

A review on current and old SCADA networks applied to water distribution systems

ABSTRACT

Water is probably the oldest factor receiving attention from the population, since the beginning of the human race. The evolution of water supply systems is directly related to the urban growth of the cities and their geographical location. This study focuses on SCADA (Supervisory Control And Data Acquisition) systems used to control and managing water distribution systems all around the world, highlighting their components and deeply approaching SCADA networks and communication protocols. Based on the need of protection and security on SCADA networks, this study aims to provide a review of the existing literature, through the case study of water distribution systems, identifying the different components of a SCADA system, as well as its communication architectures and protocols and some known attacks, to design a framework on current and old SCADA networks. Results show that SCADA systems are not just applied to water distribution and water waste systems, but also to many other industrial automated systems that control on crucial systems. The security of such systems is yet weak and faces many vulnerabilities and threats, where security mechanisms must be applied. For this purpose, the study of SCADA networks and communications is considered a crucial point for the correct development of security tools.

Keyword: DNP3 protocol; Modbus protocol; Profibus protocol; SCADA networks; SCADA security; SCADA systems; Water distribution systems