IoTSec - Security in IoT for Smart Grids

1 Relevance relative to the call for proposals

The Internet of Things (IoT) addresses the move towards a sensor-driven infrastructure for automated processes [1]. Standardised interfaces connecting cheap sensors with networks, service platforms, and applications. However, data created in the home, at work and while moving generate security and privacy challenges. The challenges are mainly related to *(i)* physical access security, *(ii)* communication network security, and *(iii)* big data security.

The vision of IoTSec is to develop secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. Such a grid will be important for both a reliable and efficient power distribution network, and for distributed, connected smart and value-added services [2]. Multiple interdependencies, uncertainties and dynamic interactions give rise to a very complex risk picture. Legacy SCADA (Supervisory Control And Data Acquisition) systems are particularly vulnerable to hacking because many were built with only physical safety in mind [4]. To ensure safe value-creation of such an interconnected power-related IoTs, preconditions from historically distinct philosophies of network management must get aligned and turned into technology and processes for safety, information security, and data protection [5]. Therefore IoTSec introduces measurable security for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties [6]. It addresses also business and end-user needs by exploring use cases for value-added IoT services. Thus IoTSec addresses the four main areas of the IKTPLUSS call:

- Resilient, secure infrastructures and systems by applying semantic modelling and provability to infrastructures;
- Privacy enhancing technologies by applying privacy measures in conjunction with measures of security and dependability;
- Cryptography and security mechanisms by establishing adaptive security and establishing measures for attack detection;
- Interaction between technology, individuals and society within the thematic areas stated above, by creating a robust cluster including academia, research institutes and industry.

IoTSec will elaborate relevant research topics, foster security methods and apply the research in the envisaged Security Centre for Smart Grids, co-located with the NCE Smart. Starting from an already existing broad international cooperation, the project is seen as a start-up to foster a cluster of research projects. The envisaged cluster of projects will gain visibility both nationally and through the EU Horizon 2020 framework, especially within the themes “Secure, clean and efficient energy” and “ICT”, as well as the ICT Cross cutting activities “IoT” and “Cybersecurity”.

2 Aspects relating to the research project

The IoTSec project aims at becoming the start-up of a research cluster in security for IoT, industrially applied by members of the NCE Smart. The project will create and consolidate the security framework for IoT, address specific research areas, and create the basis for growth through future scientific and industrial projects in the domain. The following objectives have been identified to drive the research towards a cluster of projects for secure IoT-powered critical infrastructures:

- Extend the IoTSec project to a research cluster to include at least 14 Professors/Senior Researchers, 15 PhD/PostDocs, 30 Master students and create international visibility with at least 12 projects and memberships in 5 networks/clusters.
- Tailor the research towards an operational Security Centre for Smart grids at the NCE Smart, supported by at least 15 companies and identified as an International Centre of Excellence.

2.1 Background and status of knowledge

IoTSec is built on the knowledge of the project partners, having been involved in more than 20 national and international projects related to security, IoT and Smart Grids. A short presentation of the background is presented here, while details and the research topics are listed in section 3.

Smart Grid systems, applications and networks were originally designed for pure functional purposes (e.g. connectivity, control and sensing), without considering IT security and privacy, leading to vulnerabilities that are challenging to address [5][7].

The conventional protection techniques against IT attacks in some Smart Grid subsystems, such as SCADA systems, is based on the physical isolation [8]. However, Stuxnet was an attack on such a SCADA system. The attack demonstrates that the systems are vulnerable despite physical isolation, as analysed by Langer [9]. Other attacks, such as that reported by Gorman against a U.S smart grid, show that there are general vulnerabilities that need to be addressed [10]. The coupling between cyber systems and physical system in Smart Grid raises additional security challenges for Smart Grid, because physical attacks can affect cyber systems and vice versa [11].

Smart grids also host sensors and other devices with limited resources in terms of computation, storage, power, etc. The resource constraints enforce security protocols to remain lightweight. This issue was analysed by Li [12] and Ahmed et al. [13], and some solutions to address these security challenges were proposed. Furthermore, Leister et al. proposes an assessment framework for the assessment of context-aware adaptive security solutions in the Internet of Things systems (IoT) (e.g. eHealth, smart grid…) in situations with changing environment and limited resources [14].

Additionally, Smart Grid systems raise special security challenges, merely from the size of such systems and the big volume of generated data, making it particularly difficult to detect a possible running attack [16]. Moreover, the collected data raises privacy concerns. For instance, the analysis of data collected by a smart meter could reveal the personal behaviour of house inhibitors, such as which electric devices are in use [17], and what is currently being watched on TV [18].

Finally, assessment of smart grid security, privacy and dependability level, is a challenging and complex issue. Some novel work by Noll et al. proposes to apply risk assessment methodology to Smart Grids in a simple and effective way [19]. They propose a methodology that starts with component evaluation, then tackles sub-systems and ends up with the entire system evaluation. The result is an overall level for system SPD. Moreover, the methodology shows that different system configurations cause different SPD levels. Thus, the configuration could be used to make the system reach an objective SPD level.

2.2 Approaches, hypotheses and choice of method

2.2.1 IoTSec approach

IoTSec will apply the methodologies from national and EU projects and adapt the results to establish safe value-creation on a power-related IoT. IoTSec will focus on generating security principles, aiming at industrial applicability for the Smart Grid Security Centre.

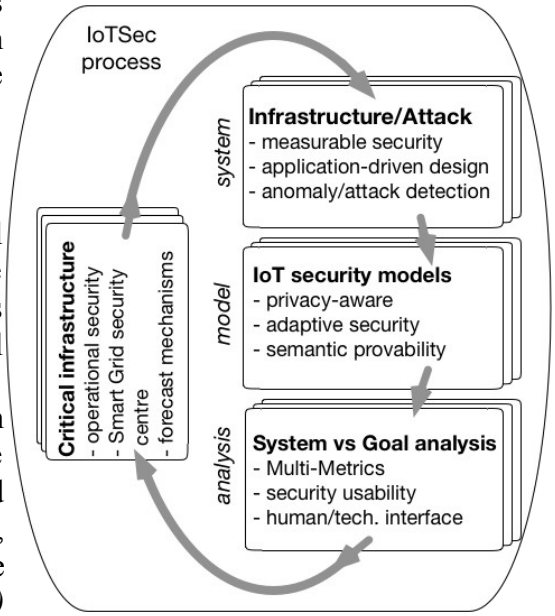

Figure 1: Overall IoTSec approach

The project follows a cyclic approach, providing in every cycle an analysis of an existing or future infrastructure with respect to security, privacy and dependability (SPD). Each cycle consists of four steps, being *(i)* the system and attack description, *(ii)* the generation and application of IoT security models, *(iii)* the evaluation of the results of the system analysis with respect to given goals for applications, and *(iv)* the applicability to critical infrastructures. Through this cyclic approach we will move from estimated security to measurable security, allowing a system description where each component and sub-system will be characterised through an (SPD)-triple. Such system analysis allows the comparison of security goals with the results from a system analysis.

In the first year of the project we will create the framework for measurable security, privacy and

security and apply it to the existing infrastructure of our industrial partner eSmartSystems. By starting with the limited current infrastructure we ensure the scalability of the measurable security demonstrated by Noll et al. in previous work [19], and provide interfaces of the security models being developed in the various activities. In the second year we will apply the framework to an envisaged infrastructures and evaluate 1-2 services with respect to their (SPD)-features. Examples of such services include billing, alarms, remote control and care taking. We will also take into operational considerations suggested by the industrial partners in order to adjust the research on system description, modelling and analysis. During the following years (3-5) the project will extend the models, apply the measurable security and provide to industry a sustainable framework.

2.2.2 Focus areas of the research

The envisaged focus areas for the research have been identified during common workshops, and are listed in the following paragraphs answering the need for system description, security modelling, evaluation and industrial applicability. The **system description** is driven by the requirements of applications, the measurability of security, and the threat modelling based on anomaly and attack detection. The expected outcome is a semantic description of the infrastructure, services, privacy and security functionality as well as attack surface.

A formal **Semantic System description** of smart Grid System infrastructure may reveal meaningful abstractions and capture relevant interfaces between different kinds of distributed units of the infrastructure. These notions will be essential when formulating dependability and security requirements, and when defining suitable metrics of system quality and behaviour. A semantic model will clarify the different subsystem interactions and notions of permitted and malicious actions. Techniques from [15] are relevant as well as probabilistic modelling [13]. The expected outcome are Semantic System descriptions transferring the formal methods into the knowledge representation of the Web, allowing for interoperability, machine-readable reasoning and runtime-checking [20].

Measurable Security, Privacy and Dependability (SPD) is a paradigm shift in the security domain. Providing goals for SPD in applications, e.g. billing information with an SPD_{Goal} of (90,80,40) and analyse the system with respect to these goals allows the criticality analysis of components, sub-systems and systems [19]. Examples of SPD analysis include for **S**ecurity the control unit of a home, or the hacking of the control center; for **P**rivacy the habit monitoring of the residents, e.g. nobody is at home; and for **D**ependability the supply security of the electrical power grid, which is mainly the component dependability of the grid. In IoTSec we will apply the JU Artemis/ECSEL SHIELD (http://newSHIELD.eu) multi-metrics methodology, and combine the SPD analysis with the semantic system description.

Event driven adaptive security addresses events such as RFID-based physical access control or sensor-based voltage monitoring. An event-driven security security architecture is seen as a perfect candidate for real-time security monitoring of the entire grid operations. The basis of the work was addressed in the MASSIF Project (http://www.massif-project.eu/), and will be adapted and extended for utilising and modelling “events”.

Anomaly detection has the goal to cope with specially tailored worms such as Havex, Stuxnet, Flame and others [21] [22]. Due to their resilience to be detected and their persistence, these worms are considered as Advanced Persistent Threats (APTs) [23]. Since APTs are considered as zero-day attacks, traditional security measures are not capable of detecting them. Industrial Control System networks are characterized as static in terms of communication patterns and configuration of devices [24]. Thus, ICS networks, and consequently Smart Grid networks, are suitable for creating network traffic models [25]. Created traffic patterns will be used to perform anomaly detection, becoming a new type of security mechanism which will increase the resilience and security of Smart Grid infrastructures and system. The expected outcome are network traffic models for each network segment to detect anomalies establishing a new type of security mechanism.

The following paragraphs describe components of **IoT security models** to establish adaptive

security models being privacy-aware. Through semantic modelling we will address formal methods for semantic provability of system of systems.

Privacy-preserving and accountable authentication framework addresses secure and reliable communication procedure among the customers and the service providers. The challenge is to preserve privacy among the entities in a distributed manner without relying on a trusted third party. We will apply different models of non-cooperative and cooperative game theory to utilize competition between the service providers to build a reputation scheme and enforce cooperation among the providers to attract a larger number of consumers to subscribe to their services.

Privacy-preserving demand response management (DRM) refers to mechanisms that can reduce or shift peak-to-average ratio, thereby reducing the peak demand and increasing grid stability. One precondition in implementing effective DRM is the power usage awareness, which needs users' active or passive participation. Power usage and operational data can be abused to infer customers' personal information, daily activities and habits. The privacy-preserving demand response management and the tradeoff involves a widespread use of electric vehicles, massive number of intelligent devices, and high penetrations of renewable energy sources. We will establish a model being able to predict and respond to individual consumer or utility preference, both competitively and cooperatively. This will potentially allow for energy consumption scheduling to coordinate and obtain mutual benefits for participating network operators.

Semantic provability builds on the semantic model description that allows machine understanding and automated tools. A model may be exploited by *(i)* model-based tools for static checking and for model-checking, *(ii)* semantic driven testing and generation of test cases (as in [26]), *(iii)* semi-automatic verification [27], and *(iv)* runtime-testing of essential properties. Finite state machines may be used to control and correct the interactions of subsystems [28], and interpretation of rule-based models may be used to check properties (as in [20]). The research in semantic provability is in an early stage, thus we expect to analyse reasoning techniques for model consistency in the first year. We will generate smart grid test cases in year two and apply a semi-automatic verification in year two. Further research will then address the complexity of system-of-systems and the heterogeneity of applications addressing different (SPD)-goals. Examples of such a research will address if alarm services (burglary with goals of (60,5,80) and billing with goals of (80,60,40)) can be provided over the same infrastructure.

The application-driven **system versus goal analysis** will be driven by a Multi-Metrics approach, taking into account security usability and the human/technology interface. **Security usability** deals with the limitations of user interfaces of smart "things". Grid-related "things", such as power meters, web services and apps used for interaction with the grid; esp. on user side, is an important aspect. Based on the EU-prosjekt UTRUSTIT [29], (http://utrustit.eu/), we will ensure the presence of trust status signals and intervenability for users [30] through usable interfaces.

Risk management of the interface between humans and technology in an IOT setting follows the privacy risk analysis from the PETweb II project (http://petweb2.projects.nislab.no) to the design of risk-based adaptive security and privacy. It includes the identification and analysis of privacy, cyber, information security threats, vulnerabilities and mitigation/response/recovery measures. Mechanisms to modify the perceived incentive structures such as to align stakeholder interests will be developed and analysed. This task will develop a library of utility factors suitable for an IoT setting involving critical infrastructure. Furthermore, we will identify and construct stakeholder archetypes and strategy taxonomies matching the smart grid operator requirements. The artefacts constructed will be evaluated and tested assuming an operational environment. The expected outcome will be a simulation platform for IoT critical infrastructure projects, offering improved accessibility and quality together with reduced cost of risk management.

Multi-Metrics analysis is a methodology which evaluates the entire system SPD level [31]. The presented methodology starts by evaluating each component of the system to jump over sub-system evaluation and end up with the entire system SPD level. Though the multi-metrics approach was

applied to sub-systems in Smart Grid [19], a complete system analysis is still to be performed to demonstrate the scalability of the system. A novel research aspect is the combination of adaptive security, e.g. using the metrics from the EU GEMOM project (http://www.gemom.eu), and the multi-metrics analysis.

Applicability of the security models and modules will be implemented in the security lab hosted by NCE Smart and drives the development of the framework components. Mechanisms to visualise security, e.g. security usability are applied to enhance the human acceptance of the measurable security. Through common workshops research institutes and industry will identify challenges such as forecast mechanisms and address upcoming infrastructures and services.

Adaptive security addresses the protection of "IoT-based smart grids" against evolutionary threats and attacks through the prediction and advanced behavioural analysis of big-real-data from IoT Smart Grids [32]. Our approach on adaptive security is based on [33], and security metrics methodology based on [34]. The adaptive security methodology addresses threats by increasing awareness and automating prevention, detection, and recovery from the failures of security and privacy protections at runtime by re-configuring control parameters and even changing structures and security goals. The objective is, therefore, to develop adaptive security mechanisms using the combination of evolutionary game theory and distributed behavioural analysis for Smart Grids. The expected outcome of this work are modules for use in the operational security.

Privacy by Design patterns deals with privacy regulations and privacy risks for processes with a large amount of personal data or personal contexts. This task will construct Privacy by Design patterns for IoT applications, involving questions such as how to design and build privacy designs for metering and control of grid-connected devices and protocols with privacy design patterns; how to carry out risk analysis [35], privacy impact analysis [36], and how to deploy user-centric privacy technology. These include patterns and protocols for removing/obscuring subscriber identity, protocols for privacy-preserving data aggregation (for statistics), and related protocols. A secondary objective of this task is security technology Task-technology-fit. It deals with the alignment og technology, business model, security model, and privacy requirements into processes such that they overlap sufficiently with business model and the economic constraints [37].

Industrial applicability is ensured through the industrial partners contributing with their operational and business knowledge in running the power grid. IoT, though being a new area for most power-distribution companies, is seen as a core technology to enhance the monitoring of the power grid. Some of the challenges identified are the inclusion of IoT technologies in the operational network, the measurable effect of load-control on infrastructure components, and privacy-aware infrastructures. Small scale forecast models addressing local distribution networks and the impact of active-load control on these forecast models are other open issues. While the latter one is not addressed through this research, the IoT-based monitoring will provide data to enhance the models and satisfy requirements from authorities like Norwegian Water Resources and Energy Directorate (NVE) and Norwegian Directorate for Civil Protection (DSB).

3 The project plan, project management, organisation and cooperation

3.1 Work packages, management and measurable outcome

The project is composed by a total of 5 work packages (WPs), subdivided into tasks (T0.1...T4.3). Three WPs (WP1-WP3) concentrate on scientific research, and WP4 focussing on validation and industrial update. WP0 has the focus on management and collaboration, and thus will coordinate scientific dissemination, industrial exploitation and international liaisons. WP4, paving the way for the industrial security centre, will also extend the cluster into industry.

WP0 Project management, Dissemination and Exploitation [UiO/UNIK]

- T0.1 Project management, Collaboration platform, supervision of PhD students
- T0.2 Dissemination, Scientific Papers, workshops, liaisons, industrial take-up

WP1 Semantic system, application, and attack description [NR]

- T1.1 Semantic description of infrastructure, attack detection, system view;
- T1.2 Measurable: security, privacy and dependability, metrics

WP2 Development of security models and modules for IoT systems [UiO/Ifi]

- T2.1 Development of privacy-aware models and measures
- T2.2 Adopting and enhancing adaptive security for system of systems
- T2.3 Formal technologies for semantic provability

WP3 System versus Goal analysis for measurable security [HiG/CCIS]

- T3.1 Multi-metrics applied for application-driven infrastructures
- T3.2 Human/technical interface, security usability

WP4 Operational security for IoT-based critical infrastructure [NCE Smart]

- T4.1 Operational security driven assessment of methods, models and modules
- T4.2 Smart Grid security centre applicability
- T4.3 Gap Analysis of security methods for critical infrastructures

The management roles and responsibilities within the project are described in figure 1. Each specific role and function will be defined in detail by the project plan. The **project owner** acts as the project's contractual partner towards the Norwegian Research Council, as well as the other project partners. The **steering committee** assists the project owner with overall guidance and priorities of the project, and will approve the updates of the project plan after 24 and 48 months. The **steering group** will initially consist of representatives from partners, but will be extended according to the growth of the cluster. Special focus is giving to industrial representatives and liaison partners, as they form the contact base to industrial associations, networks and clusters.

The project manager Prof. Josef Noll leads the project on behalf of the project owner (UiO), Dr. Habtamu Abie (NR) co-ordinates the research, and Hilde Bekkevard (NCE Smart) co-ordinates the industrial applicability. The Work Package leaders (in brackets in the list of WPs) have the responsibility for progress and co-ordination of the scientific work as well as the adaptability for industry.

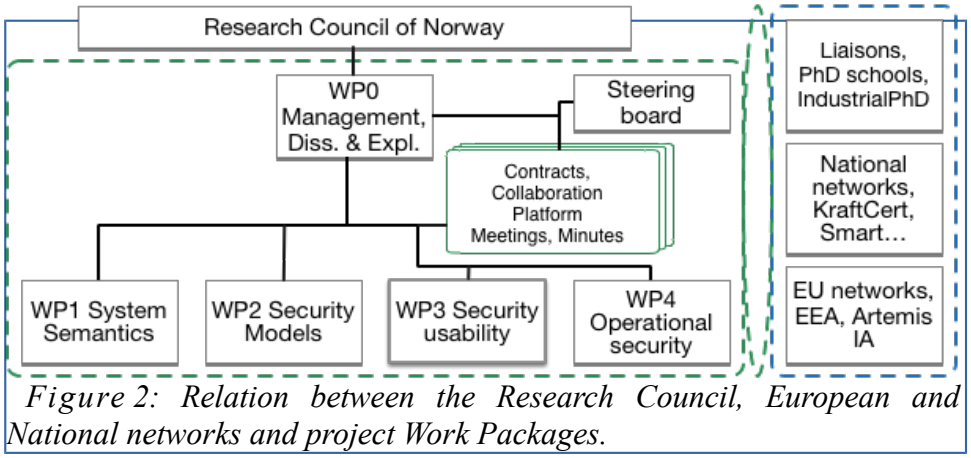

Figure 2: Relation between the Research Council, European and National networks and project Work Packages.

The 33 deliverables described in table 1 will document the achievements in the first 24 months, an update of the project plan will thereafter define further research priorities and identify new deliverables. For the technical deliverables, a draft bulleted report with a detailed TOC is foreseen at M12 on the collaborative Wiki, while the full technical notes are provided at M24.

Table 1: Deliverable descriptions and relation with Work Packages.

Deliverable	WPx	Description	Month
D0.1	WP0	Collaborative Knowledge Platform	M3
D0.2-D0.3	WP0	Annual reporting, including plans for next 12 months	M12, M24
D0.4-D0.9	WP0	4+2 scientific papers submitted	M12
D0.10-D0.18	WP0	6+3 scientific papers submitted	M24
D0.20,D0.21	WP0	Workshop invitations and minutes	M12, M24
D1.1-D1.4	WP1	Tech.rep.: infrastructure, attack, meas. sec., metrics	M12,M24

D2.1-D2.3	WP2	Tech.rep.: privacy awareness, adaptive sec, semantic provability	M12,M24
D3.1-D3.3	WP3	Tech.rep.: multi-metrics, human/technical, usability	M12,M24
D4.1	WP4	Tech.rep.: Assessment/validation of models	M12, M24
D4.2	WP4	Pres. & summary: Outline security centre	M12
D4.3	WP4	Pres.: Roadmap of security modules	M24'

The measurable outcome of IoTSec is planned along four axis, the robustness of the research cluster, the scientific outcome, the international excellency, and finally the industrial uptake (tab. 2).

Table 2: Measurable outcome of IoTSec

Year	Robust cluster	Scientific outcome	International excellency	Industrial uptake
Y1	11 Prof./Senior Researchers Hired 3 PhD/ PostDocs Research school agreement	IoTSec framework 4 conf papers 2 journal articles 2 workshop	Member of 3 ETPs, IAs 2 project proposals	Outline of Security Centre for smart Grid Uptake of 2 approaches
Y2	2 IndustrialPhD 2 envisaged/started PhD	6 conf papers 3 journal articles 2 workshops	5 international project proposals 2 international projects	Future infrastructure 3 methods/modules roadmap; Industrial project proposal
Y3	3 PhD, 1 Industrial PhD	Book IoTSec outline Special session 6 conf papers 2 journal articles	3 project proposals International partnerships	Smart Grid Security Centre established 15 companies involved
Y1-Y5	Total of 14 Prof./senior researchers, **15 PhD/PostDoc engaged**	Book published Total of 25 conf papers 12 journal articles 9 workshops	Total of **12 national and international projects;** Membership in 5 intern. networks	Total of 18 modules evaluated, 9 modules applied Int. Centre of Excellence

3.2 International cooperation, competences and contributions

The project partners are currently involved in 13 international projects in addition to the national projects. Through bundling the competences in the Smart Grid Security Centre we will increase the international visibility, and become even more attractive for international collaboration.

Table 3 provides details on key personnel, core competence and contributions of each partner.

Table 3: Competence and contribution areas of different partners.

Name	Core competence	Contribution
University of Oslo (UiO:UNIK,Ifi) Prof. Josef Noll, Prof. II Leif Nilsen, Prof Olaf Owe, Prof. Paal E. Engelstad	UiO has together with UNIK and Simula established the Strategic Research Initative for Concurrent Security and Robustness for Networked Systems (ConSeRNS), answering the needs for security in distributed infrastructures.	UiO will contibute with Measurable Security, Multi-Metrics, formal semantics, and Semantic Provability
Norwegian Computing Center (NR) Dr Habtamu Abie, Dr. Lothar Fritsch, Dr. Åsmund Skomedal	NR's research in the area of ICT has a main basis in adaptive security, privacy and interactive, network-based smart technologies. More than 10 nat./int. projects in this area.	NR will contribute with a broad range of research capabilities within adaptive security, privacy, metrics, risk assessment, modelling and simulation. NR will give access to adaptive security testbed.
Gjøvik University College (GUC) Prof. Einar. Snekkenes	Within the Faculty of Technology, GUC has established postgraduate programs of high relevancy to the IoTSec project. There is both a Master of science and a PhD program in Information Security. GUC hosts the Center for Cyber and Information Security (CCIS).	GUC will give the project access to the academic environment at NISlab. In this project the main contribution will be Prof. Snekkenes experience within theoretical modelling here applied to privacy risk modelling and analysis. GUC will run the PhD school.
Smart Innovation Østfold	CE Smart has its core competence in the	NCE Smart will contribute with its cluster

(NCE Smart) Hilde Bekkevard, Prof. Bernt A. Bremdal, Dieter Hirdes, Ulrika Holmgren	intersection between IT and energy and between industry and research. NCE Smart is host to a world-leading cluster within the energy and ICT fields,	of industries in the energy sector, i.e. energy companies and suppliers industry. NCE Smart will liaison with DSOs and SmartGrid demo sites. In addition to this, they will contribute with expertise in SmartGrid control center design.
eSmartSystems (eSmart) Erik Åsberg, Dr. Knut Johansen	eSmart Systems is delivering software for energy companies based on a state of the art data platform and cloud services. eSmart has two PhD candidates among its staff.	eSmart will contribute with ICT hands-on knowledge in Big Data technologies that will be central in tomorrow's IoT infrastructure, and evaluate the results of the academic work.
Frederikstad Energi (FEN) Vidar Kristoffersen	FEN is a Norwegian Distribution Service Provider (DSO) with core competence in planning and operation of distribution grids.	FEN is a leader in utilization of Smart Meters and will contribute as a partner for regulations, operational requirements and demonstrations
EB Nett AS (EB) Otto Andreas Rustand	EB is a significant utility in Norway and has a clear focus on new services for the distribution grid following the roll out of smart meters.	EB will focus on security related to IoT Services used for load shifting and control of end user equipment in the distribution grid. An important aspect of this is delivery of services in accordance with law and regulations.
Movation AS (MOV) Bjarne Haugen, Seraj Fayyad	Being an innovation company MOV has recognised the need for security and privacy as the drivers for collaboration in the era of IoT. MOV was project leader for the SHIELD pilot, and application leader in nSHIELD project, both preparing measurable security for IoT.	Measurable Security, Privacy and Dependabiltiy. Multi-Metrics Approach Arena for value-added-services on secure Smart Grid infrastructures. MOV provides the arena for VAS on a smart grid infrastructure through the InnoBørs.
Simula Research Laboratory (SRL) Dr. Yan Zhang	SRL is a non-profit research institute focussing on scientific challenges with long-term impact.	SRL will focus on robust and secure infrastructure, services and future distributed applications, especially the privacy-aware provisioning

University of Oslo (UiO) is the largest university in Norway, with 27.000 students. For UiO (UNIK, Ifi, Simula) the IoT project will consolidate Information Security as a key topic at the Institute of Informatics (Ifi). Both UNIK and Ifi have through their strategic groups for Information Security identified key recommendations, which are implemented a.o. through the strategic research initiative ConSeRNS. Through ConSeRNS, members of 4 research groups collaborate to focus on information security and robustness. UNIK has a tight collaboration with FFI on IoT- and communication-related security, resulting in a series of Master- and PhD theses. UiO and UNIK have been involved in a series of EU projects like Credo, Hats and nSHIELD.

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modelling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. NR has a long record of participation in EC funded related projects like HARP, CORAS, uTRUSTit, as well as national projects such as PETweb and ASSET.

Gjøvik University College (GUC) is a state University College in Norway and has approximately 2600 students and 208 employees and administrative staff. The information security group at GUC is the Norwegian Information Security laboratory (NISlab) and the Center for Cyber and Information Security (CCIS).

Simula Research Laboratory (SRL) is a non-profit research institute publicly funded by the Norwegian Government. SRL offers an environment that emphasizes and promotes basic research, but is also involved in education, and innovation. The Department of Networks focuses on research

into robust and secure infrastructure, services and future distributed applications. SRL has 2 ongoing projects in the area of Smart Grid: PRONET and TIDENET.

Smart Innovation Østvold (NCE Smart) is a cluster and a competence center that develops smart and sustainable energy solutions through innovation and business development. The company Smart Innovation Østfold AS is the facilitator of the cluster. The cluster represents internationally oriented businesses with a total revenue of €2,5 billion. NCE Smart is a pioneer in energy market design and implementation, and has a long track record in SmartGrid and Smart Energy Markets research. The cluster is responsible for innovation projects totalling more than €30m. Three of the projects in the cluster were EU commissioned. The cluster leads the H2020 EMPOWER project and is involved in the FP7 Smart Rural Grid, as well as the RCN projects FlexNett and ChargeFlex. NCE Smart currently has 3 SmartGrid related PhD candidates. Security has been identified as a key-component for the growth of smart energy solutions.

The background of the **industrial research partners** are already provided in the table, and are not repeated here.

3.3 Budget

► Budget planning is included in the grant application form.

4 Key perspectives and compliance with strategic documents

4.1 Compliance with strategic documents

For UiO (UNIK, Ifi, Simula) the IoT project will consolidate Information Security as a key topic at the Institute of Informatics (Ifi). Both UNIK and Ifi have through their strategic groups for Information Security identified key recommendations, which are implemented through strategic initiatives. By including SIMULA's research on robustness and NR's competence on secure and privacy-aware services we create a scientific cluster of international excellency. Specific aspects like user/technology and risk management are contributed by the CCIS located HiG, being amongst the leading academic institution in this field in Norway.

The NCE Smart and eSmartSystems have identified security and privacy as core drivers for the acceptance of Smart Grids. They are already one of the leading clusters in Europe in this field, and will strengthen their position through the collaboration with the academic partners.

4.2 Relevance and benefit to society

The planned roll-out for smart meters in Norway by 2019 is preparing the ground for local electricity production and a complete new prosumer centric electricity market, allowing for full integration with micro-scale renewable energy sources and a greener energy market. In addition to this positive environmental impact on the society, it will also increase the stability of the power grid, add efficiency in supply and lay the ground for other value-added services.

The project will contribute to the security of such systems, which is a prerequisite for the successful implementation of a real Smart Grid in Norway. Such security should be implemented at a high communication layer, typically requiring a gateway per household, so that several services can use the same security solution. Installing it together with a smart-meter will save about NOK 7,000-8,000 per household or about NOK 16-18b for the society.

In addition, the Internet of Things by itself is seen as one of the main drivers for innovation in the society. DNV-GL pointed out that sensors will drive the automated data management, and thus the change from passive data to automated decisions by 2020 [38]. Security in IoT is the key issue for business development, as trust and privacy-aware handling of data and information are required for multi-partner interactions. The societal benefits of IoT services are even more significant. Cost calculations done by D'Angelantonio and Oates indicate the costs for technology-assisted living are only 2-5% as compared to elderly institutions, and 0.5-1% of hospital costs [39].

The scientific research and the applicability in the novel Security Centre for Smart Grid will also be of fundamental importance for the exchange of information between service providers. Reliable

information is the basis for automated processes, as well as innovative services for the society.

4.3 Environmental impact

Smart Grids will enable a greener energy market by integrating renewable micro-scale energy sources. Furthermore, the transport and distribution grid will be better exploited, reducing the need for long distance high voltage power lines through untouched nature (e.g. the "monster masts" over Hardangervidda). The project will contribute to the security of such systems, which is a prerequisite for the successful implementation of a real Smart Grid in Norway. No negative environmental impact is expected from this project.

4.4 Ethical perspectives

Privacy issues are a core concern with respect to ethical perspectives. Having privacy-aware ICT/society as their field of work, project members will ensure that privacy is respected according to the guidelines of the Norwegian Data Protection Authority ("Datatilsynet"). Moreover, the IoTSec project will not carry out experiments beyond the borders of information systems, connected to sensors and electrical power grids. Other ethical topics, such as social justice, non-neutrality of IoT, and autonomy are considered outside of the scope of this project. Regarding all ethical topics, the project is bound to the ethical recommendations as laid out by UiO.

4.5 Gender issues

IoTSec has a specific focus on being attractive for women. Hilde Bekkevard (NCE Smart) co-ordinates the industrial applicability, is such a high-visible person, and will contribute in the recruitment process. Dr. Sabita Maharjan and Ulrika Holmgren are also members of the project team. They will help in recruiting women for the envisaged work through a.o. the Security Divas social network for women in information security.

5 Dissemination and communication of results

► Dissemination and communication of results is provided in the grant application form.

6 Additional information specifically requested in the call

► LoI from all partners and CV of key personnel is provided in the grant application form.

7 References

[1] DNV-GL, "From technology to transformation", DNV GL TT Report http://dnvgl.com/Images/From%20technology%20to%20transformation_tcm212-595538.pdf

[2] Y. F. Wang, W. M. Lin, T. Zhang, and Y. Y. Ma, "Research on application and security protection of Internet of Things in smart grid,", ICISCE, 2012.

[3] A. Koubatis and J.Y. Schönberger, Risk management of complex critical systems, Int. J. Crit. Inf., 1(2/3), pp. 195-215 2005

[4] K. McDowell, Critical Infrastructure and the Internet of Things, EDUCAUSE Review, 2014, http://www.educause.edu/blogs/vvogel/critical-infrastructure-and-internet-things

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber Physical System Security for the Electric Power Grid," Proceedings of the IEEE, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] J.Noll, "Measurable Security for Sensors - the Driver for Innovation", SICS Security Seminar, 8 April 2014, Stockholm

[7] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber-attacks," in Innovative Smart Grid Technologies (ISGT), 2010, 2010, pp. 1–7.

[8] P. E. Nordbø, "Cyber security in smart grid stations," 22nd Int. Conf. and Exhibition on Electricity Distribution, 2013.

[9] L. Langer, F. Skopik, G. Kienesberger, and Q. Li, "Privacy issues of smart e-mobility," in Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE, 2013, pp. 6682–6687.

[10] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies", The Wall Street Journal, Page A1, April 8, 2009.

[11] Yilin Mo, T.H.-H. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1):195–209, Jan 2012

[12] Y. Li, "Design of a Key Establishment Protocol for Smart Home Energy Management System," in CICSyN on, 2013, pp. 88–93.

[13] K. A. Ahmed, Z. Aung, and D. Svetinovic, "Smart Grid Wireless Network Security Requirements Analysis," in iThings/CPSCom on, 2013, pp. 871–878.

[14] W. Leister, S. Poslad, M. Hamdi, H. Abie, and A. Torjusen, "An Eval. Framework for Adaptive Security for the IoT in eHealth."

[15] F. Skopik, I. Friedberg, and R. Fiedler, "Dealing with advanced persistent threats in smart grid ICT networks," in Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES, 2014, pp. 1–5.

[16] P.-Y. Chen, S. Yang, and J. A. McCann, "Distributed Real-time Anomaly Detection in Networked Industrial Sensing Systems," IEEE Transactions on Industrial Electronics, pp. 1–1, 2014.

[17] E. Buchmann, K. Böhm, T. Burghardt, and S. Kessler, "Re-identification of Smart Meter data", Personal and Ubiquitous Computing, Springer 2012.

[18] U. Greveler, B. Justus, and D. Loehr, “Multimedia Content Identification Through Smart Meter Power Usage Profiles”, 5th international conference on Computers, Privacy & Data Protection (CPDP), 2012
[19] J.Noll, I.Garitano, S.Fayyad, Erik Åsberg and H.Abie, “Measurable Security, Privacy and Dependability in Smart Grids” accepted for publication, River Journal, 2015
[20] Crystal Chang Din, Olaf Owe, Richard Bubel, Runtime Assertion Checking and Theorem Proving for Concurrent and Distributed Systems. In Proceedings of the 2nd International Conference on Model-Driven Engineering and Software Development (Modelsward'14), SCITEPRESS, DOI: 10.5220/0004877804800487, pages 480-487, 2014.
[21] ICS-CERT. ICS-ALERT-14-176-02A, *Industrial Control Systems Cyber Emergency Response Team*. Online. Accessed on January 30, 2015. Available at: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
[22] Fidler, David P, Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think. *International Journal of Critical Infrastructure Protection*. 2012 Elsevier, (5) pp. 28-29
[23] Knapp, E.D. and Langill, J.T., Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2014 Elsevier Science. ISBN: 9780124201842
[24] Hadziosmanovic, D. and Bolzoni, D. and Etalle, S. and Hartel, P., Challenges and opportunities in securing industrial control systems. Complexity in Engineering (COMPENG), 2012. DOI: 10.1109/CompEng.2012.6242970 pp. 1-6, 2012
[25] Schuster, Franka and Paul, Andreas and König, Hartmut, Towards Learning Normality for Anomaly Detection in Industrial Control Networks. *Emerging Management Mechanisms for the Future Internet.* DOI: 10.1007/978-3-642-38998-6_8. pp. 61-72, 2013.
[26] Einar Broch Johnsen, Olaf Owe, Arild Braathen Torjusen: Validating Behavioral Component Interfaces in Rewriting Logic, Fundamenta Informaticae 82(4): 341-359. IOS Press, 2008.
[27] Crystal Chang Din, Olaf Owe: A Sound and Complete Reasoning System for Asynchronous Communication with Shared Futures. Journal of Logic and Algebraic Programming, 83(5-6):360-383, Elsevier, 2014
[28] Olaf Owe, and Gerardo Schneider: Wrap your Objects Safely. In post-proceedings of FESCA'09 (6th International Workshop on Formal Engineering approaches to Software Components and Architectures, Satellite event of ETAPS, 28th March 2009, York, UK). Electronic Notes in Theoretical Computer Science 253, pp. 127–143, 2009.
[29] Schulz, Trenton; Fritsch, Lothar (2013) Identifying Trust Strategies in the Internet of Things. I: Proceedings of the User-Centered Trust in Interactive Systems Workshop: a Workshop from NordCHI 2012. Oslo: Norwegian Computing Center 2013 ISBN 978-82-539-0538-9. p.19-23
[30] Fritsch, Lothar; Groven, Arne-Kristian, and Schulz, Trenton: On the Internet of Things, Trust is Relative, Ambi-ent Intelligence - Second International Joint Conference, AmI 2011, Lecture Notes in Computer Science (LNCS) D. Keyson, M. L. Maher, N. Streitz et al., eds., Amsterdam: Springer, 2011.
[31] I.Garitano, S.Fayyad and J.Noll, “Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems” accepted for publication, Wireless Personal Communication Journal, 2015
[32] H. Abie, Adaptive Security and Trust Management for Autonomic Message-Oriented Middleware, IEEE Symposium on Trust, Security and Privacy for Pervasive Applications (TSP 2009), 2009, Macau, China
[33] H. Abie, R. Savola, J. Bigham, I. Dattani, D. Rotondi, and G. D. Bormida, Self-Healing and Secure Adaptive Messaging Middleware for Business Critical Systems, In: Int. J. on Advances in Security, ISSN 1942-2636, 3, 1&2, September 5, 2010, pp. 34-51
[34] R. Savola and H. Abie, Development of Measurable Security for a Distributed Messaging System, In: Int. J. on Advances in Security, 2, 4, 2009, ISSN 1942-2636, pp 358-380 (Published in March 2010)
[35] Fritsch, Lothar; Snekkenes, Einar (2013) Alternative Approaches to Privacy Risk Assessment: Summary of the PETweb II VERDIKT project sponsored by the Research Council of Norway (2009-2013). Oslo: Norsk Regnesentral 2013 (ISBN 978-82-539-0539-6) ;Volum 1.31pages. Report at the Norwegian Computing Center(1029)
[36] Paintsil, Ebenezer; Fritsch, Lothar: A Taxonomy of Privacy and Security Risks Contributing Factors . IFIP Ad-vances in Information and Communication Technology, 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife Inter-national Summer School, Helsingborg, Sweden, Privacy and Identity Management for Life, Fischer-Hübner, Simone; Duquenoy, Penny; Hansen, Marit; Leenes, Ronald; Zhang, Ge, International Federation for Information Processing IFIP, ISBN 978-3642207686, Vol. 352, pp. 52-63, March 24, 2011.
[37] Fritsch, Lothar. (2009) Business risks from naive use of RFID in tracking, tracing and logistics, in: VDE Verlag GmbH (Eds.): RFID SysTech 2009 - ITG Fachbericht 216, 16-Jun-2009, Berlin, ch. 7.
[38] “Technology Outlook 2020”, DNV, Dec 2013, www.dnv.com/moreondnv/research_innovation/foresight/outlook
[39] Marco D'Angelantonio, John E. Oates, Is Ambient Assisted Living the Panacea for Ageing Population?, IOS Press, Jan 2013, p72