Abstract

Supervisory Control and Data Acquisition (SCADA) systems is one of important software systems which are used for monitoring and controlling industrial systems that are geographically spread over thousands of kilometers. These systems need to monitor and control so many field sites through thousands of devices that are varying in type, technology and usage. There are different types of people need to access SCADA systems for different purposes. Because of the sensitivity and spreading of these systems, they are vulnerable by hackers and crackers and there are many risks may causes partially or fully breakdown. To managing the SCADA systems, there are number of solutions that had been placed. These solutions varied from detecting one to more of SCADA system risk and assessed them on real system once it occurs. This way causes some damages could happen till the risk is eliminate or could need adaption
that difficult or impossible to process. We propose in this paper a new framework for assessing and managing risks of the SCADA systems before they actually implemented by using one of risk management methodologies through scanning and testing proposed SCADA system architecture and its components.

References

- D. J. Kang, J. J. Lee, S. J. Kim, and J. H. Park, "Analysis on Cyber Threats to

**Index Terms**

Computer Science  
Automation

**Keywords**

Supervisory Control and Data Acquisition (SCADA)  
Attack  
Vulnerability  
Cyber security  
Risk

Software Risk Management

Risk Assessments