Case Study: SCADA Security Project for National Water Company

A large national water company with annual sales of $500 million, has asked Comsec to assist the company in assessing the security level of its SCADA system implementation. As a part of its daily activities, the company operates more than 800 pumping stations, over 1,200 wells (the pump setting of some is as deep as 400 meters), more than 2,400 pumps and other installations that spread over 10,500 km and assist the organization with the provisioning of water supply, assurance of the water quality, infrastructure, sewage purification, desalination, rain enhancement and more.

Based on the client's specific requirements, Comsec decided to perform a comprehensive risk assessment including a high level assessment of different components of the SCADA system. This method assured that the organization would gain cross organizational information regarding its SCADA systems security. This information assisted the organization in prioritizing the various findings and deciding on the follow up SCADA security assessments to be carried out.

In order to provide such a comprehensive overview of the organization's SCADA systems security, Comsec assigned a diverse team of security consultants. This allowed the Comsec Team to assess the SCADA systems security in different levels.

- **Wireless connections** – checking whether there are non-secure wireless connections between remotely managed control points are susceptible to attack from a malicious user.
- **Physical security** – SCADA systems are often physically distributed over large areas, making physical security a challenge. Simple vandalism is a real / well known risk.
- **Simple protocols** – SCADA protocols tend to be quite simple, with little or no protection against spoofing, replay attacks, or a variety of Denial of Service attacks.
- **Password Management** – Due to the fact that there may be thousands of devices, passwords will tend to be identical in devices as a practical matter. In addition, because of the need for positive access and control of SCADA Systems, there is a trend toward simple, known and shared passwords.
- **Buffer overflow** – During an alarm event, the alarm processor can stall. With the software unable to complete that alarm event and move to the next one, the alarm processor buffer can fill and

eventually overflow. Thus, the control room operators lose the alarm function that provides audible and visual indications when a significant piece of equipment changed from an acceptable to problematic status.