Sustainable Energy with Adaptive Security (SEAS)

The aim of this project is to enable new digital services in future energy cloud ecosystems through improved security practices, including adaptive and automated risk management. Currently, there is a lack of adequate approaches to manage threats and risks in the new digital energy landscape which involve both safety and security, and which can be continuously adapted and updated throughout the entire system lifecycle. We propose an adaptive integrated safety/security risk assessment approach that enables semi-automated updates and thereby remains valid over time. This approach will allow for a more rapid pace of digitalization of the sector as it removes some of the legitimate concerns associated with exposing critical infrastructure to Internet-related threats.

The Challenge

The development of a more sustainable energy system is one of the greatest challenges that we face as a society. A stable and reliable energy access is necessary for the electrification of industries and transportation and to keep Sweden as a competitive and attractive nation. The large-scale mega power plants of the past are increasingly being replaced by distributed **renewable energy sources** such as wind and solar power. The combination these systems with the digitalization of the sector and modern information technology enables the creation of **future energy clouds** where new sustainable energy services can be designed, built and deployed as software services in a cloud environment. Figure 1 shows an illustration of this idea. This allows new services to be created in a matter of weeks rather than years (or even decades) as is the case with the current systems.

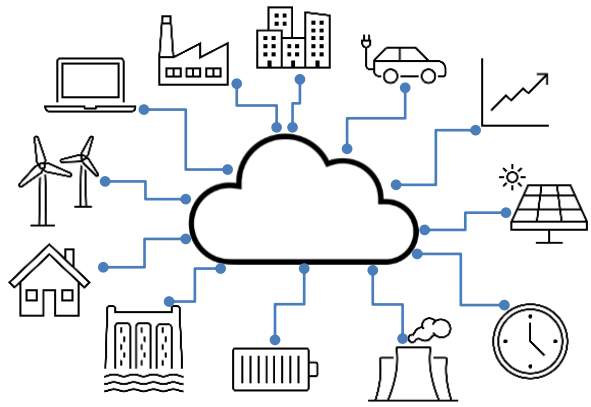

Figure 1. Future energy cloud ecosystem

The partners in this proposal see a strong shift in the market in terms of enabling new services and actors to control and aggregate parts of the energy system. This clear trend involves necessary changes that energy companies need to get involved in and adapt to. Their infrastructure and systems need to manage decentralized systems and local operators and be an active part in the development of a stable and reliable new energy landscape.

At the same time, the digitalization of the energy sector and cloudification of much of its functionality exposes these society-critical systems to **cyberattacks.** There is increasing evidence of current technologies being vulnerable to attacks as well as actual large-scale incidents (e.g. the Ukraine blackout, and the attack against Norsk Hydro). In energy systems, such attacks also pose threats to safety, and with the addition of dynamic energy clouds, risk management needs to be performed continuously rather than as a one-time effort.

When adding the fact that the threat landscape is equally dynamic with new vulnerabilities being discovered daily, it becomes clear that there is an urgent need for risk analysis and threat assessment that can adapt to changing circumstances in real-time and thus keep providing security throughout the system lifetime.

Proposed solution

In this project, we approach the problem of cybersecurity in future energy cloud ecosystems from a **risk-centred** perspective. Risk is here understood as the combination of the probability/frequency of unwanted events (i.e. attacks in the case of security) and the severity of those events. The foundation of the project is a real industrial need as established by the innovation-driven energy company Utvecklingsklustret Energi AB (UKEAB), which is collectively owned by five regional energy companies across Sweden and has the ambition to enable new digital services for sustainable energy. The use cases and innovation projects currently being initiated at UKEAB provide the starting point of this project and will be the basis of a case study on threat and risk analysis in future energy cloud systems. The project will investigate how to secure such systems and create new adaptive threat analysis and risk assessment mechanisms. The solutions will be developed by addressing and solving the following challenges:

- What kind of information flows will exist in future energy cloud ecosystems and what are the critical assets/properties that must be protected? (WP1)
- How can we adapt existing safety/security risk assessment methodologies to this domain? (WP2)
- How to enable adaptive risk management when facing changes in both the threat landscape (newly identified vulnerabilities), as well as changes to, and the introduction of new system services? (WP3)
- How can we demonstrate the feasibility of future energy cloud services as well as the adaptation of current security mechanisms to this setting? (WP4)

Project objective

The overarching aim of this project is to enable the development of new digital services in future energy cloud ecosystems through improved security practices and adaptive safety/security risk assessment.

Project partners

Linköping University (LiU): The project will be hosted by the Department of Computer and Information science, Real-time systems laboratory. The group conducts research on dependability and security of distributed systems.

Utvecklingsklustret Energi AB (UKEAB) is an innovation company in the energy sector focusing on the necessary changes associated with the digitalization of society. To meet the challenges of tomorrow, the company develops new services, engages in partnerships and invests in technical capabilities.

RISE Research Institutes of Sweden is one of the leading international research institutes with over 2800 employees and our vision is to be an international leading innovation partner. We work closely with our customers to create value, delivering high-quality input in all parts of the innovation chain, and thus playing an important part in assisting the competitiveness of industry and its evolution towards sustainable development.

Sectra: Sectra has a 40-year track record of innovation within secure communications and cybersecurity, already in the mid-1980s, Sectra received its first commission for crypto hardware from the Swedish armed forces. Ever since, Sectra has been breaking new ground in the cybersecurity area. Sectra provides managed security services for several Swedish energy companies using start-of-the-art intrusion detection technologies.