Backup Control Center Design and Implementation Criteria

Savu C. Savulescu, *Senior Member, IEEE*

***Abstract* -- This presentation describes a "mirrored" two-control center architecture where each one of the two SCADA/EMS involved is able to operate in capacity of "primary system" without loss of data and functionality and with no impact on performance and other key attributes. The guiding principles and the conceptual overview of this architecture are addressed, and a number of key performance requirements are discussed. The approach presented herein can help utilities, consultants and system integrators design and implement utility information systems that can operate 24/7 without functional and performance degradation and virtually without loss of operational data.**

***Index Terms* -- energy management systems, utility information systems, SCADA/EMS, market systems, independent system operators.**

I. Introduction

THIS presentation addresses a topic that has been increasingly focused upon during the last few years in the SCADA/EMS industry: ability to maintain full and continuous supervision and control of power system operations during major and unexpected emergencies without loss of current and historical operational data and with no adverse impact on functionality, performance and other key attributes. This is particularly relevant in the aftermath of disasters that occurred naturally, or were created by humans, and could have impacted, and in some cases did impact, either the physical or the IT and communications infrastructures, or both.

In this context, utilities have started to implement fully redundant and continuously operational supervision and control systems either by extending existing SCADA/EMS installations with so-called “emergency backup” systems, or by implementing new SCADA/EMS facilities *in addition* to the existing ones while *upgrading* the old installations rather than disabling them. In both scenarios, the end result is supposed to be a "mirrored" two-control center architecture where each one of the SCADA/EMS could operate in capacity of "primary system" without adverse effect on their key attributes.

Mirrored architectures offer significant benefits – but these benefits wouldn’t come free. On the one hand, the overall cost of ownership and operation of such complex installations would increase by an order of magnitude. On the other, the technical difficulties that would have to be overcome render the design and implementation of mirrored control center architectures far from trivial.

In the subsequent sections we develop the underlying principles, illustrate the main ideas with a conceptual solution, and discuss a number of key performance requirements that need to be addressed by utility engineers, SCADA/EMS consultants and system integrators when designing and implementing backup control centers.

II. Terminology

When describing the "mirrored" two-control center architecture and its basic principles, the terminology "primary system" and, respectively, "backup system" is used only for convenience. In reality:

- Each one of the two SCADA/EMS involved in this architecture shall be able to operate in capacity of "primary” system
- By definition, the SCADA/EMS which, at any given point in time, is not operating in capacity of "primary” system, is referred to as "backup” system
- The names "primary” and "backup” system are thus interchangeable
- The architecture is called "mirrored" because the two SCADA/EMS systems that comprise it are the mirror image of each other.

The guiding principles for defining and specifying this two-control center architecture along with a conceptual overview are discussed in the following.

III. Guiding Principles

The key concept in this paradigm is that both the "primary" and the "backup" system are required to:

- Operate in the same data environment, or data model
- Use identical applications and algorithms
- Deploy identical user interfaces and operational procedures.

A. Real-time Data Gathering and Processing

As far as the data are concerned, they are collected simultaneously both from the primary and from the backup system but at are processed in one single place at a time. In order to illustrate this concept, let's consider one cycle of

Invited paper SGM-2011GM0351 presented at the “Control Center Issues” session, IEEE PES General Meeting 2011, Detroit, MI, July 24-29, 2011

Savu C. Savulescu is with Energy Consulting International, Inc, New York, New York, e-mail scs@eciqs.com

gathering real-time data from RTUs and/or Substation Automation Systems (SAS). The RTUs and SAS are scanned simultaneously by both the primary SCADA/EMS and the backup SCADA/EMS. Under this scenario, each and every data item travels from the place where it was collected to two different locations, but the *real-time database is built and maintained in only one place, which is the SCADA/EMS that operates in capacity of primary system*.

Otherwise, i.e., if two real-time databases were created, one at the primary and the other one at the backup location, due to inherent time delays, even if very small, the time stamps of database snapshots taken from these real-time databases would not be identical - but which real-time snapshot would be right? There is no obvious answer to this question, which is why we propose to build/update the real-time database only at the primary location.

Another difficulty concerns the concept of “data model master”. As opposed to conventionally distributed data environments, where data model modifications are entered at a data model master and, from there, get distributed to all the systems that use them, in our mirrored architecture the primary and backup locations are interchangeable, thus making it impossible to assign a real-time data model master that resides 24/7 in one and the same physical place.

We solve this dilemma by requiring that, at one single time, one and only one control center shall act as "master"; when the roles are reversed, for whatever reason, the control center that, until then, was operating as back-up, shall become "master" and assume the role of maintaining the data model as well.

One implication of this requirement is that the *data model master has to reside simultaneously in two places* and, somehow, has to be simultaneously updated. Another implication is that the *data histories of the primary and backup system have to be identical*, i.e., that the Historical Information Systems residing at both locations have to be continuously updated and synchronized.

B. Applications and algorithms

The need to use identical applications and algorithms at both the primary and the backup location is obvious. Most of the computational results are stored in save cases and become part of the system's history. If the primary and backup application subsystems were not identical, it would be possible for computations based on similar raw data to produce different results, which would be troubling under normal operation conditions, outright confusing during system state changes, and legally unacceptable if audits were conducted.

C. User interface and operational procedures

The requirement that the primary and, respectively, the backup SCADA/EMS be predicated on identical user interfaces and operational procedures stems from the need to provide all the system users, from Operators to engineers and to maintenance personnel, with one single set of computer skills and to train them uniformly - asking an Operator to perform his/her duties in two different environments would be an invitation to disaster.

As a corollary to the above considerations, we conclude that the primary and the backup system, although autonomous and independent, shall:

- Use the same data model
- Have the ability to act as master systems for the same data points but only the primary system shall have data responsibility
- Have the same data histories
- Be equipped with identical applications and user interfaces.

By contrast, the operation control tasks shall be assigned only to the system acting in "primary" role.

IV. Operating Modes of the Two-Control Center Architecture

Another key concept that sits at the foundation of the two-control center architecture is the *operating mode*, which can be one of the following:

- Normal Operating Mode
- Short-Term Emergency Operating Mode
- Long-Term Emergency Operating Mode.

Although both the primary and the backup systems have identical functional capabilities, it is the operating mode that dictates which functions are active at a single point in time, and which functions get activated if the operating mode has changed.

The detailed specification of these operating modes goes beyond the scope of this presentation, but a brief description is provided in the following based on the assumptions that:

- A SCADA/EMS exists already and, after the implementation of the mirrored two-control center architecture, it will be designated as Backup Control Center
- A new SCADA/EMS will be commissioned and installed at a new location and, within the mirrored two-control center architecture, it will be designated as Primary Control Center.

A. Normal Operating Mode

During this mode of operation, both control centers are available, fully operational, and ready to be switched-over between them.

Certain activities, however, do not have to be included in this paradigm. Training, for example, most of which is normally performed on the Dispatcher Training Simulator (DTS), could be executed only at the primary location but would get suspended if the control jurisdiction has been switched between the two control centers. Some other functions could be executed only at the backup location, for example, point-to-point checking and related testing of new RTUs and/or SAS that might get incorporated in the system if new substations are built. The functions which are executed only at the Backup Control Center would be:

- Suspended immediately after the control jurisdiction has been inherited from the Primary Control Center
- Restored once the control jurisdiction has been switched back to the Primary Control Center

B. Short-Term Emergency Operating Mode

During this mode of operation, one of the control centers is not available, but *only for a short period of time*.

In this case:

- The control center that is operational would be used in capacity of primary system
- For a short period of time, a backup system would be unavailable and the mirrored two control center paradigm would be disabled
- The training activities would be suspended
- An unscheduled HIS synchronization would be performed immediately after the Normal Operating Mode was resumed.

C. Long-Term Emergency Operating Mode

During this mode of operation, when one of the control centers is *not available for a long period of time*:

- The control center that is still operational would be reconfigured as primary system *with all the functions active, including the DTS*
- For a long period of time, a backup system would be unavailable and the mirrored two control center paradigm would be disabled
- An unscheduled HIS synchronization would be performed immediately after the Normal Operating Mode was resumed.

D. Further considerations

For the purpose of maintaining the jurisdiction transfer capability fully operational, the primary and backup roles will have to be routinely switched between the Primary Control Center and the Backup Control Center and vice-versa.

Also, let’s say *en passant* that the management of the telecommunications network goes beyond the scope of our presentation because, at least in theory, the communications network management facilities do not have to be located on the SCADA/EMS premises. If they were, the concepts and principles identified for SCADA/EMS would be applicable for the management of telecommunications as well.

V. Conceptual Solution Overview

The conceptual overview of the proposed two-control center architecture is illustrated in Figure 1. At the outset, let's state that the "boxes" identified as Primary Control Center SCADA/EMS and, respectively, Backup Control Center SCADA/EMS, encompass exactly the same array of functions even if some capabilities are suspended during a particular operating mode.

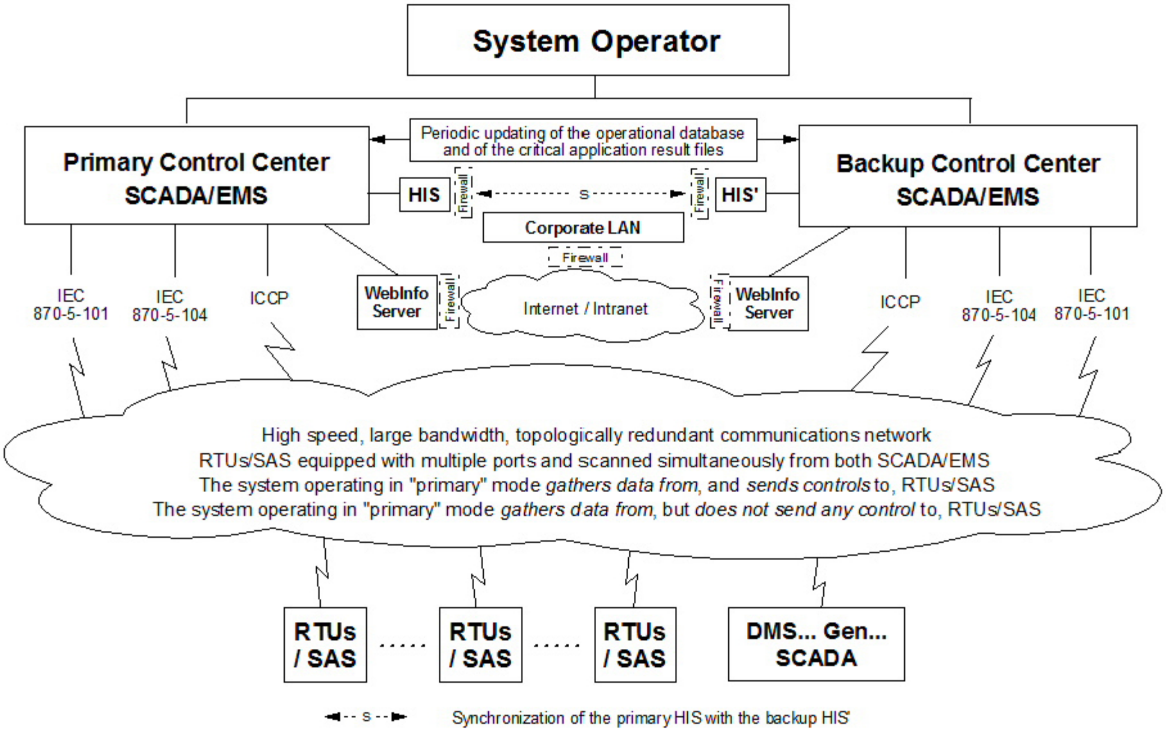
System Operator
Periodic updating of the operational database and of the critical application result files
Primary Control Center SCADA/EMS
Backup Control Center SCADA/EMS
HIS
Firewall
S
Firewall
HIS'
Corporate LAN
Firewall
WebInfo Server
Firewall
Internet / Intranet
Firewall
WebInfo Server
IEC 870-5-101
IEC 870-5-104
ICCP
ICCP
IEC 870-5-104
IEC 870-5-101
High speed, large bandwidth, topologically redundant communications network
RTUs/SAS equipped with multiple ports and scanned simultaneously from both SCADA/EMS
The system operating in "primary" mode gathers data from, and sends controls to, RTUs/SAS
The system operating in "primary" mode gathers data from, but does not send any control to, RTUs/SAS
RTUs / SAS
.....
RTUs / SAS
.....
RTUs / SAS
DMS... Gen... SCADA
◄-- S --► Synchronization of the primary HIS with the backup HIS'

Figure 1 Conceptual Primary - Backup Control Center Architecture

The terminology "System Operator" applies to an ISO, TSO, or to any other type of utility entity that performs supervision and control operations. It is assumed that the SCADA/EMS systems deploy both point-to-point and IP protocols. The box "DMS... Gen..." designates other systems, if any, such as generation control, distribution management, and so on.

The DTS, for example, is one of those capabilities that can be executed only at one single *physical* location, which can de reassigned if the system enters the Long-Term Emergency Operating Mode.

Let's also note that the Historical Information Systems HIS (primary) and HIS’ (backup) are shown as separate boxes although they actually belong to their respective SCADA/EMS. This was done only for the purpose of simplifying the drawing where the HIS synchronization process is illustrated schematically together with the process of updating the data models and a privileged subset of save cases that are critical for decision making.

As shown in Figure 1, both SCADA/EMS systems are connected to all the RTUs and SAS, which are scanned from both locations in order to simultaneously feed both control centers with the same data. The control actions, however, are performed by only one system at a time.

A similar rule applies to data exchanges with other systems that either are external or belong in second control hierarchy level. The incoming data would be channeled to both the primary and the backup system, but the outbound information, if any, would be posted only by the Primary Control Center.

Also depicted in Figure 1 are firewalls that protect the SCADA/EMS against cyber attacks. In this regard, the HIS and, respectively, HIS' are particularly vulnerable because they could be accessed not only from the demilitarized zones of the SCADA/EMS LANs, but also by other users as well, e.g., users of the corporate information system, market agents with appropriate jurisdiction, and so on. In order to simplify the drawing, firewalls at the entry point of communications that use IP protocols are not shown, but they are certainly required.

VI. Key Performance Requirements

Just like any other SCADA/EMS project, the design of mirrored two-control center architecture entails developing functional, operational, performance and implementation requirements, among others. Most of them are relatively standard, and certainly well known, across the SCADA/EMS industry and do not need to be reiterated herein. Certain performance criteria, however, are key to the successful operation of the two-control center solution, require special analysis, and are addressed in the following.

A. General Considerations about Performance

When establishing the performance requirements for an information system, it is important to distinguish between what's *desirable*, what's *needed*, and what's *achievable*.

What's desirable is relatively easy to guess. Nowadays, we are driven by speed and everything has to be quick and easy. Sometime, a second may seem too long and the word "instantaneous" easily comes to mind. For example, the desire to cut the few seconds needed for the results of a spreadsheet recalculation to become available, or for a web page to pop up, can be justified by the need to increase productivity, by the time pressure to take some action, or by some other reason more or less valid. Accordingly, it is "desirable" for an information system to be always available and to reply instantaneously to user entries.

What's needed is not necessarily synonymous to what's desirable. For example, one might think that it may be desirable to refresh the readings of system analog values every other few cycles and to update the display monitors in the control room with a similar frequency. However, ergonomic considerations and the way the human vision works tell us a different story.

Accordingly, a display refresh cycle of 1 or 2 seconds is quite appropriate, and, in turn, drives the requirements for data to be collected from the field and the real-time database to be updated with approximately 1 or 2 seconds frequency as well. By the same token, 1 or 2 seconds elapsed time for transferring the control from a primary to a backup information system appears to be justified, at least at the first sight.

What's achievable is not always in line with the needs and the reality. For example, periodicities of 1 or 2 seconds for collecting analog readings from the field, updating the real-time database and refreshing the displays in the control room are perfectly achievable -- but it is not necessarily true that transferring very large amounts of data between two information systems that are separated by a significant geographical distance can be achieved within 1 or 2 seconds.

On this basis, a down-to-earth assessment of the performance requirements that should govern the transfer of control jurisdiction from the Primary Control Center to the Backup Control Center and vice-versa should be conducted for each separate situation and in the following order:

- Determine what's really needed
- Postulate a metric for quantifying performance
- Identify the factors that affect performance
- Establish response time requirements that are both reasonable and achievable.

These aspects are briefly discussed in the following.

1) What's Needed

In order to provide continuity, reliability and accountability in the execution of supervision, control and operations support tasks when the operational jurisdiction is transferred from the Primary Control Center to the Backup Control Center and vice-versa, the following requirements shall be met:

- The time lag between the data model in the control center that is operating in backup mode and the data model in the control center that is operating in primary mode shall be *smaller than a small number of database refresh cycles*. This implies that the time elapsed between the initiation of a data model update by the primary system and its completion on the backup system be equal to, or at least comparable with, the time needed to refresh the real-time database

- The elapsed time for synchronizing the primary SCADA/EMS HIS with the backup SCADA/EMS HIS shall be consistent with the time lag between the real-time databases. Thus, since the time needed to update the backup data model would be equal to the time needed to synchronize the two historical information systems, it follows by implication that, at any single point in time, both the data model and the HIS' at the backup location would: be mutually consistent; and lag the primary data model and HIS by a time interval smaller than a small number of database refresh cycles
- Both the primary and the backup SCADA/EMS shall be designed for the same level of availability. In other words, if the primary SCADA/EMS is available 99.95% of the time, the backup SCADA/EMS should also be available 99.95% of the time.

The later requirement is trivial and its implementation is readily achievable, but a question comes immediately to mind in regard with the first two criteria: what does "a small number of database refresh cycles" mean?

Let's say that the database refresh cycle is 2 (two) seconds. In light of the earlier discussion of what's desired, what's needed, and what's achievable, during the transfer of control jurisdiction from the primary to the backup location, it may be desirable to lose no more than 2 seconds of data, but the actual need could be relaxed to time lags of up to two or even three minutes. How to quantify a "small number of database refresh cycles" that makes sense is discussed in the following.

2) Metric for Quantifying Performance

A metric that can help quantify the "small number of database refresh cycles" can be developed directly from the responsibilities of the owner of the two-control center solution. For example, let's consider the following scenario:

- The backup data model is updated as discussed earlier
- At any point in time, a small information gap between the backup and the primary data models and historical data repositories is inherent due to the time lag implicit in the data updating process
- If a dramatic event takes place, the control jurisdiction is transferred instantaneously from the primary to the backup system

  Note: this is an ideal assumption which is made just for the purpose of defining a metric that quantifies the "small number of database refresh cycles". In reality, the control transfer: is not instantaneous; takes time; and increases the information gap between the backup and the principal data models - for example, the RTU and SAS readings and the revenue metering data that should have been collected during this short time period are lost
- Since the backup SCADA/EMS was already scanning the RTUs and SAS, the real-time database updating process begins immediately - but there is a time gap between the time stamps in the first real-time database refresh cycle at the backup location and the last real-time database refresh cycle at the primary system immediately before the event that caused the transfer of operational jurisdiction.

It is clear that the ensuing information gap can never be recovered. If, for example, the user of the two-control center architecture has both system operator and market operator responsibilities, and, furthermore, if the data collected from SAS include revenue metering data, an *economic metric* could be defined to allow associating a cost to the "small number of database refresh cycles" by which the data model at the "backup" location would lag behind the data model at the primary location.

An *operating reliability metric* can also be defined. The elapsed time of the jurisdiction control transfer between the two SCADA/EMS systems corresponds to a time window, no matter how small, when the power system would be operated by telephone. If we compound this time window with the time lag between the primary and backup data models, we reach the conclusion that, for a brief period of time, in addition to operating the system by telephone, the security assessment functions wouldn't be operational, either. Hence, the "small number of database refresh cycles" can be quantified in terms of operating reliability by answering the question "for how long can such a degraded mode of power system operation be sustained".

3) Factors that Affect Performance

There are three processes where performance is an issue: updating the data model at the backup location; synchronizing the HIS; and transferring the control jurisdiction from the primary to the backup SCADA/EMS. The speed of these processes is affected by the:

- Efficiency of the software tools that maintain the data models at the primary and backup location, and, respectively, synchronize the historical data repositories
- Throughput of the computer configurations at each location, which, in turn, depends on factors such as speed of the processors, bandwidth of the I/O data paths, and seek and access time of the hard disks
- Bandwidth of the communication links between the two locations, including the: primary SCADA/EMS LAN; backup SCADA/EMS LAN; and the telecommunications network
- Amount of data involved in each cycle of updating the data model at the backup location and synchronizing the primary and backup HIS systems
- Degree of awareness and preparedness of operations personnel and the readiness of the surrounding logistics at the backup location.

VII. Conclusions

This presentation has described a mirrored two-control center architecture where each one of the two

SCADA/EMS involved is able to operate in capacity of primary system without loss of data and functionality and with no impact on performance and other key attributes. The guiding principles and the conceptual overview of this architecture have been addressed, and the performance requirements have been discussed and analyzed.

The approach presented herein can help utility engineers, SCADA/EMS consultants and system integrators to design and implement utility information systems that are able to operate 24/7 without functional and performance degradation and, virtually, with no loss of operational data.

Savu C. Savulescu (M’1972, SM’1975) graduated in electrical engineering from the Polytechnic Institute of Bucharest, Romania, obtained the degree of Doctor of Sciences (Ph.D.) from the Polytechnic School of Mons, Belgium, holds a post-doctoral degree from the University of Sao Paulo, Brazil, and is a Professional Engineer in the State of New York. Currently with Energy Consulting International, Inc., a New York corporation that specializes in utility information systems, he has worked predominantly in the design and implementation of SCADA/EMS, SCADA/DMS, SAS and Market Systems, and developed stability assessment software that is being used in real-time and offline in US, Europe, Latin America and Asia. Dr. Savulescu has taught electric power systems and software engineering at major universities in Belgium, Brazil and United States, and speaks, writes and reads fluently in English, Spanish, French, Portuguese and Romanian.