# ETSNS0005 - Security Challenges in Control Network Protocols

**Abstract**

With the ongoing adoption of remotely communicating and interacting control systems harbored by critical infrastructures, the potential attack surface of such systems also increases drastically. Therefore, not only the need for standardized and manufacturer-agnostic control system communication protocols has grown, but also the requirement to protect those control systems' communication. There have already been numerous security analyses of different control system communication protocols; yet, these have not been combined with each other sufficiently, mainly due to three reasons: First, the life cycles of such protocols are usually much longer than those of other Internet and communication technologies. Therefore legacy protocols are often not considered in current security analyses. Second, the usage of certain control system communication protocols is usually restricted to a particular infrastructure domain, which leads to an isolated view on them. Third, with the accelerating pace at which both control system communication protocols and threats against them develop, existing surveys are aging at an increased rate, making their re-investigation a necessity. In this paper, a comprehensive survey on the security of the most important control system communication protocols, namely Modbus, OPC UA, TASE.2, DNP3, IEC 60870-5-101, IEC 60870-5-104, and IEC 61850 is performed. To achieve comparability, a common test methodology based on attacks exploiting well-known control system protocol vulnerabilities is created for all protocols. In addition, the effectiveness of the related security standard IEC 62351 is analyzed by a pre- and post-IEC 62351 comparison.

**Index Terms** — Control systems, Network protocols, Network security