Fostering SCADA and IT Relationships:
An Industry Perspective

Christopher Beggs, Security Infrastructure Solutions, Australia

Ryan McGowan, Goulburn Valley Water, Australia

ABSTRACT

In recent years, critical infrastructure utilities have been faced with conflicting attitudes and cultural differences of where SCADA (Supervisory Control and Data Acquisition) and IT fit into an organizational structure. This lack of understanding between SCADA, IT processes, and business operations remains a concern for many utilities within the SCADA community. The importance of SCADA and IT relationships is an area of the SCADA landscape that is often unrecognised. This paper examines the results and findings of a SCADA and IT relationship survey that was undertaken to identify where SCADA operations fit within organizations around the world. It describes several proposed models that define the role and responsibility of SCADA within an organizational structure. It also presents a concept model for SCADA security responsibility and identifies key observations of SCADA and IT working together at the INL Control System Cyber Security Training in Idaho, USA. The main findings of the research suggest that clear defined roles and responsibilities for SCADA operations and SCADA security need to be established and secondly, that immediate cultural driven change is required in order to improve SCADA and IT relationships.

Keywords: *Information Technology (IT), Relationships, Responsibility, Security, Supervisory Control and Data Acquisition (SCADA)*

1. INTRODUCTION

SCADA (Supervisory Control and Data Acquisition) systems have evolved since the 1960s from stand alone systems to networked architectures that communicate across large distances. Their implementation has migrated from custom hardware and software to standard hardware and software platforms (Krutz, 2006). SCADA systems form part of Australia's critical infrastructure. They are used to remotely monitor and control the delivery of essential services and products, such as electricity, gas, water, waste treatment and transport systems (TISN, 2008).

The need for security measures within these systems was not anticipated in the early development stages as they were designed to be closed systems not open systems such as the Internet. The increasingly networked and linked infrastructure of modern SCADA systems has changed those early security plans. Utilities in the industrial control sector have integrated

DOI: 10.4018/ijcwt.2011070101

these SCADA networks with their business networks which unfortunately has exposed them to a series of vulnerabilities and risks Internet Security Systems (INL, 2005).

These risks and vulnerabilities have arisen because of system development on open based communications standards like Ethernet Communications and web enabled screens. SCADA software companies have embraced the Transmission Control Protocol and Internet Protocol (TCP/IP) to improve integration across multiple systems. However, these developments have exposed the industrial sector to common Internet vulnerabilities within communication protocols, which increase the risk of attack (Pollet, 2002).

More importantly, minimal recognition has been given surrounding the conflicting cultural attitudes between SCADA and IT departments amongst many utilities around the globe. Wiese (2002) claims that there are common reactions from SCADA engineers when the topic of SCADA and IT integration is raised. He argues that it is hard enough installing SCADA without opening up all sorts of project interfaces. Some examples may include but are not limited to:

- Lack of understanding regarding the requirements of availability and reliability;
- Lack of understanding of each other's roles and responsibilities;
- Lack of commitment between both departments; and
- Support arrangements.

These issues as well as others are discussed throughout this paper formulating the main research topic for discussion. The paper examines the findings of a SCADA and IT survey that was undertaken to identify where SCADA and IT fit into an organizational structure. It proposes that developing better relationships between SCADA and IT will improve better utilisation of resources, cross-skill multi-disciplined teams as well as improving SCADA security practices. The paper identifies the need for improvement and change in organizational dynamics in order to foster SCADA and IT relationships.

2. SCADA AND IT SURVEY METHODOLOGY

A SCADA and IT survey was undertaken with the intention to measure where SCADA and IT fit into utilities organizational structure. The survey's purpose was to identify the following:

- Current relationship trends between SCADA and IT departments?
- Should SCADA and IT be under the one operations department?
- What are the security implications of integrating both SCADA and enterprise networks? (*A discussion of the security implications is beyond the scope of this paper: see sources NIST, 2008; NISCC, 2005*).

The survey sample (see Appendix) was conducted by the authors using the SCADA Perspective mailing list and the SCADASEC mailing list. Both mailing lists are international and include members who own and operate critical infrastructure. A total of 56 members from the mailing lists participated in the survey. Majority of these members were SCADA engineers, IT professionals and security personnel. The results and findings of the survey are discussed throughout this paper.

Figure 1 provides a high level overview of the participants and their industry sector. These results indicate that participants were predominantly from large utilities such as water and electricity. It should be further noted that 80% of respondents indicated they were from large organizations of greater than 200 employees. Figure 2 provides information regarding breakdown of the country of the respondents.

3. SCADA AND IT RELATIONSHIPS

The adoption of Ethernet and TCP based protocols has provided many benefits to SCADA systems by improving system performance, load balancing and measurement analysis. These