Teodor Sommestad
PhD Student, Industrial Information and Control Systems (KTH)

SCADA System Security

The operation and management of the electric power system depend on computerized industrial control systems, often referred to as SCADA systems. Keeping these systems secure and resilient to external attacks as well as to internal operational errors is thus vital for uninterrupted operations of power systems. This is however challenging since the control systems are extremely complex: they contain highly advanced functionality; they are heterogeneous and include several third party components; they are extensively networked, both internally and with external systems, and they depend on the human organization that manages and uses them. Yet, the systems are operating under stringent requirements on availability and performance: If control and supervision are not done in real-time, the power network may come to a collapse.

To efficiently protect systems against attacks decision makers need to be able to assess the current security posture of the enterprise's systems as well as the security posture after potential improvements. This research project aims at developing an assessment framework for SCADA system security based on enterprise architecture models. This project will from a holistic point of view develop a quantitative model of:

1) Plausible attacks on SCADA systems
2) The consequences of these attacks
3) Countermeasures and strategies for mitigating attacks

The combination of these factors will enable decision makers to assess risks with the current security posture. By expressing the influence of countermeasures on the difficulty for attackers, the intent is also to guide decision makers in selecting the appropriate security measures to employ given the architecture and posture of the system.