The distinguishing feature of modern control centers is the addition of monitoring and control functions related to the security of system operation. This brief note presents an overview of the essential features of security control. The conceptual framework and the principal security control functions are discussed.
I. INTRODUCTION

A major trend throughout the electric utility industry in the world today is the replacement of traditional dispatcher's offices by modern system control centers. The change is basically from a limited concept of generation dispatching and supervisory control to a more comprehensive and unified approach to power system monitoring and control. Modern system control centers use a systems approach for the proper integration of both automatic and manual control functions. In the design of these control centers the role of the dispatcher is considered to be an integral part of the total control system. In a modern system control center the capability to recognize the various operating conditions is provided. This man-machine system can carry out control decisions under the various conditions of power system operation.

There are a number of factors that have contributed to the need for modern system control centers. A major one is the growing complexity of utility operating problems. In a traditional control center, the dispatchers, who are solely responsible for resolving these increasingly difficult operating problems, are generally left to their own resources. They make their operating decisions based on limited information concerning the nature of the problems and the implications of each decision alternative. At best only a limited capability for systematically analyzing various decision options exists; a dispatcher must use his experience and intuition to provide answers to any "what if" questions.
In more recent years, the constraints imposed on the utility's operating environment by a variety of economic, environmental, regulatory, and other factors (such as long construction delays,) have made the life of the system operator increasingly more difficult. The inability of utilities to build badly-needed new generation resources and transmission facilities makes the present and future power systems at best marginally adequate from the operating point of view. This, coupled with the continuously escalating fuel costs, makes it mandatory for utilities to operate the system as optimally as possible. Therefore the great challenge facing system dispatchers is to operate a marginal system and to make the most out of it. In this operating environment, more hard decision making is required than ever before.

Fortunately, rapid advances in computer technology have led to a major breakthrough in the application of more powerful computers as monitoring and control aids for power system operations. Computers can provide substantial help to system dispatchers by making information, on which operating decisions are based, available where and when it is needed. In a well designed modern system control center the computer enables operators to investigate a variety of "what if" situations and to carry out certain real-time analysis functions. Thus, the computers assist the operators in preserving the system's security - its freedom from danger or risk.

We have recently witnessed the emergence of modern computer control centers at many utilities. According to a recent survey [1] some 80 modern control centers are now in service or under development. In addition, a number of utilities are in the process of identifying their needs, preparing
specifications or reviewing proposals for new control centers. Appendix A presents the relevant information on the modern system control centers covered in the survey in [1].

The major considerations that enter into the economic justification for the building of modern system control centers include the following:

. Building a modern control center is essentially equivalent to buying relatively inexpensive insurance for the big capital investment in the utility's generation-transmission system.

. Modern system control centers provide for the potential avoidance of service outages.

. The availability of real-time information allows for better economic dispatch.

II. SECURITY CONTROL

The essential difference between a modern control center and the traditional one is the implementation of functions related to system security. A conceptual framework of system security control was first suggested by Dy Liacco [2] and it has since been widely adopted. We present first a brief review of the basic concepts of security control. This is followed by a discussion of security control functions.
Basic Framework

The Dy Liacco framework considers the power system as being operated under two sets of constraints:

- Load Constraints
- Operating Constraints

The load constraints impose the requirement that the load demands must be met by the system. The operating constraints impose maximum or minimum operating limits on system variables and are associated with both steady-state and stability limitations. The conditions of operation can then be categorized into three operating states:

- Normal
- Emergency
- Restorative

A system is in the normal state when the load and operating constraints are satisfied. A system is in the emergency state when the operating constraints are not completely satisfied. A system is in the restorative state when the load constraints are not completely satisfied. This means a condition of either a partial or a total system shutdown. The conceptual framework established by these three operating states is illustrated in Figure 1.
System Security is the ability of a power system in normal operation to undergo a likely disturbance without entering into an emergency or restorative state. The objective of security control is to keep the power system operating in the normal state; i.e., to shield the power system from the risks of equipment overloads, abnormal voltages, frequency decay, system instability, loss of load, loss of generation and the ultimate risk of a catastrophic system shutdown. System security is defined with respect to what is called a set of next contingencies. This is a collection of contingencies whose selection should be based on their probability of occurrence and the consequences they would entail. The operating state of the power system is secure if no disturbance in the next contingency set could bring about an emergency operating condition and is insecure otherwise.
FIG. 1 — POWER SYSTEM OPERATING STATES AND THE ASSOCIATED STATE TRANSITIONS DUE TO CONTINGENCIES AND CONTROL FUNCTIONS
Basic Functions

For a specified next contingency set, the set of all normal operating states can be partitioned into two disjoint subsets, one with all the secure states and the other consisting of all the insecure states. Various security control functions are carried out with the help of computers to meet the objective of preventing or minimizing departures from the normal state. The general nature of these functions is made clear by considering the following sequence of operating decisions:

**Step 1:** Using real-time system measurements, identify whether the power system is normal or not. If the system is in an emergency, go to Step 4. If load has been lost, go to Step 5.

**Step 2:** If the system is normal, determine whether it is secure or insecure with respect to the specified next contingency set.

**Step 3:** If it is insecure - i.e., there is at least one contingency that can cause an emergency - determine what preventive action should be taken to make the system secure.

**Step 4:** Execute proper corrective action to make the system normal.

**Step 5:** Restore service to system loads.
Figure 2 illustrates a possible structure for the various security functions. Additional functions, required to support the security functions, are shown. These will be discussed in the following section.

The security functions in the five steps above have given the following terminology:

Security Monitoring (Step 1)
Security Analysis (Step 2)
Preventive Control (Step 3)
Emergency Control (Step 4)
Restorative Control (Step 5)

The effectiveness of system control depends heavily on the control actions undertaken when the system operates in a normal state. If a system can be controlled so that it always remains normal, then the maximum opportunity is afforded for realizing the full economic benefits of sound operation. It is basically the development and implementation of the control carried out in the normal state that represent the state-of-the-art in system control centers.

III. DATA ACQUISITION AND PROCESSING

The first step in the real-time control and monitoring of power systems is the setting up of a real-time data base. The data acquisition function starts with the measurement of the physical quantities in a power
FIG. 2 – THE SECURITY CONTROL FUNCTIONS
system such as bus voltage magnitudes, phase angles, line flows and bus power injections. In addition, data on the status (open or closed) of circuit breakers and switches are required. The measurement data are telemetered from location to the control center computer. Glaringly bad data such as transient excursions in the measured values are rejected by filtering the transmitted data through a simple check of their reasonability or of the consistency between breaker status and analog information, or by some smoothing routine.

Theoretically, one could make measurements of each physical variable of interest. However, in practice it is economically infeasible to install transducers all over the power system. There are three possible alternatives:

(1) Measuring only those quantities which would be needed to monitor certain "key" sections of the power system.

(2) Acquiring the necessary data to perform a conventional load flow in real-time.

(3) Processing all of the available data through a so-called state estimator in real-time.

We next elaborate on these three alternatives to provide the rationale for state estimation, which is the only viable option.
(1) The Inadequacy of Monitoring Key Facilities Only

The monitoring of certain key facilities of a power system results in an incomplete monitoring system. In a system with low generation reserves and limited transmission facilities, it is reasonable to expect that under certain operating conditions, any facility may become critical and require monitoring. The inadequacy of a monitoring system with a limited scope becomes clear when such a critical facility is not among the key ones which are monitored. Moreover, the objective of security analysis, which is to alert operators of unexpected emergencies, cannot then be carried out. It is exactly such unexpected situations that impose the greatest threat to the system's security.

(2) The Drawbacks of Conventional Load Flows

It is well-known that if we know the system network configuration, the status of the breakers and the switches, the values of certain variables, the real and reactive power injections at each load bus, and the real power injection and voltage magnitude at each regulated bus, then we can perform a conventional load flow calculation. The results enable us to compute any quantity of interest in the system. It would seem that the approach based on the use of a limited set of
measurements and a conventional load flow could form a complete monitoring system. However, such an approach suffers from very serious drawbacks:

a. Measurements of other variables that are easily available and have good accuracy cannot be used within this approach.

b. If one or more measurements of the quantities of interest were to become unavailable, a solution could not be obtained.

c. If a piece of the measurement data is incorrect all the results might be completely useless.

Missing and erroneous data occur frequently in the real-time environment. The following is a list of possible sources of data errors:

a. Failures in measuring or telemetry equipment.
b. Errors in the measuring instrumentation.
c. Noise in the communication system.
d. Delays in the transmission of data.

A study by AEP of grossly bad data [3] indicates that at any point in time there is a significant likelihood of having at least one bad datum point.
(3) The Role of State Estimation

Faced with errors in the measurements, missing measurements, and errors in the transmitted data we must process the available data to obtain an estimate of the state variables — the vector of bus voltage magnitudes and phase angles — of the power system. Once the state variables are determined, any other quantities of interest can be computed. State estimation is a mathematical procedure for computing a "best" estimate of the state variables of the power system.

Intimately tied in with state estimation is the determination of the current topology of the network. The tool used for this purpose is sometimes called a network configurator. Its functions are to analyze the status of circuit breakers and the telemetered measurements, and to determine the current configuration of the network.

The state estimator processes a set of redundant measurements to obtain an estimate of the state variables. The set of measurements used by a state estimator can be any combination of the following:

a. MW and MVAR line flows.
b. MW and MVAR bus injections.
c. Bus Voltages.
d. Line Currents.
The data set is processed using statistical estimation techniques which take into account the accuracy of each measurement. The state estimator obtains the current topology of the network from the network configurator, and uses this information to set up the system model. On the basis of real-time measurements, the system's state variables are estimated. These are then used to determine the real and reactive power injections at each node of the system and other quantities of interest. In this way, the state estimator provides an "accurate" estimate of the variables of interest in a power system.

The estimator reduces the expenditure for watt and var transducers and remote terminal units by allowing the algorithm to fill in the non-telemetered or missing measurements. If properly designed, a state estimator can allow the loss of a measurement without reducing the accuracy of the estimates significantly. A major benefit of state estimation is bad data detection and identification.

IV. SECURITY MONITORING

Security monitoring is the on-line identification of the actual operating condition of a system by checking real-time data to determine whether or not the system is in a normal state. The security monitoring function uses the real-time data base obtained from the state estimator and network configurator to determine which constraints, if any, are violated.
V. SECURITY ANALYSIS

If the security monitoring function assesses the state of the system to be normal, then the security analysis function is involved to determine whether the normal system is secure or insecure. The security of a system is determined with reference to a set of next contingencies. This set consists in general of certain generator and transmission outages. Existing control centers can carry out only steady state contingency studies; dynamic security analysis is still a rather distant future prospect.

Basically, contingency evaluation answers the question, "What if a contingency out of a set of probable next contingencies takes place?" The possibilities are that the system will either ride through the disturbance and settle down to a normal state, or it will find itself in an emergency state. In the latter case, the system is insecure and the contingency-evaluation function must inform the operator as to which contingency is causing the insecurity and of the nature and severity of the anticipated emergency. The ability of the security analysis function to alert operators to the possible consequences of postulated future events is especially important when the system has already undergone one or more equipment outages due to previous disturbances or operating actions.

Contingency evaluation - the study of the effects of the next contingency set - is carried out using simulation. For this purpose load flow based techniques have been implemented for the real-time environment and are known as on-line load flows. The on-line load flow employs a detailed model of the power network based on the information obtained from the network
configurator. The results of the state estimator and the forecasted loads are inputs to the on-line load flow. In addition, the on-line load flow function requires as input an up-to-date model of the external system. This is called an external equivalent. The external system is defined as that portion of the interconnected network which is outside the reach of the direct monitoring system of the power system of interest.

The simplified representation of the external system in the external equivalent is constructed using only minimal information about the external interconnection and the values of the intertie variables obtained from the state estimator. As the external equivalent must represent real-time conditions, some scheme is necessary for its updating. This is a topic which is currently in the research stage.

VI. PREVENTIVE CONTROL

If one or more contingencies in the next contingency set can result in an emergency condition (overloading of equipment, poor bus voltages, etc.) preventive actions should be taken to make an insecure system secure or less insecure. The preventive control function determines which corrective strategies (active generation rescheduling, switching of reactive sources and transformer taps, load shedding, power interchange with neighbors, etc.) should be deployed in order to bring the system back to normal. At present, corrective actions are based on operator experience and off-line studies, a procedure which is becoming inadequate. The application of analytical techniques used in optimal power flows appear suitable to the problem of determining corrective strategies; however, to date no control center has
implemented a full fledged real-time optimal power flow function. The optimal power flow problem minimizes some cost function such as system losses or production costs subject to the constraints imposed by the load flow equations, the equipment limits, operating and security considerations. Work is currently underway in the development of optimal power flow solution techniques which can be used in a real-time environment. With such techniques the proper corrective actions would be obtained as solutions to the security-constrained optimization problem. The benefits of such information to the operator in making difficult operating decisions will be substantial.

VII. REFERENCES


