

# ENTELEC 2001 PROS AND CONS OF SCADA SYSTEM DEPENDENCE ON THE CORPORATE DATA NETWORK

By Duane P. Clementson  
UTSI International Corporation

## INTRODUCTION

For better or worse, most SCADA system users have already changed, or are in the process of changing, the communications media and methods used to communicate between critical components of the SCADA system. The change I speak of is from the traditional dedicated SCADA LANs, leased lines, microwave circuits, etc., to complete reliance on the corporate data network. A change of this magnitude should be seriously evaluated to ensure the reliability and performance of the SCADA system are not degraded.

## EVALUATION

I like to begin most evaluations of this type by listing the pros and cons of implementing the suggested changes. It is a fairly simple and straightforward method that ensures we do not get too one-sided by only focusing on the benefits without adequately accounting for the possible pitfalls. Often, the suggested change is still worth implementing after considering all the pros and cons, but the method of implementation changes to address some of the potential problems found in the initial planned implementation.

<b>Pros and Cons of SCADA System Dependence On the Corporate Data Network</b>	
<b>Pros</b> No need for parallel network Easier to exchange data Utilize IT communication expertise Saves money	<b>Cons</b> Insufficient capacity Lower reliability Less secure Loss of control

Let us look at each of these in more detail, starting with the pros.

## **No Need for Parallel Network**

There is an inherent appeal to having one network serve all corporate needs, rather than having several unique networks serving unique parts of the enterprise. If implemented well, and expansion keeps pace with increasing traffic loads, this can result in a better, higher capacity network for all users.

## **Easier to Exchange Data**

Data is much easier to exchange between different computer systems within the company if they all use the same network. Communication protocols, media, etc., are consistent and do not pose problems. Furthermore, the more easily a company can exchange data between departments, the more valuable the data becomes because it is more readily available to any and all parties who can make profitable use of it.

## **Utilize IT Communication Expertise**

SCADA system support staffs have become smaller and smaller over the years. This makes it increasingly difficult to maintain sufficient technical expertise in all necessary areas. By moving to the corporate IT network, the SCADA system support staff will no longer need to maintain or expand the network used by the SCADA system.

## **Saves Money**

This is usually the biggest single motivator to move the SCADA system to the corporate data network. In some ways, saving money is just a summary of the earlier benefits but, in other ways, the move to more up-to-date standardized network protocols and media would produce cost savings, whether done as part of a consolidation or just an upgrade of a separate SCADA network.

## **Insufficient Capacity**

A major concern about moving the SCADA system to the corporate data network is the issue of adequate communications capacity. This can manifest itself in several ways:

1. SCADA system performance suffers from a consistent lack of adequate capacity, reacting by being sluggish and unresponsive to dispatcher requests with many communication errors and inability to maintain the defined scan rates for RTUs/PLCs.
2. SCADA system performance suffers from periodic lack of adequate capacity caused by peak use by either the SCADA system or other users on the network. This situation can be difficult to diagnose since problems caused by excessive network loading may not be observed until after the network load has subsided.

3. Latency differences caused by different network routing of messages can cause trouble with precisely tuned timeouts implemented in many SCADA systems. Timeouts for polling of field data may need to be increased to account for the slowest possible path. This will reduce the throughput of the affected circuit whenever a field unit is truly not responding.

### **Lower Reliability**

There is still a significant difference in the mindsets of the IT and SCADA departments regarding what is sufficient reliability. The most glaring example of this is when you discuss availability figures with each department. In most cases, the SCADA department determines reliability, assuming 24 x 7 with NO SCHEDULED DOWNTIME. Conversely, the IT department determines their reliability figure, assuming they get several hours of SCHEDULED DOWNTIME each week which do not count against availability. The IT group also often considers a single point of failure to be acceptable, while the SCADA system designers do not.

### **Less Secure**

Using one network for all corporate and SCADA needs introduces security issues never addressed by the current generation of SCADA systems. Systems, including more products in wide commercial use, are much more susceptible to abuse by people both within and outside the company because they are so much more easily understood and so many more hacking tools are available. Just think about the havoc one employee could cause by loading any of a number of PC-based SCADA packages on their office PC and configuring it to poll and control your SCADA RTUs/PLCs!

### **Loss of Control**

The SCADA system support group is still coming to terms with the loss of control of the entire system inherent in its reduced headcount. Relying on another department for support may relieve them of some responsibility, but it can be very frustrating when the other department does not have the same sense of urgency about an existing problem.

### **CONCLUSION**

Now that we have reviewed the pros and cons of SCADA system dependence on the corporate data network, what recommendations do we have for pipeline operating companies? The economics of the situation are so overwhelming that we believe virtually all SCADA systems will soon be dependent on the corporate data network for critical SCADA functionality. Thus, the real issue is how to maintain the requisite level of reliability, performance, and security.

We suggest the following:

1. Segment the network to logically isolate the SCADA portions of the network as much as possible. The goal here is to prevent the widely varying traffic load on the corporate data network from adversely affecting the SCADA system.
2. Regularly audit the network responsiveness and throughput to ensure the SCADA system will always have adequate capacity to handle normal and abnormal conditions.
3. Ensure there is no single point of failure in the corporate data network that would make any critical SCADA function unavailable.
4. Negotiate the network availability with the IT network support staff and make sure both are using the same assumptions in calculating the percentage available figure. Follow up by verifying compliance during audits.
5. Work with the IT network support staff to implement methods to ensure only properly authorized SCADA resources can monitor and control field devices and components of the SCADA system.