243

IMPROVING RESILIENCE IN POWER CONTROL CENTRES

Working Group
C2.01

April 2004

cigré

243

IMPROVING RESILIENCE IN POWER CONTROL CENTRES

Working Group C2.01

Working Group Members

Peter ROCHE
Jose AMARANTE
Ninel CUKALEVSKI
Kurt LINDSTROM

April 2004

IMPROVING RESILIENCE IN POWER CONTROL CENTRES

Working Group C2.01

TABLE OF CONTENTS

IMPROVING RESILIENCE IN POWER CONTROL CENTRES

By

Peter Roche, Jose Amarante, Ninel Cukalevski, Kurt Lindstrom
On behalf of WG C2.01

Summary

This paper examines the factors which influence utilities, or those segments which are responsible for Power Control Centre (PCC) operations, to examine the risks posed to continuous and satisfactory operations of their enterprises. The forces which generate a need for increased resilience are summarised; the technological developments which act as enabling factors in increasing resilience are summarised.

The steps that can be taken to increase the levels of resilience are examined. The steps that can be taken in system and equipment design, staff training and business continuity planning are discussed.

Introduction

In the first chapter the paper examines the factors which influence utilities, or those segments which are responsible for PCC operations, to examine the risks posed to continuous and satisfactory operations of their enterprises. Firstly the threats to continuous and satisfactory operations must be identified; secondly the cost of countering the threat needs to be estimated and thirdly a realistic statistical risk should be assigned to the threat so as to assist in evaluating if the losses associated with the threat warrant the investment required to counter the risk.

In the second chapter the recent technological developments which have the potential to assist in improving resilience are examined. These developments may provide a computing or communications capacity or capability that was not previously available; the emergence of standard hardware or software products may now be available at an affordable price to improve the resilience of the systems.

The factors which enable company management to realistically consider improving the resilience of their PCCs are largely dependent on the growing maturity and commoditisation of the IT and SCADA / EMS market place. The emergence of a much more 'intelligent' communications networks in the power utility sector has also provided a very important capability to create resilient systems.

In the third chapter the scope of the systems and equipment which constitute the PCC are defined and described. In general the extent of the PCC is set at the boundaries of the hardware and software that makes up the central control system, together with the telecommunications and data acquisition system in substations.

In the fourth chapter the choices of system architecture, which can be used to provide a high degree of resilience to a PCC, are examined. It is noted that the objective of improved system resilience must be addressed from an architectural view-point from the outset. Over time a number of equipment configurations have emerged as being appropriate for providing a high level of resilience. Thus there are good reasons for choosing a system architecture that has 1) already been developed by a PCC supplier, 2) is provided with ongoing support from the supplier and 3) has been proven to be effective in other utilities. A number of proven architectures, that have been shown to improve the level of resilience, are described. Additionally the means by which RTUs can be switched between main to stand-by PCCs are discussed.

In the fifth chapter the key performance or design criteria which will form the basis for the design are discussed. At the outset it is clear that nature of the disaster / event against which the system must display resilience has to be defined. In addition it

is necessary to set out critical performance and availability parameters which must be achieved by the design.

In the sixth chapter human factors are shown to be important in very many aspects of the performance of the overall system. The considerations relating to planning and design of the training of personnel is explored. Not so obvious in the quest for improved resilience is the need for all relevant personnel to be trained to be aware of the cyber-based threats to system security. In particular there is a need for operations personnel to be aware of the roles and activities of the many 'players' in today's electricity market.

1. Motivators for Improving Resilience

There are many reasons why a high level of resilience is required of Power Control Centres (PCCs) – some arise as a consequence of the recent restructuring of the electric utility industry, while others are long-standing and apply regardless of the structure of the industry.

This paper examines the factors which influence utilities, or those segments which are responsible for PCC operations, to examine the risks posed to continuous and satisfactory operations of their enterprises. In order to arrive at a conclusion a three stage analysis is required. Firstly the threats to continuous and satisfactory operations must be identified; secondly the cost of countering the threat needs to be estimated and thirdly a realistic statistical risk should be assigned to the threat so as to assist in evaluating if the losses associated with the threat warrant the investment required to counter the risk.

At present many PCCs have achieved a high degree of resilience by means of duplicated systems, usually employing redundant equipment configurations with automatic fail-over. The risk that is being countered in this situation is of a limited loss of equipment or functionality. However the risk of a catastrophic loss of the entire system, while obviously low in probability, is a distinct possibility. It is this statistically unlikely event that is concentrated upon in this paper.

1.1 Extent of Power Control Centre System

In this paper the extent of the PCC is taken to extend from the actual hardware and software in the physical control centre, through the telecommunications subsystem and onto the equipment in substations, such as Remote Terminal Units or digital Substation Control Systems, plus the general overall supporting infrastructural schemes such as power supply schemes. The subsystems are briefly discussed in Chapter 3.

1.2 Cost of Non-optimised Power System Dispatch in Vertically Integrated Utilities.

Implicit in the decision to establish any PCC is the expectation that the benefits will exceed the costs. In Vertically Integrated Utilities (VIU) the business objective is to minimise total costs, while meeting specified security or reserve criteria. The benefits flowing from the effective use of Energy Management System (EMS) software are perhaps easier to estimate than those flowing from use of Supervisory Control and Data Acquisition System (SCADA). Within a VIU estimates of the benefits obtainable from EMS have ranged from 2% to 4% of the total generation costs.

It is clear that one cannot consider an EMS system in isolation – it has to be viewed in conjunction with its associated SCADA system. Thus in considering a catastrophic event that disables the EMS system, disablement of the SCADA system must also be assumed. So in order to provide against total loss of the EMS system, an alternative SCADA / EMS system needs to be considered.

The question that each PCC has to answer is: *what will the consequences be of loosing EMS or SCADA functionality over an extended period ?*

Firstly an estimate is made of the costs of the non-availability of an EMS system:

Annual generation costs per 1,000MW of peak load, with a load factor of about 60%	€200M
% loss of cost effectiveness when EMS is unavailable:	3%
Cost per month of loss of EMS facilities, per 1,000MW:	€0.5M

Secondly an estimate of the incremental cost of providing an alternative SCADA / EMS system looks exclusively at the cost of hardware and software – no account is taken of the cost of providing accommodation or infrastructural services:

Cost of base SCADA central system platform with full data acquisition facilities for a 5,000MW peak load utility:	€1M
Cost of typical EMS software and supporting hardware:	€1M
Cost of providing central SCADA / EMS system:	€2M
Incremental cost of providing a standby central SCADA/EMS system:	€0.75M

On the above simplified basis alone, it is evident that the cost of the non-availability of an EMS system can rapidly exceed the price of developing a standby EMS system. As the size of the utility – and the consequent cost of the non-availability of the EMS system - grows then the payback period becomes even less.

There is a very low probability of an event leading to the catastrophic loss of the SCADA / EMS system. Such a low probability may be dealt with through an insurance policy. Alternatively, in light of the relatively low cost of providing a standby control centre, a decision may be made to develop a Stand-by Power Control Centre.

1.3 Risk of Destruction Due to Natural or Man-made Disaster

There is always a remote possibility that fire, flood, earthquake, etc. could destroy a PCC. In the modern era when important infrastructural systems may be targeted by terrorists, a risk of destruction arises from this particular source. Some examples of disasters or near-disasters to PCCs include:

Location	**Cause of Disaster**	**Impact & Recovery**
Russia	Fire	Loss of dispatching centre
Denmark	Fire in bearing of ventilating motor	System Op and dispatch centre destroyed. Emergency Dispatch Centre used after a few hours
Western USA	Earthquake	Primary Dispatch Centre lost power and standby generator failed. System control transferred to another city
USA	Fire alarm requiring evacuation of prime dispatch centre	Dispatch recommenced in backup centre. Returned to prime centre when fire alarm was resolved.
Australia	Minor fire with release of voluminous smoke quantities.	Control transferred to alternative control centre without disruption.
USA	Cyber hackers seized 95% of EMS bandwidth.	Operations continued and issue was resolved.
USA	Cyber hackers implanted virus in PCC	Operations continued and issue was resolved.

1.4 Risks of Non-Authorised Access to PCC Systems

There has always been a risk that un-authorised access to the PCC hardware or software could jeopardise the security of operations. The risks can come from internal or external sources. The software and hardware solutions and architectures now being adopted by PCCs may make the system vulnerable to external malicious or unintentional un-authorised access. Traditionally PCCs have used conventional access control mechanisms whereby physical access was confined to authorised persons and access to software or databases was controlled by multiple levels of password control.

The actual risks to business could be any of: 1) access to confidential information, 2) un-authorised control of devices {circuit breakers, plant Automatic Generation Control (AGC)}, 3) interference with database content or IT system functioning or 4) impairment of normal operations of SCADA, EMS or other PCC applications.

The risks arise from a number of sources: 1) access to PCCs systems through a connection to the company corporate office LAN which may be designed to offer remote access for normal IT applications, 2) access via a maintenance dial-in port which is designed to allow the SCADA/EMS vendor provide remote support, 3) access to the PCC from a connection to the World Wide Web which is installed to allow remote access to operations staff who need to provide operational or software support to dispatch room staff, 4) access via a digital Substation Control System {that may be emulating a Remote Terminal Unit (RTU)} which is intended to provide remote access for relay setting / disturbance recorded data downloading or 5) access via the corporate telecommunications network, where multiple users share an aggregated data stream that may be built up of very many 64kbits/s channels originating from a wide mix of corporate business users.

The consequential costs associated with intrusion into IT systems may be most readily measured by the number of days where SCADA or EMS functions become unavailable. As estimated above the cost of non-availability of EMS in a VIU is about €0.02M per day. The cost of preventative measures will range from perhaps an estimated €500 per accessible node that is defended, plus management time, plus perhaps €100,000 per annum for a dedicated security specialist.

1.5 Potential Claims by Non-Dispatched IPP for Loss of Sale

In a competitive market a number of Independent Power Producers (IPPs) will at various times compete to provide energy or services to the market. The usual obligation imposed on the Independent System Operator (ISO) is to engage the most price-attractive offer of energy or services. The PCC's procedure for choosing the most price-attractive offer must be transparent and equitable. In the short term the ISO may rely upon short-term economic dispatch algorithms to choose the IPPs to dispatch (depending on the actual market rules applying in the area). Transmission security constraints could also cause an IPP not to be dispatched or cause a prohibitive cost/price penalty to be added to the transaction.

If the EMS system is out of service, a situation could arise where a particular IPP, whose generator was not dispatched, could claim that the non-dispatch of their generator arose as the result of the failure of the PCC to select the most price-attractive option. In the extreme the IPP could claim for loss of profit, or extra costs, attributable to the failure of the ISO / PCC to dispatch his plant. The exposure of the ISO / PCC to such a claim would depend on: 1) the obligations imposed on it by the market regulator, and / or 2) the terms of the IPP license. Each PCC will need to consider its own specific obligations and exposures to quantify the risks to which it is exposed.

The consequential costs of exposures cannot be estimated without detailed information on the particular contracts and market codes.

1.6 Complying with Dispatch Effectiveness Targets set by Market Regulator

In many markets the ISO's performance is examined post-event. The actual dispatch that did take place may be compared with the optimal theoretical dispatch and the dispatch effectiveness will be calculated. At the same time the actual costs incurred, as compared to the minimised costs, can be determined. The cost / price differences between the targets set by the Market Regulator and the actual dispatch may then be charged against the ISO / PCC. If over an extended period of time the ISO / PCC is unable to optimise their dispatch then a considerable penalty can accumulate.

Each ISO will need to consider the possible penalties that might arise if their EMS / SCADA system is unavailable. This analysis may lead to a conclusion that an investment should be made to reduce the risk exposure under this heading. The consequential costs of exposures cannot be estimated without detailed information on the particular contracts and market codes.

The costs of not meeting the set targets may not be very different from those discussed in Section 1.2 above. The price of establishing a Stand-by PCC, as a means of offsetting this risk, are also presented in Section 1.2.

1.7 Company-wide Business Continuity Planning

The concept of Business Continuity Planning (BCP) is a philosophy that is being adopted by many of today's businesses. As part of the implementation of BCP, key activities are identified, their importance is determined and the consequences and costs of failure to provide the service are estimated.

Within a VIU or ISO the responsibilities of the PCC are key business activities, no different from those of issuing bills, physically restoring electrical supplies etc. Thus the BCP type analysis can be applied to ISO / PCC activities and conclusions drawn as to what steps should be taken and what investments should be made to assure the resilience of Power Control Centres.

The analysis of PCC operations and the application of company standards may then lead to the determination of tolerable durations of disruptions and acceptable costs for providing standby facilities. Plans can then be drawn up for providing the agreed levels of standby services.

2. Factors Assisting in Improving Resilience

In responding to the need to improve the resilience of PCCs, one can exploit a number of relatively recent technological developments. These developments may provide a computing or communications capacity or capability that was not previously available; standard hardware or software products may now be available at an affordable price to improve the resilience of the systems.

The factors which enable company management to realistically consider improving the resilience of their PCCs are largely dependent on the growing maturity and commoditisation of the IT and SCADA / EMS market place. The emergence of a much more 'intelligent' communications networks in the power utility sector has also provided a very important capability to create resilient systems. In the following subsections the main developments that can support an increase in resilience are briefly described.

2.1 Higher Processing Power of Modern Hardware

The continuing growth in the processing power and improvement in the price performance ratios of computers has acquired the status of a natural law – Moore's Law – which states that processing power of computers doubles every 18 months. For a small fraction of the price of a mini-computer of the 1970s, one can now buy a Pentium processor, with a clock speed of 1.8GHz and a processing power equivalent to many powerful mini-computers.

The availability of very keenly priced hardware has effectively made almost unlimited processing power available to the PCC. Thus the most complex algorithms and processor intensive applications can be executed at a rate which meets all of the performance and response requirements of very large utilities – and at a modest price for the necessary hardware. Most requirements for processing power needed to enable Stand-by PCC to replicate activities in the main PCC are readily met by modern technology at relatively modest costs.

2.2 Large Capacity and Distributed Databases

The introduction of 32-bit hardware – and more recently 64-bit hardware – has enormously increased the manageable size of databases. Effectively there is no upper limit on the number of data-points that a SCADA system can now handle.

Many manufacturers now offer Data Base Management Systems which can be 1) geographically distributed and 2) processed through standard SQL interfaces. Coupled with the larger capacity database is the ability of fast processors to search, retrieve and manipulate data from such large files. This ability is in turn built on the very large capacity disk storage devices with their short data access times.

All these factors have made it possible for modern SCADA / EMS systems to deal with models of very large power networks in a highly responsive manner – in a way that earlier computer systems could never emulate. Equally the advances in technology enable replica or shared databases to be established, e.g. as may be required for a Stand-by PCC to shadow the actual PCC databases.

2.3 Standardised Software and Protocols

The algorithms needed to support State Estimation, fast decoupled load-flows etc. were largely well developed many years ago. More recently Optimal Power Flow packages became widely available. The low price of high performance processors means that it is now economical to run computationally intensive applications, in a manner which was unthinkable a decade ago. Thus a PCC can now install and operate virtually any application that it chooses. Additionally the price of all applications software is falling. Stemming from 2 factors – firstly there is a larger customer base over which the development costs can be spread, secondly an improvement in the quality of software and a greater degree of standardisation -- means that customisation costs have reduced.

Over recent years internationally accepted telecommunications standards have been more widely adopted. For inter control centre links the UCA / ICCP (TASE 2) protocol has been adopted in preference to the ELCOM (TASE 1) protocol. For communications with RTUs the IEC 60870-5 series of protocols has been adopted widely, with DNP being used frequently in North America. With the adoption of these standard protocols the task of setting up and communicating with PCC and emergency PCCs has been greatly eased. Naturally the cost of commissioning systems using standard protocols is generally lower than when proprietary protocols are used.

2.4 Bandwidth and Capacity of Telecommunications Networks

A generation ago many links supporting SCADA applications relied on Power Line Carrier equipment, or on analogue voice channels on pilot cables. The effective available bandwidth was probably under 2,400 bauds.

The rapid installation of high capacity digital radio links and the increasing deployment of fibre optic facilities are 2 examples of how a modern utility is now moving into a situation where the basic building block for any application is at least 64kbit/s. Indeed with the increasing deployment of Synchronous Digital Hierarchy (SDH) or Synchronous Optical Networks (SONET) links in fibre optic networks, bandwidth in multiples of 2Mbits/s is readily available. The ready availability of such high-speed links, and of very high capacity backbone networks, makes the design and

implementation of links from a PCC to remote substations or to other control centres easy to implement.

2.5 Intelligent Networks which Route RTU Signals Adaptively

In order to provide resilience for communications from a PCC to its RTUs and from one PCC to an interconnected PCC, it has been traditional to use duplicated telecommunications routes, with automatic switchover between the routes. The traditional mechanism was to assign a separate physical connection to each of the redundant routes. This effectively 'hardwired' the devices together and thereby presented a difficulty if, for instance, the RTUs were to be switched to a Stand-by PCC. The advent of intelligent telecommunications based on digital technology has fundamentally altered this situation.

Modern digital telecommunications systems employ a Network Management System (NMS) which can be configured with a series of routing tables. The basic routing table may be used when all elements of the network are in service and data flows along 'primary' routes. On the detection of a fault the NMS will identify the location and extent of the disruption and can then invoke an alternative routing table, (of which there will be many) which will attempt to re-route traffic past the fault. Such a NMS mechanism can make better use of network data carrying capacity, can obviate the need for the assignment of a fixed 'alternative' route and can more efficiently respond to network problems.

Specifically for the improvement of resilience the NMS features can be exploited to detect and react to the loss of the PCC and to automatically route RTU data to another predefined location, e.g. the Stand-by PCC. Thus the implementation of fall-back traffic routing procedures can be automated with modern technology.

2.6 Improved Resilience for Hardware Units

In any SCADA / EMS system there are many points of potential hardware failure – e.g. multiplexer I/O cards, SDH / PDH / SONET network element cards, power supply boards in RTUs, etc. With the increasing modularisation of electronic equipment it is possible to include a specified level of redundancy in the basic hardware design, at relatively low incremental cost. The concept of including standby hardware is sometimes referred to as 1:n level of redundancy. By including such additional hardware an improved level of resilience can be incorporated into the PCC supporting systems.

2.7 Protection against Un-Authorised Access

The risks associated with un-authorised access can be mitigated by a number of methods, both technological and organisational. On the technology front the following mechanisms can be used to improve security and resilience: 1) access to all functions permitted only after entry of correct passwords, 2) dial-up access confined to a small closed group of VPN (Virtual Private Network) users, 3) dial-up always initiating a dial-back connection, 4) implementation of Firewall security provisions, 5) employment of encryption techniques where appropriate, 5) restriction of Web access to information retrieval only, with no capability for command issuance.

Technology alone can never adequately protect against un-authorised access. Active management involvement in the design of security systems, in the review of the effectiveness of the systems and in keeping abreast of best practices and of recent threats can improve the resilience of a PCC.

3. Major Subsystem in Power Control Centres

In considering ways of improving the resilience of PCCs, it is necessary to define the scope of the systems and equipment which constitute the PCC. In general the

extent of the PCC is set at the boundaries of the hardware and software that makes up the central control system, together with the telecommunications and substations data acquisition systems. The major subsystems being examined in the context of improving the resilience of PCCs are briefly described below.

3.1 Control Centre, Substation and Generating Plant Equipment

Included here are all hardware and software components which support SCADA, EMS, inter control centre links and other vital activities of a Power Control Centre. The basic hardware will include the HMI consoles, the supporting servers, the LAN, Front End Processors, routers supporting communications with external processor, etc.

Under the heading of software will come the basic Operating System, SCADA, EMS and other applications software. Where web browsers are included these are a vital part of the PCC, which require special consideration, especially from the viewpoint of access control.

The equipment in substations and generating plants will include RTUs, any special AGC interfaces, interfaces to digital control systems, power supply equipment such as battery / charger systems, etc.

3.2 Telecommunications System

Included here are all elements of the links from the Front End Processors as far as the RTUs or to other interconnected control centres. Both the basic hardware and the superimposed Network Management System software are of particular interest to the PCC. It should be noted that the PCC is typically one of many users of a multi-user high capacity telecommunications network. Other business units will share the network resources, perhaps even sharing capacity in 2Mbits/s data streams. Of particular concern to the PCC may be the fact that the Network Management System, the multiplexers and network elements may be managed and accessed by non-PCC staff.

3.3 Infrastructural Systems

The infrastructural subsystems are particularly important in the control centre proper. The subsystems include Uninterruptible Power Supply (UPS) schemes to maintain continuity of supply to the PCC hardware, air-conditioning schemes, fire detection and extinguishing systems, security and access control systems, etc.

4. Choice of System Architecture

In order to provide a high degree of resilience to a PCC, the basic system architecture must be appropriately designed from the outset. Over time a number of equipment configurations have emerged as being appropriate for providing a high level of resilience. In theory it may be possible to arrange the basic elements of a PCC in a large number of different configurations in order to achieve resilience. But as every utility has learnt from experience, to adopt a non-proven solution can be unwise, expensive and prone to unpredictable delays. Thus there are good reasons for choosing a system architecture that has 1) already been developed by a PCC supplier, 2) is provided with ongoing support from the supplier and 3) has been proven to be effective in other utilities.

In the following subsections a number of proven architectures, that have been shown to improve the level of resilience, are examined and described. In the first 4 subsections different configurations of main and stand-by PCC are described. In the last subsection the means by which RTUs can be switched between main to stand-by PCCs are discussed.

4.1 Mirror Image Standby Power Control Centre

With the current hardware prices it is "affordable" to install a second computer system, being a mirror image of the main one. The affordability comes from the percentage of the total system price needed to achieve this goal and while some years ago the system incremental price could be more than 50%, now it may be in the range of 10-15% and will have a tendency to decrease.

Before the award of a new contract (this will not be the case when a system has already been installed) it will be relatively easy to convince the supplier that the software licenses being bought for the main system should also apply, at no extra cost, for the backup system, since the systems will not be used at the same time. Engineering of the system may imply some extra costs but the client may also argue that, after the commissioning of the main system, it is straightforward to make a full backup and then use the media to restore the already configured software at the backup system. These operations will be the easier to achieve as the backup system is almost identical to the main system.

With this type of price increment, building up a backup control centre is highly affordable. After installing the first SCADA system, the ISOs normally initiate a process of de-manning the substations. If SCADA is used not only as data provider to the EMS system but also as a telecontrol tool to perform switching operations, the complete loss of the control centre, that might have been tolerable years ago by redeploying the substations' operators to their old jobs, is no longer an option.

Although Moore's law has stayed unchallenged for a considerable time, experience has also shown that whatever their size disks get always full after less time than expected and CPUs which seemed so powerful become overburdened after some time. This means that, in order to keep the system at an acceptable performance level, there is a need to upgrade the hardware and when this needs arises, the user is already a captive customer of the supplier and the supplier will try to get (at last) a return from the investment he has made, to get more market share, when he sold the system at an alleged loss.

The mirror image Standby PCC shows then the problem that you have to update two configurations instead of only one and the engineering costs presented by the supplier will be larger than for only one system. Maybe the supplier will also try to get some extra money for the extended licensing. Although the software management work will not be the double of the "only one centre" situation, some effort is also needed to keep the standby centre as a credible working replica of the main one. So, the total lifecycle cost increase of one backup centre will probably be higher than the 10-15% portion of the initial purchase.

Even if the existence of an idle standby system can be justified from a security point of view, engineers do not like to have idle equipment and the first candidate that may be proposed to avail of all the available computer power is naturally the OTS (Operator Training Simulator).

4.2 Installing Half of the System at Each Centre

Another possibility to minimise the amount of idle equipment, when there is a redundant high-speed link between both sites, is to dispense with a duplicated configuration at each of the sites, the hot standby function being assured for each machine by its duplicate at the other site. The existence of 2 links at 2 Mbits/s each will be probably enough for the RTU data traffic and for the MMIs. As the EMS suppliers have now experience with Relational Database Management Systems (RDBMS) they will be able to specify the minimum acceptable bandwidth between the two sites to have acceptable synchronisation times between the DBs, which are probably the heaviest consumer of the bandwidth.

This architecture has the obvious advantage of reducing the extra hardware needed. There are other costs associated with a second control centre, viz. a full duplicated UPS, redundant high-speed links, LAN infrastructure and some extra MMIs but no extra servers will be necessary. This solution has also the advantage that there is almost no increase in the software management of the system and there is a guarantee that the standby system will be an updated replica of the main one when any disaster occurs because there is, from a logical point of view, only one system.

The obvious disadvantage of this type of solution, half the system at each site, is that in case of a catastrophe there remains only a non-duplicated system. However, it will be relatively easy to buy extra standby machines when that occurs, if the owner takes the precaution to keep its system updated and compatible with the machines available at the market. This will imply, for instance, the need to ensure that the latest operating system version of the computer vendor is installed. In any case, the situation will be much easier to solve than to have no standby centre and the additional risk may seem acceptable to many utilities.

In this half-half solution there is a situation which must be considered, viz. when the redundant high-speed link fails. In principle there will be a distributed front-end system and the data from the RTUs will normally be arriving only to one of the sites, or may be arriving to both but only processed in one of them. When the link breaks, then at each pair of primary-hot standby servers the following will happen:

- the primary server will consider that the stand-by has failed since communication with it was lost,
- the standby server will consider that the primary has failed and will become primary.

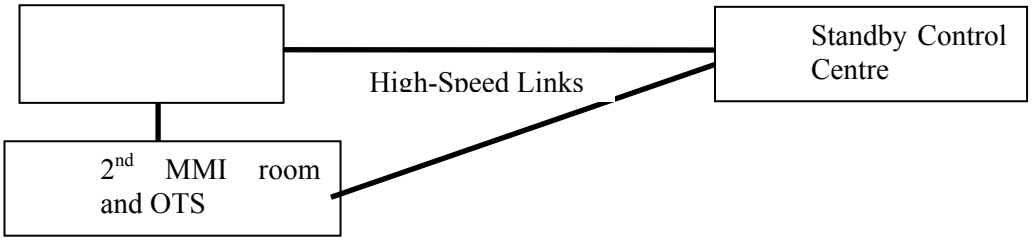
So, in each site we will then have a full set of servers as primary machines and the communication with the RTUs during this split situation must be considered. The systems will evolve differently and when the link is re-established one of them must "die" and its historical data will be lost. The AGC function must be managed with special care because there should not be two active AGC programs over the same electrical system! These are the main problems associated with this half-half solution and if they are considered at the design phase they will not be hard to solve.

4.3 PCC with Reduced Level of Functionality

Some years ago, when computers were very expensive and the dependence on SCADA systems was not so strong, "emergency control centres" were implemented with a small subset of the information available in the main control room. With the increasing dependence on computerised tools for the operation of the network and the more complex interfaces with the several new actors of the electrical system, the PCC will require full access to all the data available in the main control centre. Thus there may not be much benefit for the intermediate solution of a "Reduced Functionality PCC".

Nonetheless, the displacement of the personnel from destroyed primary control room to the standby control room may cause great inconvenience for the involved operators and that can be made worse by large distances between the centres.

A compromise to avoid that inconvenience is shown below:



By setting up in a different but nearby building a 2nd room with MMIs, in the case of a fire in the main PCC, the operators may move only to that room instead of having to move to a distant town. Care must be taken in the establishment of the connections to avoid any dependence of the connection between the 2nd MMI room and the Standby PCC. As the 2nd MMI room is near to the main building it will also be easy to connect the LANs in the two buildings. As the second MMI room is prepared to accommodate the operators, it makes this room a very good place to conduct the OTS sessions.

However this solution does not adequately address a geographically widespread disaster.

4.4 1:n Redundancy for a Number of Control Centres

The hierarchical organisation of the real-time data flow in large ISOs was very common: RTUs communicated directly with the first level of telecontrol centres and these shipped a subset of their data to the control centre at the next hierarchical level. In some ISOs there were two hierarchical levels, in others even three. The problem with this type of organisation is that when there is a catastrophe at one of the centres, large portions of the network become un-observable to the higher level centres. There is also another inconvenience in this arrangement, related with information at the borders of two centres of the same level controlling adjacent areas of the network. Each centre is blind to the neighbouring substations and that makes the reconnection of adjacent zones more difficult.

With the current tendency to reduce costs, some companies have their centre fully manned during working hours but try to reduce the number of shift operators during the night, handing over the control of one control centre area to another one.

This kind of difficulty has provided an incentive for RTUs to be able to talk to more than one centre. Although in some systems the RTUs keep having a "normal" master, which has the responsibility to transmit the RTU data to one or more centres, in case of failure of this centre, another one may start to interrogate the RTU and transmit its data to the other interested centres.

Not all control centre software supports this type of switching. The majority of available control centre software is able to get data either from its "own" RTUs or from "foreign" RTUs, via a link with the centre owning the foreign RTU.

Two figures to illustrate this issue are shown below:

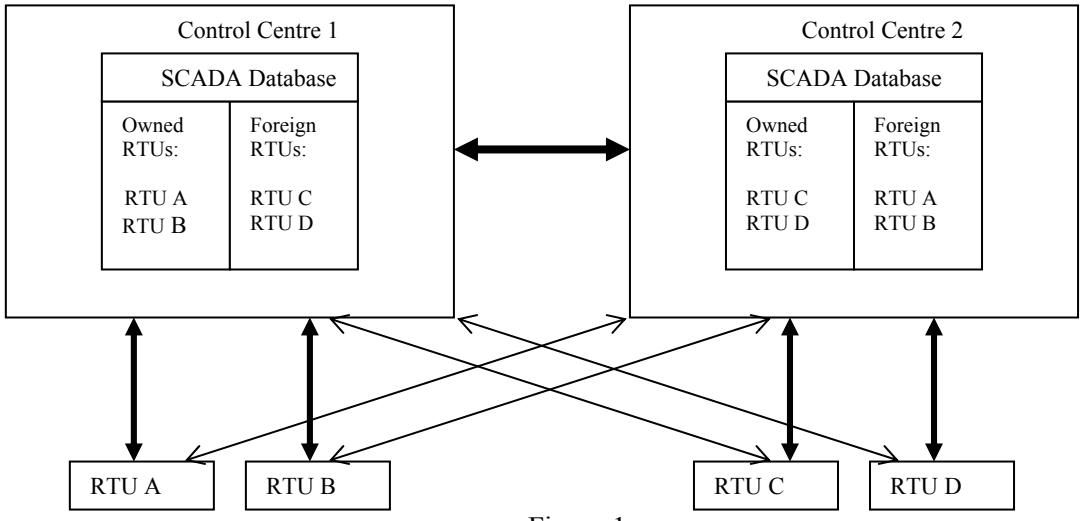


Figure 1

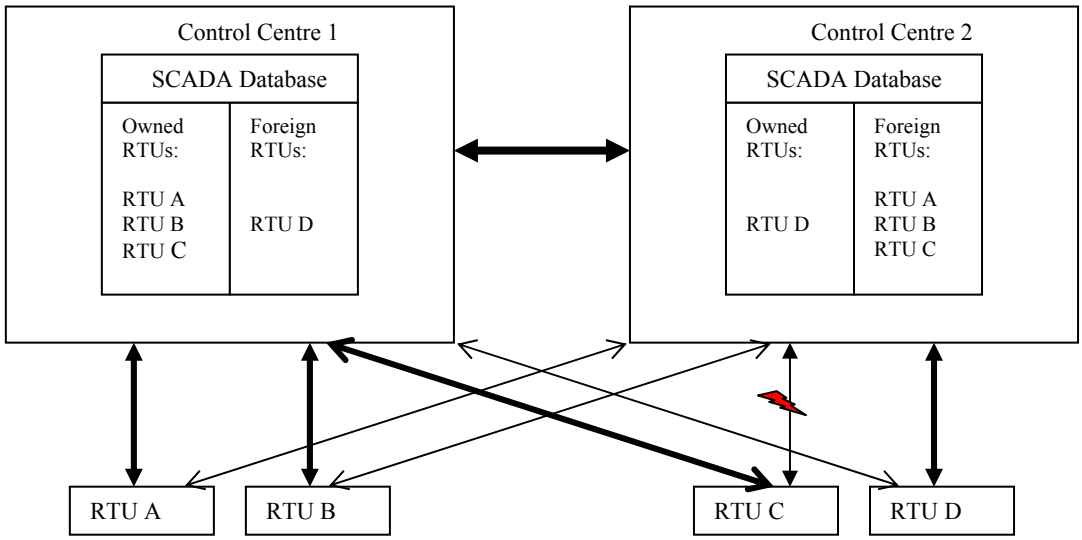


Figure 2

The first figure shows the normal situation where RTUs A and B are directly connected to Centre 1 and RTUs C and D communicate directly with Centre 2. In this situation the Centre 1 gets the data from locations C and D *via Centre 2* and Centre 2 gets data from A and B *via Centre 1*.

In the second figure the link between Centre 2 and RTU C has failed and the direct link between Centre 1 and RTU C has been activated. RTU C now "belongs to Centre 1" and the SCADA Databases have to be updated accordingly. "Belonging" should not prevent the RTU from receiving telecontrols from Centre 2 *via Centre 1*.

In the real world there are usually intermediate devices between the Centres and the RTUs which make things a bit more complicated but the above diagrams give a general idea. RTUs do not need to be dual ported because at each time they are only talking with one of the Centres.

When **Multi-site** is supported, switching RTU C belonging from Centre 2 to Centre 1 and vice-versa is an easy task. The switching may be done by a shift operator, or even automatically by the system.

If there are two or more centres and a data communications network incorporating this multi-site concept, there may be no need for setting up a backup control centre for real-time data acquisition, since each one may have the capability to become a full backup of all the others.

However, EMS functions are normally performed at only one site per ISO, so there will be a need to install additional servers at one of the other sites. Historical data should also be periodically shipped to the other centre. The increasing interactions with the market must also be considered and additional PCs will need to be installed there, along with some extra MMIs. If the dialogues with the market are done via Internet the needed additional infrastructure will not be significant.

Last but not least, when two centres perform different functions the operators from each centre will not be able to substitute for their colleagues unless they have been trained to do so. This means that although each centre may be a backup of the others it will be necessary to relocate some personnel from the failed centre to another place in order to maintain normal operations.

4.5 Redundant RTU Communication from Prime and Backup Control Centre

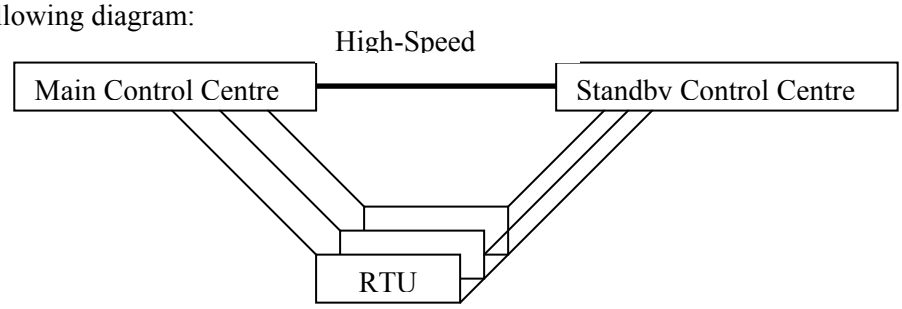
A vital consideration in increasing the level of resilience concerns how RTUs are switched from one control centre to another. A number of solutions have been successfully adopted: one solution requires the use of dual-ported RTUs, another

utilises a distributed configuration of Front-end Processors while yet another exploits the inherent circuit switching abilities of an intelligent telecommunications network.

4.5.1 A Classical Approach

For a system employing classical RTUs, with each one communicating with its master control centre using a proprietary protocol, the building of a new telecommunications infrastructure capable of supporting the existence of a primary and a standby control centres is probably the biggest challenge.

As a first approach there is the possibility to consider the solution presented in the following diagram:



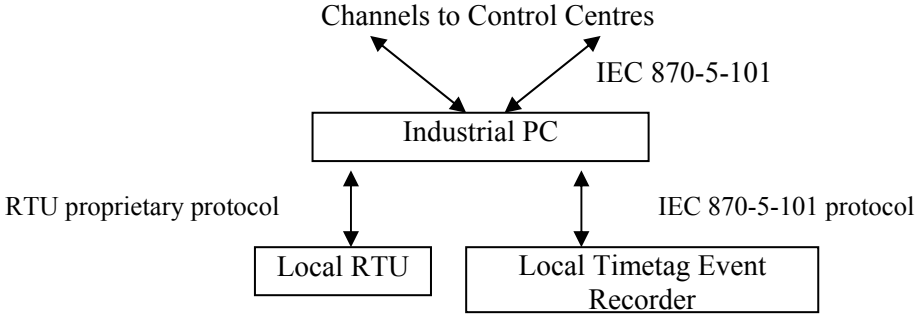
In the diagram each RTU is connected to both centres by a point-to-point communication channel. The redundancy of the RTU communication is split between both centres because, if half of the RTUs were to be linked by redundant channels to only one centre and the other half to the other, that would mean that in case of catastrophe the remaining centre would only have access to half of the installations.

To avoid changes in the RTU hardware, the centres must coordinate between themselves which one will talk with the RTU at each time and the simpler solution will be to have all RTUs talking to the main PCC, only changing to the standby PCC in case of failure of main one. This raises the problem of channel failure monitoring, being probable that, unless active channel monitoring is practised, several channels connecting RTUs to the standby PCC will be out-of-service.

For a long time the RTUs employ a bus structure with one controller card and dedicated cards for indications, measurements and controls. It may be possible to change only the controller card for a new type, allowing dual-porting of the RTU (the RTU being capable of reporting to two masters) and eventually to make its protocol compliant with the IEC 870-5-101 standard, making the installation of the new control centre easier. However, the RTU owner is by this time a captive customer and the RTU supplier will probably bid high prices for the controller substitution.

For processing the RTU proprietary protocols, the cheaper location would be the front-end, because these are now intelligent devices and the processing requires no extra hardware. However, if it is decided in the future to change the control centre it will be necessary to provide special support for the proprietary RTU protocol.

One system is known of where a PC was installed in front of each RTU, this PC talking to the RTU in the proprietary protocol and to the centres in IEC, allowing access to Local Timetag event recorders and also providing the convenience of the dual-porting, as shown in the figure that follows.



In this system and in a few other cases, one or two additional remote RTUs (not possessing telecontrol capability) have additionally been connected to the industrial PC, turning it into a kind of data concentrator. The rule was

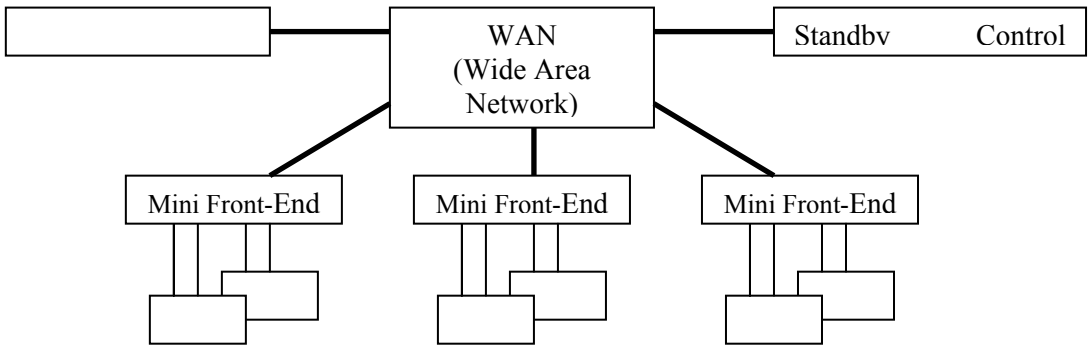
⇒ not to lose the telecontrol of more than one installation when one PC fails, although data acquisition from more than one installation would then be lost.

The disadvantage of doing the protocol conversion at each RTU instead of the front-end lies in the need to buy an extra PC for each RTU and of decreasing somewhat the reliability of the RTU which then becomes also dependent on the availability of the PC.

To create large data concentrators for aggregation of channels before routing them to the two PCCs should in principle be avoided since the catastrophic loss of any of those data concentrators would prevent large portions of the network to be known and controlled by the PCC.

4.5.2 Using a Distributed Front-end Configuration

An alternative to the design previously presented, in modern circumstances where the front-ends are built around LANs, is to use the "Distributed front-end" approach, illustrated in the following figure:



This approach looks very attractive because it is consistent with the increasing availability of high bandwidth links. For many substations there are strong communications links and a high-performance WAN with dynamic rerouting in case of failure of one or more single links. However, there may be some substations where installation of fibre-optic or microwave is hard to economically justify and their connection to the WAN is a problem. In this type of situation the bandwidth capacity is no longer a problem since the slow connections from each RTU to the front-end do not have to reach both control centres but only a substation which is not very far away and which has high capacity links.

From a physical point of view this may not be so different from the "classical solution" as it may seem, because the telecommunications department would probably aggregate RTU channels in some places and ship them via a WAN to the control centre but one is spared the inelegant cable mess typical of a concentrated front-end and the redundancy of connections is more visible to the control centre personnel.

Each mini front-end should be duplicated and the number of RTUs connected to each one should be less than say, half-a-dozen, to avoid that a catastrophic loss of a mini front-end (a building fire, for example) would cause the loss of connections to many RTUs, leaving a difficult task for the State Estimator.

4.5.3 Direct Connection to a Company-wide WAN

Some companies may already have a powerful WAN at all Substations and then it may be possible to use the IEC 870-5-104 profile, a protocol which may be defined as the former IEC 870-5-101 point-to-point profile encapsulated in TCP/IP. As this protocol was approved only a couple of years ago, it may be difficult to convert existing RTUs to this solution, because it may happen that the RTU supplier has not done this implementation before.

The issue will become easier if a PC is located before the RTU, to create the dual porting and to convert the proprietary protocol to IEC, as shown in Section 4.5.1. The difference between converting to IEC 870-5-101 or to IEC 870-5-104 will not have a big price impact.

With protocol IEC 870-5-104, the RTU is directly connected to the main WAN and there is no need for a front-end.

For some time the concept of "Substation Gateway" has been discussed. This should be a device able to communicate with the increasingly intelligent devices that are being installed at the substations like time tagged event recorders, parameterisable protection and fault-recorders. The problem with this concept is that when these devices are not prepared to communicate via a LAN, the effort in software development to establish communication between the "Substation Gateway" and the proprietary devices is substantial, because there is a probability that there will be a large variety of devices and specific interfaces to be implemented. If they are able to communicate via a LAN, the "Substation Gateway" is redundant because the devices may be directly connected to the company WAN and made accessible to anyone.

A further concern where a common company-wide WAN is used is that unless a special Virtual Private Network is created, there will be no guaranteed Quality of Service for the SCADA / EMS traffic and indeed there is no guarantee that data packets will be delivered to their destination.

4.5.4 Substation Control Systems

In new Substations the RTU functions tends to be a module of the local digital Substation Control System. Until recently this system had one or two serial ports where the "virtual" RTU could be interrogated by the Control Centre. Recently these systems started being able to communicate using the ICCP (Inter Control Centre Protocol, also called TASE.2) and this may be an alternative to the IEC 870-5-104 protocol. It usually requires 2 Mbits/s channels but much more types of data may be exchanged between the Control Centre and the Substation Control System than between the PCC and an RTU.

5. Operational Standards

When setting out to improve the resilience of PCCs the key performance or design criteria which will form the basis for the design must be established. The first challenge is to define the nature of the disaster / event against which the system must display resilience.

Additionally it is necessary to set out critical performance and availability parameters which must be achieved by the design. In the following subsections the design parameters relating to time-skew between main and stand-by PCC databases, availability targets for main equipment subsystems and other general performance issues are discussed.

5.1 Scale of Disaster and Distance between Primary and Backup Centre

The distance to be established between the standby centre and the main one depends on the type of threats which the owner wants to prevent. If fire is the only concern, then installing the standby centre in the same complex but in a different

building will be the most convenient solution. To counter terrorist or military attacks a few kilometres separation may be needed. For an earthquake, another town seems necessary.

The placement of the standby centre will also depend heavily on the available telecommunication infrastructure. With the investments made in fibre optics by ISOs in recent years, the probability is increasing that there will exist several redundant Mbits/s capacity between the main and the standby centres. This connection is a necessity, to keep the software management effort at a reasonable level.

5.2 Frequency of Updating of Standby PCC Databases and Software

If half of the system is installed at each centre, as described in Section 4.2, there is no concern about this issue since the automatic backup of the hot-standby configuration will keep each primary-backup server pair conveniently synchronised.

In case there is a full hot-standby configuration at both centres, the frequency of updating either the databases or the software patches that are frequently installed will depend on the amount of data that can be lost in a catastrophe and on the resources that can be spent on the task.

Not only need the databases and software be updated but also the capability of the backup control centre to perform its duties must be checked periodically. That check may occur on a monthly basis but larger periods may also be adopted if the change over requires a considerable effort.

If there is a 2 Mbits/s or faster link between the main and the standby centre it will be desirable to have the standby database updated frequently – say half-hourly. Larger periods may be used in the absence of such a link but the choice of a longer update interval may give rise to a considerable increase in the ECC maintenance effort.

Another point is that when operations are regularly conducted from the Stand-by PCC, a smooth transition should take place so that the system remains visible and controllable, except for a very short window of perhaps 20 seconds.

5.3 Adoption of Standard RTU and ICCP Protocols

Since there are now standard protocols for RTUs, the installation of a new system is a good time to adopt the current international standards. If one is pessimistic one may have noticed that there are many standards and while some are widely used others dwindle and one may back the wrong horse. Having said that, it is obviously better to adopt a standard than to keep using a proprietary protocol because this will minimise the problems and the risks associated with the Centre-RTU communication.

The current choice for point-to-point and multi-point RTU connections is the IEC 870-5-101 profile and it may run over 1200 bit/s serial connections. When this profile gets encapsulated in TCP/IP it is named IEC 870-5-104 and this type of link can operate at much higher speeds.

If there is more than one control centre, the communication between them should use of the Inter Control Centre Communication Protocol (ICCP) also called TASE.2. There should be an ICCP link between the primary and the backup control centre to allow the latter to exchange real-time data between the two centres. In Europe in the recent years there have been several installations of ICCP to ease the real-time data flow between different ISOs.

5.4 Availability Requirements for Major Subsystems (PCC, telecoms, RTUs)

The PCC, being a hot-standby configuration, should be always available. The major difficulties in keeping the Stand-by PCC in a ‘ready to operate’ mode do not come from the hardware but from database changes, installation of software patches and software upgrades. The increasing complexity of the installed software makes it very difficult to have an in-house team capable of solving all software problems.

The in-house software team acquires a good notion of how important it is to keep the system running at all times because they see the anxiety of the dispatchers when the system is down. For the supplier's personnel, who are remotely accessing the system, that concern is not so strongly reflected in their consciousness and they may have more difficulty grasping the difference between the test machines they are working with and the machines performing a critical mission.

The ubiquity of PCs and of the many occasions where a problem is solved by restarting the machine may also explain some indulgence of difficulties attributed to software bugs.

As a tentative number one would say that the system should not be completely down for more than 30 minutes per annum and there should not be more than one incident of this type once a year. In the first year after commissioning, a higher incidence of this type of problem may arise and may be accepted as part of the settling-in period.

Telecommunications systems are increasing in reliability and as the channels are duplicated they only become critical when one single fault blocks the communication to several RTUs at the same time. The telecommunications network should be designed to avoid this type of occurrence.

RTUs are normally not duplicated but they usually are also very reliable. RTUs for power plants are usually less critical for a control centre than those in substations. Although a power plant may be very important to the electrical system, its output power is stable when compared to the loads and its value may be manually adjusted by the operator, through telephone contact with the plant operator, while the RTU is being repaired. Loss of visibility of large substations may cause some convergence problems on the State Estimator. Maintenance personnel responsible for the high-voltage equipment may also help at card substitution level to solve the problem. As the RTU affects only one installation and it is very unlikely that at the same time there is a power system problem at the substation, RTU reliability normally is not a pressing issue.

The RTU and telecommunications system availability depends on the MTTR (Median Time To Repair) as for all equipment. Even with old RTUs, a yearly failure of 50% is achievable, i.e. in a system with n RTUs there will be n/2 failures per year. Considering that they are in remote unmanned locations, one may assume each failure is solved in one day. This means that, on average, each RTU will be unavailable half a day for every 365 days. Availability will then be: 1- 0.5/365 = 99.86%.

As single telecommunications channels do not normally have this level of availability of RTUs it is usual to duplicate the telecommunications channels to get an availability similar to that of an RTU.

5.5 Performance Requirements when Main PCC is Lost

As far as the EMS applications are concerned, the performance of the standby centre should be identical to the primary one.

The most controversial item in the control room is the mimic board, the large diagram that contributed most to the architectural atmosphere of the control rooms over the world. The wall with lots of LEDS is now being substituted by rear lit projectors but this type of equipment is expensive. As there are always discussions about the real value for those devices, it seems natural that they will not be available at the backup control centre.

Another set of machines that will probably be fewer in number at the Stand-by PCC are the MMIs. Although the same number of MMIs should be available for the shift operators, one would expect less MMIs for people doing studies about unavailability planning, available transfer capacity calculations and so forth. In principle this may be quickly recovered by the quick installation of some extra PCs,

that now are either the basis for the standard MMIs themselves or capable of functioning as an X-terminal to the telecontrol system.

5.6 Cyber Security

There has always been an awareness that IT systems such as those used in PCCs may be vulnerable to cyber attacks. The risks from cyber attacks have significantly increased as a consequence of the interconnection of many disparate IT systems. An event in one small relatively unimportant part of the network, say in the IT system of a minor IPP market participant, may propagate throughout the network.

Over recent months increased attention has been given to this source of risk. In the USA NERC has proposed that stringent cyber-protective standards should apply to all real-time systems. International standards in this area may become applicable in the near future. The ISO/IEC 17799 standard is a useful document in this area, though it does not deal with IT Security for real-time systems.

6. Improving PCC Resilience Through Training

An analysis of the factors which can contribute to improving resilience shows that the human factor impinges on very many aspects of the performance of the overall system. The need to ensure that dispatchers are thoroughly trained is obvious. The considerations relating to planning and design of training of personnel is explored below.

Not so obvious in the quest for improved resilience is the need for all relevant personnel to be trained to be aware of the cyber-based threats to system security. A further non-evident factor is that in today's competitive and deregulated market provision for access to certain confidential information can expose the system to manipulation or to malicious abuse. In particular there is a need for operations personnel to be aware of the roles and activities of the many 'players' in today's electricity market.

These matters are discussed in the following subsections.

6.1 The Training Aspects of the Architecture Design

An increase in the resilience of the PCC may be achieved by the careful analysis of the human operator aspects and by suitably training all personnel. While both the Standby PCC configuration and the 1:n redundancy configuration may both provide the same level of functional backup, they require different knowledge and skills from the power system dispatcher. Thus different training programs will be required.

In the former case of a Standby PCC, or mirror image PCC, the operators will continue to use the same Human Machine dialogue, albeit from a different location. The operators will continue to carry out the same tasks while managing the power network with which they are quite familiar.

In the latter case, where a RCC takes over the role of the main PCC, the operators in the RCC who normally operate only a regional part of the network or its lower voltage levels, may be required to take over the PCC functions / responsibilities. Although with enough training they can do so, the level of the additional training needed may be prohibitive to justify such a solution. In any event the utility must devote enough resources to training of the RCC operators so that they can take over the role of the PCC in an emergency.

In order to improve power control system resilience from the human operator perspective, sufficient training of operating personnel training is required. Thus after defining the system architecture it is possible to approach the development of training programs for the operating personnel training in a detailed manner. The training to be provided to personnel needs to address three important aspects: 1) alerting staff to risks

and dangers, 2) planning and designing a suitable training program and 3) practical delivery of the training. These aspects are discussed below.

Regarding the design of the RTU communications scheme, a number of options are available today as described in Section 4.5. Although the options differ in cost and capabilities, whatever choice the utility makes in this respect, it will not significantly influence the human operator aspects and thus final selection of the control system architecture.

6.2 Alerting Staff to Risk and Essential Precautions

Alerting personnel to all the dangers and risks involved when working in an environment of complex technical systems and human interaction is essential. The purpose of alerting personnel to the risks and dangers is to provide them with a more acute awareness of the security risks within the Information and Communication Technology (ICT) security in general and process control in particular. The primary goal is to ensure that personnel recognise where the main risks arise. It is a question of learning to be aware of all the risks as well as learning to work under those unusual circumstances with limited technical tools and in an environment where full information may be lacking.

Threats and consequences need to be identified for the process control functions. To be able to manage the ICT-security issues, it is necessary to analyse the threats and consequences on a regular basis.

A human error arises when someone takes some action that he is privileged to do but not supposed to. To protect a business entirely from human errors is more or less impossible. Protection levels can be increased by adding more people into every step of the process, one person to decide and another to verify and execute etc. To be cost-effective it is necessary in one way or another to trust personnel in the organisation as well as in other organisations. A way to reduce human errors is to have competent and satisfied personnel.

Good recovery procedures will reduce the consequences of human errors.

6.2.1 Analysis of Sources of Security Threats

Threats to the security and resilience of the PCC arise from:

- Natural incidents,
- Equipment failures,
- Legitimate users inadvertently acting on an insufficiently protected system,
- Physical intruders, terror and sabotage,
- Legitimate users violating the limits of authorisation for malicious reasons,
- Terrorist action or warfare,
- Human mistakes and computer errors,
- Interaction of sources above and ICT threats.

Today many employers allow access to process control systems from offices and homes. As a consequence of this it is necessary to consider the physical access into those areas as well. Alerting staff to the risks involved and implementing appropriate security measures is clearly essential.

It is also necessary to take security precautions against breaking and entering control centres and substations. Another security threat is mailed bombs or items that will set the control facility out of order. The latter is more likely to be a terror threat.

In order to be able to handle security issues in a cost-effective manner and to minimise the risks and consequences security management has to:

- know the security scheme objectives,
- recognise the human risks,
- have knowledge of the systems and interfaces.

Objectives of the Security Scheme include:

- Integrity - To safeguard the accuracy and completeness of information and processing methods.
- Availability - To ensure that authorised users are guaranteed access to information and associated assets when they need it.
- Verification - Prove that agreements, etc., that are made electronically really have been made.
- Confidentiality - Means that information is available and used only by people with authorisation.
- Administration – Cost effective management of security issues.

Human risks are high because people handling control systems may have relatively high authorisation. Malicious human actions may stem from:

- People who are unsatisfied with their position, work or salary
- People who are fired or have notice of employment termination
- People with lack of competence and knowledge.

Knowledge of the systems and interfaces is an end-to-end security issue. There needs to be strong and clear guidance and control on security procedures such that use of computer applications and data sets are appropriately restricted, maintained and controlled. Rapid changes in the ICT industry and rapid development may lead to lack of competence by the vendors in 3-5 years.

Integration (or interaction) of SCADA applications with interrelated applications (management, market and other information systems) involves the development of new software and may also imply adjustments to the SCADA software. Of course the new software should be stable and include security features.

System security will also include stability and redundancy issues in a system that is growing more and more complex.

6.3 Training of the Operating Personnel- Planning and Design Issues

It is well recognised today that education and training are the first steps in the process of coping with the increased complexity, which characterises modern power system operation.

The totality of personnel training extends far wider than merely addressing the issues of operating and maintaining the PCC and any Stand-by PCC – as outlined in the previous section. The entire training plan for PCC personnel should be designed and extended to include new topics and practices related, not alone with the PCC, but also with the operations of the Stand-by PCC and the broad topic of security issues. The training plan and program should also contain the following:

- Training program for the PCC to Stand-by PCC transfer procedure,
- Training on security issues and counter-measures,
- Training program for the Stand-by PCC operators,
- Training program for the Stand-by PCC maintenance (support) staff.

The training program for the PCC to Stand-by PCC transfer procedures should contain, in a written procedure, the transfer preparation procedure, its time schedule and transfer procedure description, as well as other details related with this type of training (i.e. periodicity of testing, responsible persons and their contact details, method of verification, means and methods of training, and its location).

The well structured and state of the art methodology for the power system operator training program design can be found in the Electra, December ’99.

6.4 Practical Implementation of the Operator Training Program

In order to achieve the required level of knowledge and skills, a regular exercise using 1) all of the capabilities acquired in the training programs suggested above and 2) one which exercises all of the subsystems in the PCC and in the Standby PCC configuration should be carried out.

In this respect, in order that the transfer from the PCC to the Stand-by PCC becomes routine, the transfer procedure should be practised frequently (perhaps once a month). Actual operation of the power systems from the Stand-by PCC location can be performed less frequently (perhaps once or twice a year, as a refresher type training).

The training for the normal system operation from the Stand-by PCC is also important as it may be that different arrangements in RTU communication, different constraints and perhaps the functionality of the Stand-by PCC may differ from that of the PCC.

The training should also include simulation of power system emergency conditions. This is where system restoration and "black-start" training (including drills) are very important for the Stand-by PCC operators – though the procedures may be dictated by the Grid Code or similar regulatory obligations.

Power system operators should also be trained in the:

- Coordination of activities between the different segments of the utility (operators, maintenance, back-office…),
- Communication with the outside parties (neighbouring utilities, other ESI entities), with the special attention given to the common understanding of terminology.

Finally, back-office hardware and software support personnel should also undergo sufficient training to grasp all the specific arrangements and constraints that operation and maintenance (h/w, s/w, database, auxiliary equipment, etc.) procedures at the Stand-by PCC may have. This should include actions to be performed by the support personnel during the PCC to Stand-by PCC transfer. Where the intervention of a Telecommunication Network Management Centre (private or public, or both depending of the telecommunication network structure and ownership) is required to redirect telecommunications links, the actions required to coordinate the transfer of control from the main to Standby PCC and the redirection of the telecommunications links should be rehearsed and procedurised.

Special attention should be placed at the understanding of the potential threats to power system control system arising from the IT domain e.g. malicious use, viruses, etc. The technical and organisational counter measures, e.g. firewall, password, encryption, etc., that could be applied preventively or after the fact (reconfiguration, recovery procedures) to safeguard the power control system should be studied, procedurised and practised.

6.5 Extent of Involvement of Partners in Power Market

The deregulated electricity market has imposed **new human threats**.

Knowledge of the assets of a competitor and the operation of his system can be beneficial and acquisition of such information is an increasing possibility. This sets new demands for secure handling of data and the security levels of the information that are exchanged.

Internal or external communication networks have become common in utilities. In the past utilities held their information tightly and controlled but this is no longer the case. Networks have often been based on special protocols and vendor specific applications. The trend today is to move towards an "open" infrastructure, "open" information exchange and increasing use of standard applications and communication technologies. The "open" infrastructure is itself vulnerable by its open nature, so it is necessary to alert the staff to the necessity of keeping the information well controlled and confined to authorised users.

Shared communication networks and information exchanges over public networks are both becoming common. This trend allows for general attacks by other parties (e.g. hackers, disgruntled employees, or terrorists). There is a large amount of technology available in the market that can be used in such an attack and it is increasingly probable that such attacks may be successful.

The involvement of partners in an open power market has specifically brought up the **issue of confidentiality.**

System operators use their SCADA systems to gather real time information relating to the transmission grid in their area and relevant information concerning the connected neighbouring areas. Most of this information as a whole is used to ensure a stable supply of electricity. On the other hand, can a player on the market use the same information to see - for example - bottlenecks in the transmission grid and exploit this information to his advantage ?

This threat can arise by hacking into the SCADA servers, listening to communication from external network connections (WAN), or the threat could be perpetrated by staff with authorised (or unauthorised) access to the system. Therefore it is important to consider which data the different departments and persons may see and use for which purpose. Some kind of access control and authority must be built in the SCADA system, and - even more importantly - the control authority must be used and maintained.

The time range of data held in historical archives varies typically from several years to minutes thus giving the possibility to see 'almost' real time data. Using historical data combined with suitable data models and intelligent guesses it is possible to pinpoint bottlenecks in the transmission grid, which can be used by the market players for their benefit. The historical data should be handled as confidential information and it is important to consider which kind of data different users can see and for what purpose. Access control and authority mechanisms should be built and maintained on the same level as in SCADA and EMS systems.

7. Conclusions

There are many factors which may lead to the demand for high resilience in Power Control Centres. Each utility, or entity responsible for the PCC, needs to assess the business environment in which it operates. The risks posed to continuing operations from various physical factors – such as fire, flood, earthquake, etc. – plus those posed by terrorists, cyber attacks and from other malicious sources will vary from country to country. Based on the risk assessment, a conclusion as to whether to establish a Stand-by PCC will hinge on the costs of improving resilience and the benefits which may flow from the proposed development. The outcome from this analysis may lead to a decision to establish a Stand-by PCC.

The design of a resilient PCC, especially if a Stand-by PCC is planned, is best addressed at the earliest possible time. Among the architectural arrangements that can be adopted for a Stand-by PCC are: 1) a mirror PCC; 2) 1:n redundant configuration, 3) reduced functionality emergency PCC and 4) geographically split PCC. In choosing an architecture to be adopted consideration needs to be given to the characteristics of the existing and planned RTUs and the telecommunications network.

The impact of the design for a Stand-by PCC on the telecommunications system can be significant. A key challenge is how to switch RTUs from one control centre to the other. If dual-ported RTUs are installed then a simpler and less expensive solution may be possible. If RTUs communicate through an IP network based on the IEC 870-5-104 protocol – as is recommended by many designers – then the establishment of a Stand-by PCC and the switching of data flows between control centres is greatly simplified.

The design and performance parameters of the PCC and any Stand-by PCC need to be determined. Among the issues to be considered are: what scale of disaster is being countered, what degree of synchronicity is required between the main and Stand-by PCC, what level of functionality will be provided by the Stand-by PCC, etc. The adoption of industry standards for communications with RTUs, for inter control centre communications and for the architecture of the telecommunications infrastructure will greatly ease the path towards a flexible and resilient control scheme.

The importance of a well designed personnel training program and its contribution to improving resilience should not be overlooked. Training of dispatchers and support staff in the procedures involved in keeping the Stand-by PCC up to date and in the procedure for transferring operations between centres will obviously be valuable. Recognition of the increasing risk of cyber threats is also essential. The proverb regarding prevention being better than cure is highly apt. Personnel need to be advised of security threats and the means of recognising and dealing with them.

In an open market environment information from many sources may be held in the PCC or in interconnected databases. Access to some of this data may be restricted to authorised persons; at the same time general internet / web access may be provided to all market participants. The maintenance of the integrity of the data and software in this complex situation is a significant challenge. Clearly careful thought has to be given to the training of those responsible for the design and maintenance of the IT systems supporting the PCC.

Acknowledgements

Colleagues in various parts of the world assisted in the preparation of this paper. Their contributions are acknowledged with thanks.

References:

1. E. Kenneth Nielsen at all, “Backup Control Centres- Justification, Requirements, Emergency Planning, and Drills”, IEEE Transactions Power Systems, Vol. 4, No.1, February 1989, pp.248-256

2. M. Power, “Report on Backup Control Procedures and Emergency Back-up Control Centres”, CIGRE SC-39 Colloquium, Montreal, Canada, 1991.

3. NERC Backup Control Centre, A Reference Document, EPRI Project RP 2473-68, July 1993.

4. NERC Operating Manual, Policy 6 E (Control Centre Backup), http://www.nerc.com/~oc/opermanl.html

5. N. Cukalevski, H. Jones, “Power System Operator Training Program Design, Development and Utilisation”, ELECTRA, No.187, December 1999, pp.117-131.