

## Basics of SCADA Security: A Technical Approach

**Authors :** Michał Witas

**Abstract :** This paper presents a technical approach to analysis of security of SCADA systems. Main goal of the paper is to make SCADA administrators aware of risks resulting from SCADA systems usage and to familiarize with methods that can be adopt to existing or planned system, to increase overall system security level. Because SCADA based systems become a industrial standard, more attention should be paid to the security of that systems. Industrial Control Systems (ICS) like SCADA are responsible for controlling crucial aspects of wide range of industrial processes. In pair with that responsibility, goes a lot of money that can be earned or lost - this fact is main reason of increased interest of attackers. Additionally ICS are often responsible for maintaining resources strategic from the point of view of national economy, like electricity (including nuclear power plants), heating, water resources or military facilities, so they can be targets of terrorist cybernetic attacks. Without proper risk analysis and management, vulnerabilities resulting from the usage of SCADA can be easily exploited by potential attacker. Paper is based mostly on own experience in systems security, gathered during academic studies and professional work in international company. As title suggests, it will cover only basics of topic, because every of points mentioned in the document can be base for additional research and papers.

**Keywords :** denial of service, SCADA, security policy, distributed network

**Conference Title :** ICCINS 2014 : International Conference on Computer, Information and Network Security

**Conference Location :** Paris, France

**Conference Dates :** November 21-22, 2014