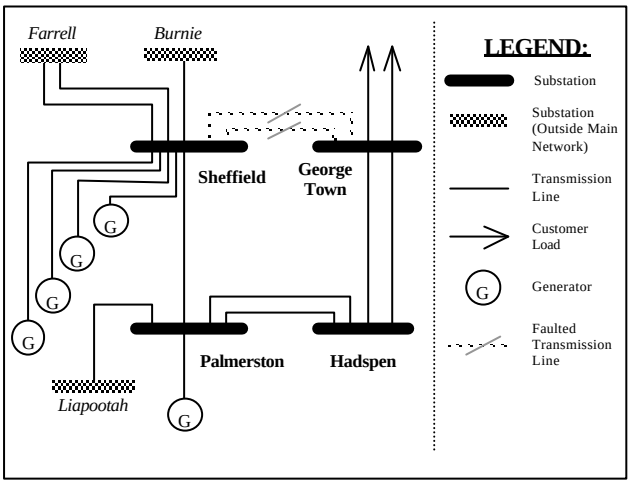

Figure 4. Diagram of 220 kV network when the two transmission lines connecting Sheffield and George Town substations are faulted.

The simulation by the Contingency Analyser found that there was one violation for this emergency scenario, shown in Figure 5. Advice given to the system operator for this scenario produced a list of four recommended actions, all sorted by the percentage expected improvement as shown in Figure 6. After selecting the first recommended action in the advice dialog, a more detailed explanation for increasing the generation at Fisher power station is given in Figure 7, showing how the control action relieves the overloading on the Palmerston-Sheffield transmission line.

After performing four control action simulations to clear all the violations, the dialog displaying the list of the simulated actions and details of their outcomes can be seen in Figure 8.

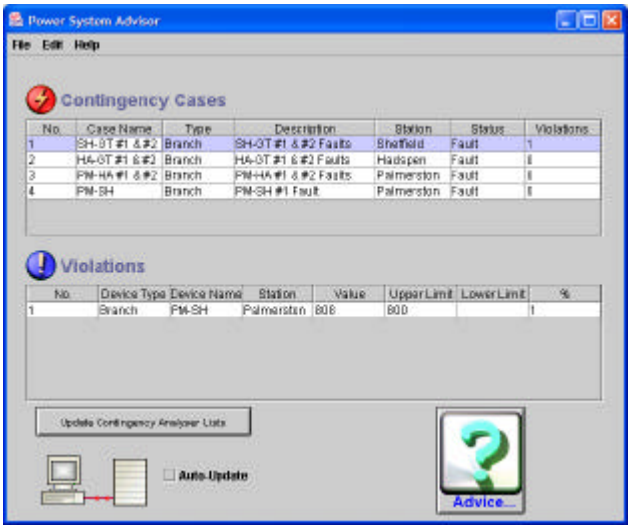

Figure 5. Main screen that displays the simulated contingency cases and violations found by the Contingency Analyser.

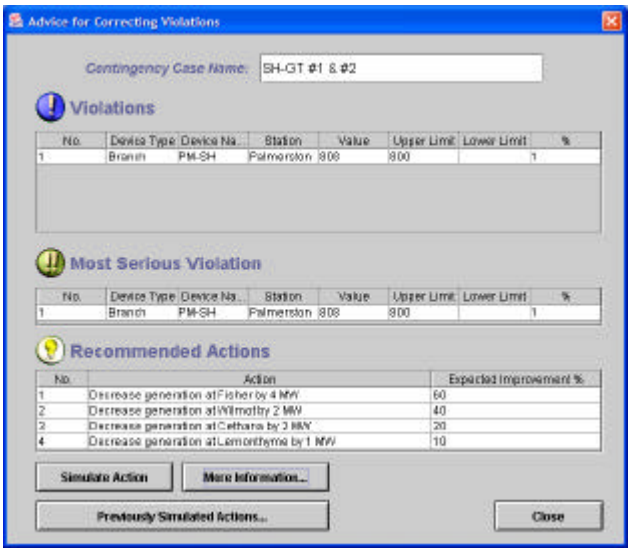

Figure 6. Advice dialog for the violations resulting from the Sheffield-George Town transmission line faults.

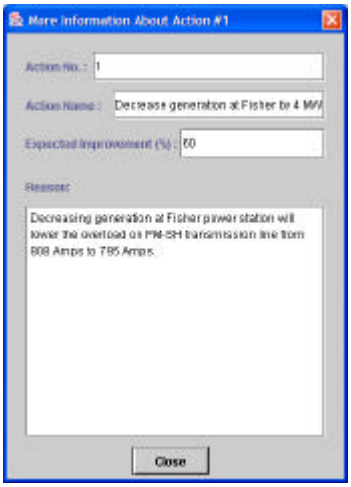

Figure 7. Dialog for explaining the reason for a recommended action.

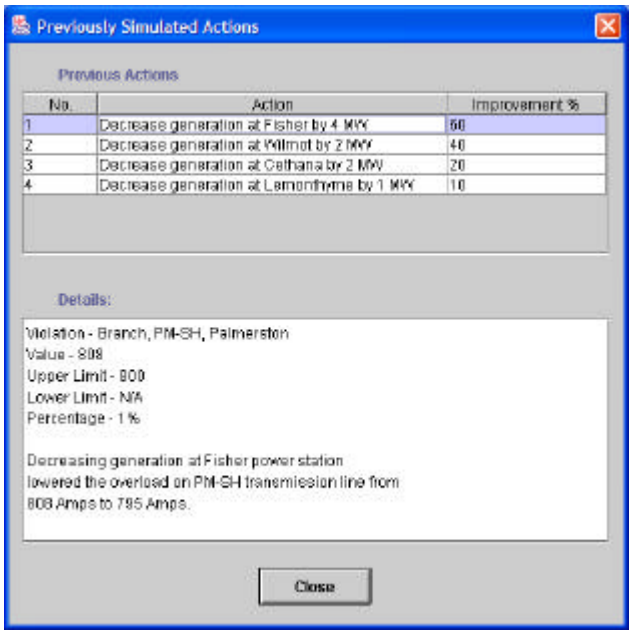

Figure 8. A dialog listing all the control actions previously simulated by the expert system.

6. Conclusion

This paper has demonstrated the development of a Java-based prototype expert system for preventing emergencies in power systems. Feasible solutions were provided to the system operators and simulated in the operations control center of Transend, Tasmania.

Currently, the prototype expert system can operate in off-line mode for simulation purposes only. Further work on the development of the Java-based expert system will include the on-line operation and providing advice to system operators in real-time during actual emergency situations.

7. Acknowledgements

This project was supported by Transend Networks Pty Ltd. Thanks to Richard Power, Mat Hosan, Michael Verrier of Transend Networks. Special thanks goes to Michael Whitehead, Craig Collins, Jan Dittmann and Stewart Sayer for contributing their invaluable knowledge towards the project.

8. References

[1] M. Negnevitsky, *Artificial intelligence : a guide to intelligent systems*. New York: Addison Wesley, 2002.

[2] C. S. Chang, "Application of pattern recognition techniques for online security-economy and reactive control of power systems," *IEE Proceedings - Part C*, vol. 138, no. 1, pp. 1-10, Jan 1991.

[3] M. Negnevitsky, "An Expert System Application for Clearing Overloads," *International Journal of Electrical Power & Energy Systems*, vol. 15, no. 1, pp. 9-13.

[4] I. Hano, Y. Tamura, S. Narita, and K. Matsumoto, "Real time control of system voltage and reactive power," *IEEE Transactions on Power Apparatus and Systems*, vol. Pas-88, no. 10, pp. 1544-1559, Oct. 1969.