Module 6 : Preventive, Emergency and Restorative Control

Lecture 27 : Normal and Alert State in a Power System

Objectives

In this lecture you will learn the following

- Different states in a power system
- Schematic of Security Assesment Procedure
- Preventive Re-scheduling of generation

A Power System in the Normal State

Once a system operator has the *static* estimate of all the system variables (voltage, current phase angular differences), he may wish to check whether the state can be characterised as a normal, alert, or emergency state.

While dynamic state information may also available, a system operator may not be able to directly utilize it since the time frame to do so may be limited (for example loss of synchronism may take place within seconds and even if an operator sees it happening, he may not be able to take corrective action). Therefore dynamic measurements can be made use of mainly by *automatic* control or protection strategies.

For the time being we restrict our discussion to static state estimation.

If all the equipment in the system are within their respective limits, then a system could be in the normal or alert state. If a system can withstand *potential* contingencies (like a fault followed by line tripping or a generator trip) without equipment limits being violated or without losing stability, then we say that the system is in a normal or "secure state". A network configuration or loading state which can withstand an element outage without loss off supply to any load is called "n-1" secure. Otherwise we classify the system as being "insecure", i.e., in the alert state.

By a potential contingency we do not mean that the contingency has occured, but has a finite chance of occuring. The classification of secure and insecure is done by simulating (mimicking) contingencies on a computer.

Normal and Alert state

To distinguish between a normal state and an alert state, a system operator carries out the following studies using the network configuration, load and generation values obtained from a static state estimation procedure:

a) Static Security analysis :This involves checking for equipment limit violations, *if* one of the elements of the network/load/generation configuration existing at that point of time were to be tripped due to some contingency. Note that this element is not actually tripped by an operator, but only simulated using a computer program (essentially a load-flow study which computes the steady state power flows in transmission lines, generator real and reactive power output, and voltages at various nodes for such a tripping).

b) Dynamic Security analysis : This involves checking the stability of the system, *if* one of the elements of the network/load/generation configuration existing at that point of time were to be tripped due to some contingency. The exact nature of the contigency can impact the transient behaviour. For example, the contingency could be due to a single phase to ground fault which results in protective action (circuit breakers disconnecting the faulted element) within, say, 0.1s. Note again, that this element is not actually tripped by an operator, but only simulated using a computer transient analysis program (which essentially does a numerical integration of the differential equations which describe the system). A computer program which checks for angular stability requires a significantly large amount of computation time. Therefore, it is not implemented in most load dispatch centres at present.

It is important to carefully choose the element whose outage is to be simulated since the number of elements in a power system are too numerous for all of them to be considered one by one. Usually a set of critical elements are chosen by some rough screening based on an operator's experience and the security analyses are carried out for the outage of these elements.

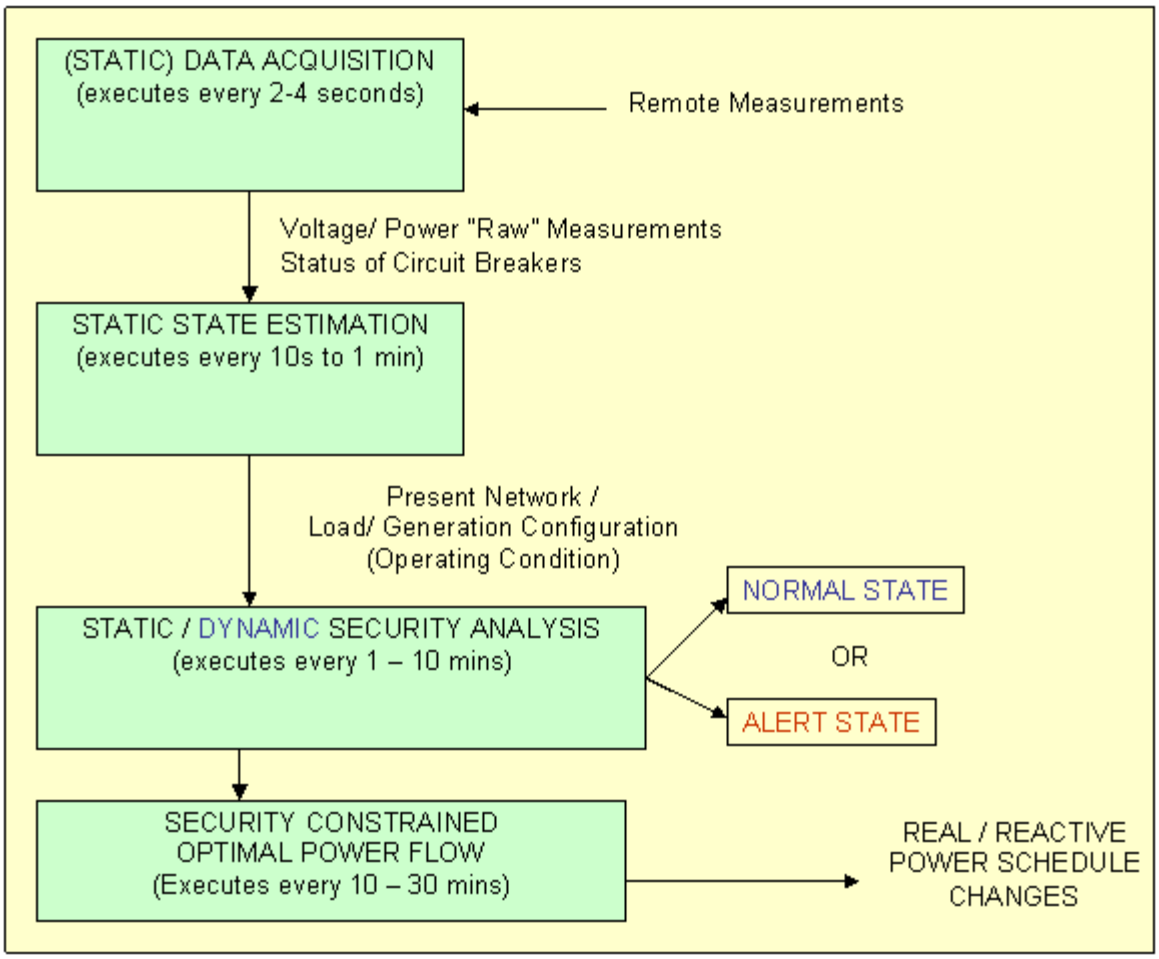
If the security analysis shows that the system is secure, it is classified as a normal state. If the state is normal, then a system operator may wish to do some minor changes in real and reactive scheduling (from an economic perspective), if such flexibility exists. However any such change should not bring the system out of the secure state.

If the system is not secure (alert), then the operator *has to* try to steer it into the secure state by real or reactive power re-scheduling (**Preventive Control**). However, note that this re-scheduling is done to improve security and may result in higher cost if cheaper generators are asked to "back down" their generated power while costlier ones are ramped up. Therefore, even if preventive control is to be done, it should be done in a way which will minimize any cost increase while simulateneously ensuring security.

This is done using a *security constrained* optimal power flow program (discussed in the previous module).

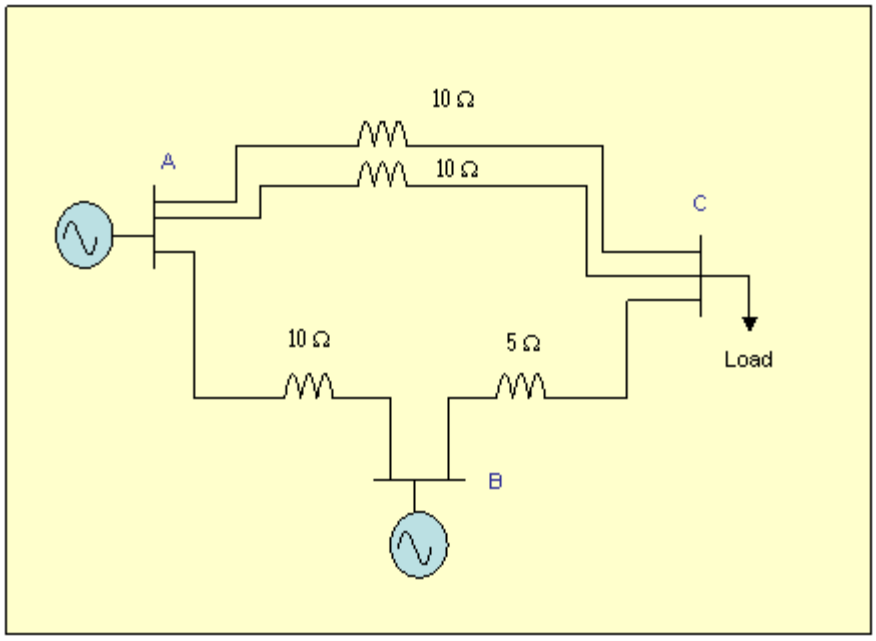
Schematic of Security Assessment Procedure

A schematic of the procedure discussed in the previous slide is shown below.



An Example

Two Generators supply a load at bus 'C' via transmission lines. It is assumed for simplicity that voltages at all buses are equal to the nominal value (1.0 pu). Also, we assume that sin(ddiff) = ddiff and cos(ddiff) = 1, where ddiff is the phase angle difference between the voltages at any 2 buses. This simplifies the circuit



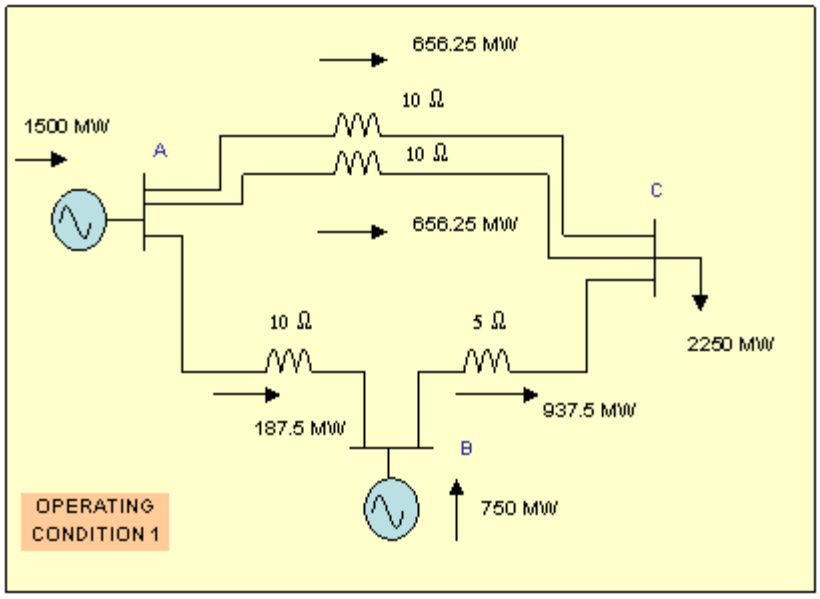
solution (load flow!) considerably.

Moreover, under these assumptions, power flow is directly proportional to the line current magnitude.

We now attempt to assess the static security of the given system.

We assume that the thermal limits of all the lines are equal and they dictate that the power flow should not exceed 1500 MW. There are other limits due to voltage & stability. However, we restrict our discussion to thermal limits only.

An Example : Case I



Here the generator at A generates 1500 MW and the one at B generates 750 MW.

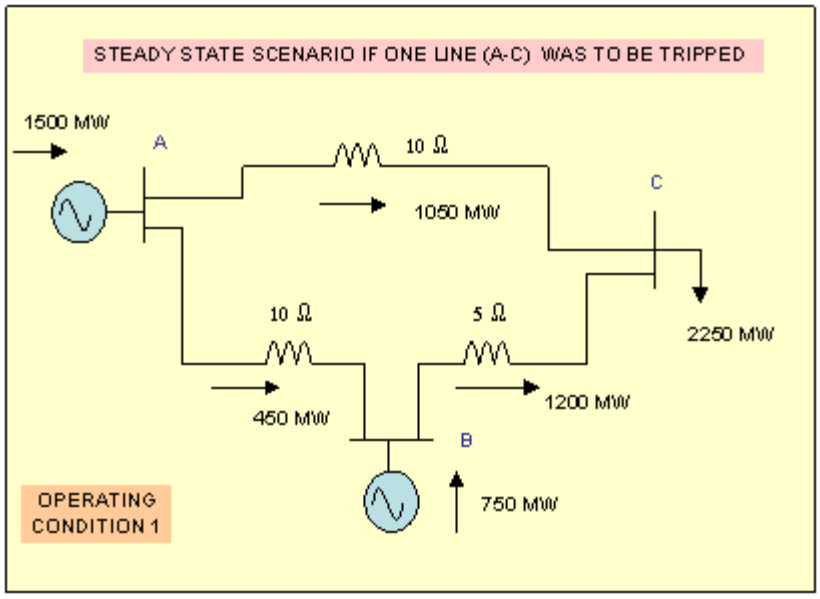
Under this operating condition, the flows for all lines are below the thermal limits (1500 MW for every line).

We are interested to know what happens if one of the lines trips.

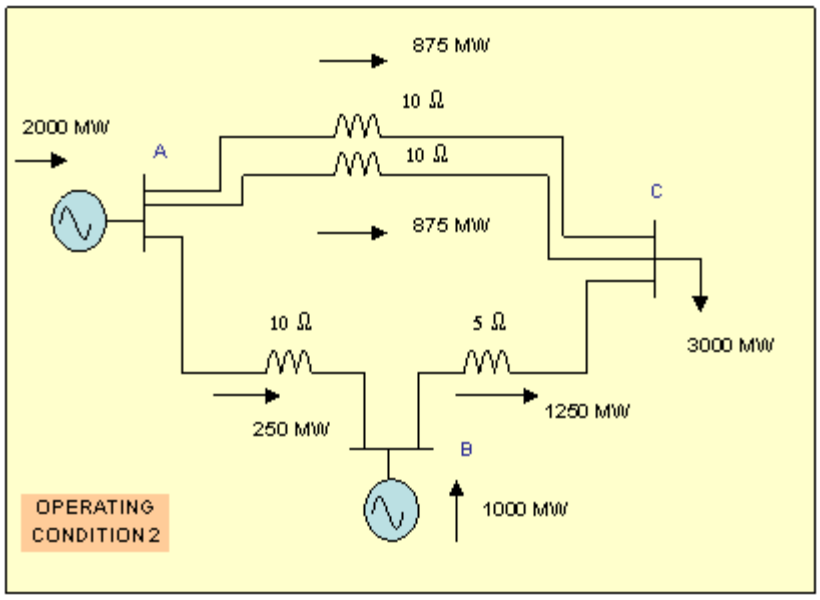
The steady state flows subsequent to the loss of one line between A & C are shown in the figure on the left.

One can verify the loss of any one line will not cause any of the remaining lines to overload.

Thus the operating condition is said to be **steady state secure** (or normal) for a line outage contingency.



An Example : Case II

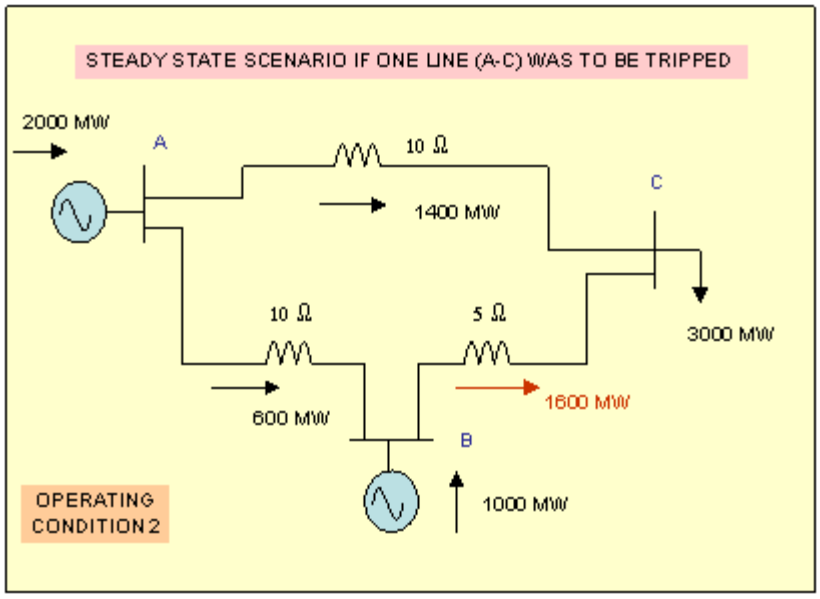


In this operating condition, the generator at A generates 2000 MW and the one at B generates 1000 MW.

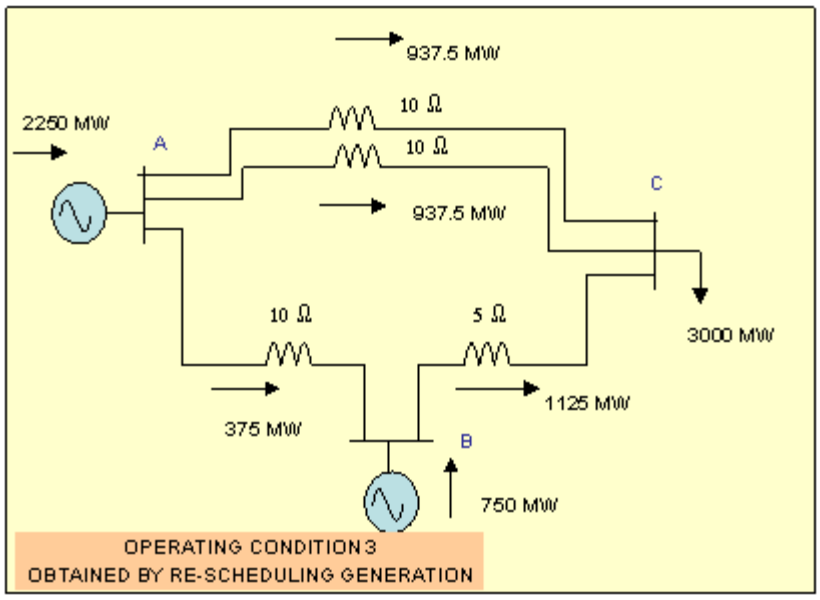
Under this operating condition, the flows for all lines are below the thermal limits (1500 MW for every line).

We are interested to know what happens if one of the lines trips.

One can verify the loss of any one line will cause line B-C to overload.



Preventive Re-scheduling of generation



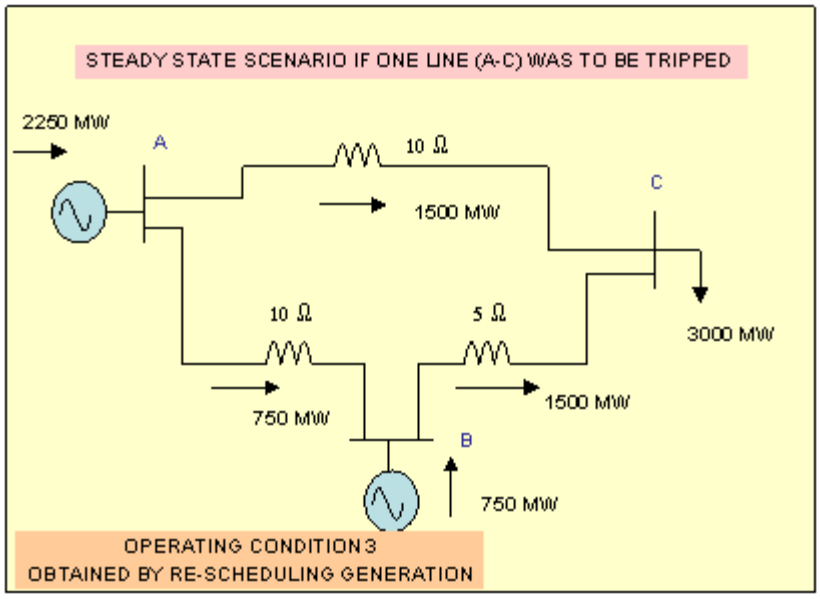
It is clear that operating condition 2 is not a secure operating condition (i.e. the system is in 'alert state')

Therefore in order to bring the system back to normal state, a system operator has to re-schedule the generation.

An adjustment of 250 MW between the generators can ensure that the system is secure, as is evident from the power flows for the contingency of line A-C outage.

Note, however, re-scheduling may increase the cost, if generation at A is costly.

This is the price one has to pay for improved security.



A concluding note: System security cannot be assessed by only considering post-contingency *steady state* power flows (as is done in the example presented). A system could be unstable (**angular and voltage instability were discussed in module 2**) for a disturbance even if a post - disturbance *steady state* exists and power flows and voltages for that steady state are within equipment limits. If a system is unstable, it will not settle down to that steady state.

The assessment of dynamic security (stability) is a more complex task as it requires numerical integration of the system dynamic equations (e.g. swing equations of all generators). This is a computationally intensive and many probable contingencies have to be considered. Direct numerical integration of differential equations can be avoided if one uses criteria like "equal area criterion" to adjudge system angular stability. However, equal area criterion cannot be extended in a straightforward manner for multi-machine systems with detailed models of all system components. Therefore quick assessment of dynamic stability is still a challenge to system engineers.

Recap

In this lecture you have learnt the following

- Classification of system into normal or alert state
- An example to illustrate preventive control

Congratulations, you have finished Lecture 27. To view the next lecture select it from the left hand side menu of the page