IoTSec - Security in IoT for Smart Grids

Relevance

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”.

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 5 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.

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.

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.

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. 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. A more detailed description is provided on the open project Web IoTSec.no and in Appendix A.

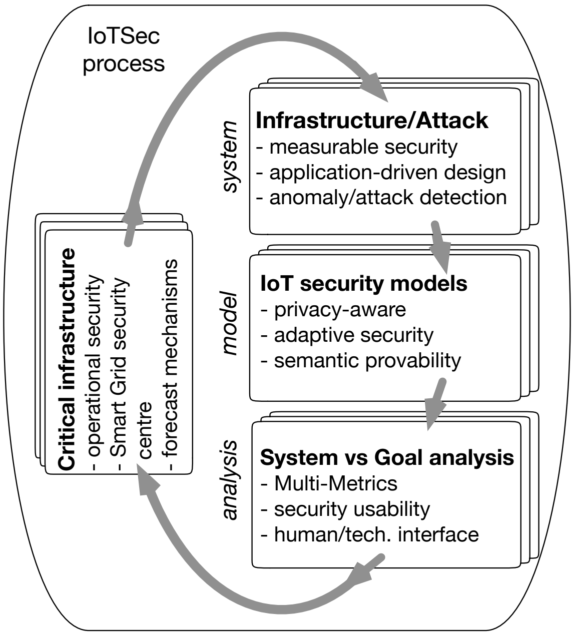

Figure 1: Overall IoTSec approach

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 suitable metrics of system quality and behaviour. 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 $\mathrm{SPD}_{\mathrm{Goal}}$ of (90,80,40) and analyse the system with respect to these goals allows the criticality analysis of components, sub-systems and systems [19]. One outcome of the measurable description is the application-driven **system versus goal analysis,** taking into account security usability and the human/technology interface.

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. Together with the multi-metrics formulations, 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. The envisaged outcome is 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.

Risk management of the interface between humans and technology in an IOT setting includes 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 using an enhanced version of the Conflicting Incentives Risk Analysis (CIRA) method. 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.

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. 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.

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.

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).

The project plan, project management, organisation and cooperation

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 [UiO/Ifi]

- 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 [NR]

- 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 IoTSec ecosystem and industrial applicability
- T4.2 Smart Grid security centre applicability, assessment, simulation and pilots
- T4.3 Gap Analysis of security methods for critical infrastructures

The following chapter contains a detailed WP and task description, including the lead partner (bold), the other partners being involved, and the list of expected results of each task.

WP0 - Project management, Dissemination and Exploitation

- T0.1 Project Management (**UNIK**, NR, Ifi, SIMULA, HiG)

- T0.2 Dissemination (**NCE Smart**, Ifi, UNIK, NR, Fredrikstad Energi, ESmart Systems, EB Nett, HiG)

Tasks in WP0

T0.1 Project management, Collaboration platform, supervision of PhD students
Objective: This task has the overall responsibility for collaboration
The task will

- manage the project
- create and maintain the collaboration platform at http://iotsec.no
- supervise PhD students

Expected results: a collaboration platform supporting up-to-date and online information (M3), the recruitment of 3 PhD students (M9), established the competence profile and collaboration between at least 11 professors/senior researchers (M12), established an Security in IoT track in the COINS Research school (M10)

T0.2 Dissemination, Scientific Papers, workshops, liaisons, industrial take-up
Objective: The main objectives of this task are

- to disseminate the research results on conferences and through papers and journal articles
- to broaden the reach through national and international liaisons
- to involve industry through targeted dissemination
- to pave the way for industrial take-up through the security centre for Smart Grid

Expected results: Scientific research results are disseminated to at least 4 conferences and 2 journals (M12), Research direction of new research topics are established (M6), At least two project proposals have been initiated (M12), At least one business workshop for industrial awareness was organised (M12), Business ecosystem and key players are identified (M8, in collaboration with T4.1), Initial research perspectives have been discussed with industry to establish the Smart Grid Security Centre (M12, in collaboration with T4.2), Research results developed in this project will be presented and transferred to business initiatives (M24), Smart Grid Security Centre serves as meeting point for 5 new research initiatives and new cooperation initiatives (M24), Smart Grid Security Centre will establish international visibility through participation in at least 3 EU events (M12)
Subtasks: 0.2.1 Scientific Dissemination, 0.2.2 Industrial Dissemination, 0.2.3 Liaison

WP1 - Semantic Descriptions

- T1.1 Semantic Descriptions (**Ifi**, UNIK, NR, NCE Smart)
- T1.2 Measurable Security (**UNIK**, NR, Ifi, Movation)

Tasks in WP1

T1.1 Semantic description of infrastructure, attack detection, system view
Objective: This task will create the semantic descriptions for the infrastructure components and the attack surface, and thus establish the semantic model for the IoT System
Expected results: a minimum of 3 papers, including one journal paper (M12-36), the completion of a PhD candidate within the project period (M48), a non-trivial case study (M12)

T1.2 Measurable: security, privacy and dependability, metrics
Objective: This task will establish the Multi-Metrics Model for the Smart Grid use case. The task includes

- the adaptation to the real world infrastructure
- the analysis of the most relevant sub-systems
- application specific goals for security, privacy and dependability

Expected results: System analysis for main sub-systems on current infrastructure (M12), identification of 3-5 use cases, to be further elaborated in T3.1 (M12), Feedback from industry on applicability of system analysis (M12), Extension of the Smart Grid system to include at least 2 new functionalities (M24), Identification of challenges for industrial applicability (M24)

WP2 - Security Models

- T2.1 Privacy-aware models (**SIMULA**, UNIK, NR, NCE Smart, SIMULA)
- T2.2 Adaptive Security (**NR**, Ifi, ESmart Systems)
- T2.3 Semantic Provability (**Ifi**, UNIK, NR)

T2.1 Development of privacy-aware models and measures
Objective: This task will establish privacy-aware models and related measures of privacy. It will also

introduce privacy design patterns for industrial devices and programs. The task will also address security models for business interactions between stakeholders.
Expected results: construction of privacy by Design patterns for IoT applications and the deployment of user-centric privacy technology (M12), cooperation and competition framework among different players in the smart grid (M12), processes integrating technology, business model, security model and privacy requirements (M24)

T2.2 Adopting and enhancing adaptive security for system of systems
Objective: This task will review, extend and establish models for

- adaptive security through predication and advanced behavioural analysis of big-real-data
- real-time security monitoring of the entire grid operations
- prevention, detection and recovery from the failures of security and privacy protections

Expected results: Functional architecture of adaptive security models (M12), Working prototype of adaptive security models (M24), Working prototype of adaptive user interface (M30), Optimised adaptive security models (M48), 8 conference papers (M6-M48) and 5 journal papers (1 paper per year)
Subtasks: T2.2.1 Develop and implement anticipatory adaptive security, T2.2.2 develop adaptive user interface with contextual intelligence, T2.2.3 Optimise adaptive security models

T2.3 Formal technologies for semantic provability
Objective: This task will establish formal technologies for semantic provability
Expected results: a non-trivial case study (M12), a tool for semantic provability (M48), a minimum of 3 papers, including one journal paper (M12-36)

WP3 - System versus Goal Analysis

- T3.1 Multi-Metrics (**UNIK**, NR, NCE Smart, SIMULA, Movation)
- T3.2 Security usability (**HiG**, NR, ESmart Systems, NCE Smart)

T3.1 Multi-metrics applied for application-driven infrastructures
Objective: This task will create the Multi-metrics models for Smart Grids. The Multi-Metrics analysis will be applied for application-driven infrastructures, e.g. reporting, monitoring, and control through the smart grid.
Expected results: a minimum of 3 services being defined, e.g. billing, reporting, alarm (M12), formulation of privacy-preserving modelling and negotiation (M12), a minimum of 5 services being analyses as a comparison between goals and system capabilities (M24), privacy-preserving modell with test case (M24)

T3.2 Security usability in IoT ecosystem
Objective: This task will

- analyse conflicting incentives for IoT, based on the IoTSec ecosystem of T4.1
- establish a platform for multi-shareholder risk analysis
- create impact assessement for stakeholder in the IoTSec ecosystem

Expected results: Functional description of risk platform for IoT multi-operator (M12), A platform for cost effective risk analysis platform based on CIRA/PETweb II results, suitable for IoT critical infrastructure projects (M24), Risk analysis of the system to be used by the infrastructure operators in their decision making (M36),

WP4 - Security Centre

- T4.1 IoTSec ecosystem (**NCE Smart**, UNIK, Ifi, NR, ESmart Systems, HiG, EB Nett, Fredrikstad Energi, SIMULA)
- T4.2 Security Centre assessment (**NCE Smart**, UNIK, Ifi, NR, ESmart Systems, NCE Smart, HiG)
- T4.3 Operational Assessment (**NR**, UNIK, Ifi, ESmart Systems, NCE Smart, HiG)

T4.1 IoTSec ecosystem and industrial applicability
Objective: This task will establish the industrial requirements, analyse the IoTSec ecosystem and ensure industrial applicability.
Expected results: A clearly defined scope of the project in terms of stakeholders, their interests, technological components and their functionality and interconnection (M08), A clarification of what is considered to be outside of the research and industrial applicability (M12), Industrial network enhanced by at least 4 members (M12), Established Industrial workshop and defined industrial shareholder

involvement in the project (in collaboration with T0.2 - M18)
Subtasks: T4.1.1 IoTSec ecosystem, T4.1.2 Industrial network

T4.2 Smart Grid security centre applicability, assessment, simulation and pilots
Objective: This task will perform the detailed assessment of modules applicable for the Smart Grid Security Centre and the pre-industrial pilots
Expected results: Outline of the Smart Grid Security Center is ready including technical design of the visualization platform for security modules and operational plan of the Centre (M12), First Models or Modules are implemented into the visualization platform (M24), Smart Grid Security Centre is operational (M36)

T4.3 Gap Analysis of security methods for critical infrastructures
Objective: This task will perform the Gap Analysis of security methods for critical infrastructures
Expected results: an analysis of IoT ecosystems similar to Smart Grids (M18), establish contacts for applicability in IoT-based critical infrastructures (M24), provide a roadmap of the operational applicability of IoTSec results (M24)

Management roles and responsibilities

The management roles and responsibilities within the project are described in figure Figure. 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), Prof. Olaf Owe (UiO) co-ordinates the research, and Erik Åsberg (eSmart) 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.

The 33 deliverables are described in table 1. Table 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

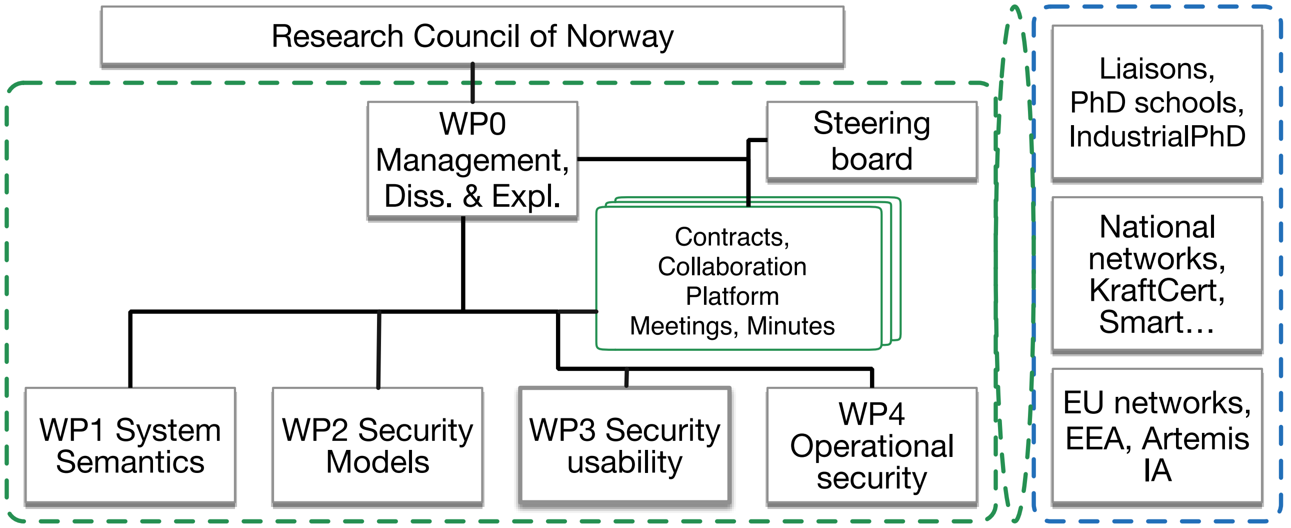
Research Council of Norway
WP0 Management, Diss. & Expl.
Steering board
Contracts, Collaboration Platform Meetings, Minutes
WP1 System Semantics
WP2 Security Models
WP3 Security usability
WP4 Operational security
Liaisons, PhD schools, IndustrialPhD
National networks, KraftCert, Smart…
EU networks, EEA, Artemis IA

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

Wiki[1], while the full technical notes are provided at 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. Table).

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. A detailed overview on key personnel, core competence and contributions of each partner is provided in Appendix B.

Budget

► Budget planning is included in the grant application form.

Table 1: Deliverable descriptions for the first 24 months.

Del. nr	Title	month	partner	editor	release form
D0.1.1	Collaborative Knowledge Platform	M03	UNIK	Josef Noll	Public
D4.1.1	Tech. rep.: Analysis of IoTSec ecosystem	M08	HiG	Einar Snekkenes	Restricted
D0.1.2	Annual Reporting Year 1	M12	UNIK	Josef Noll	Restricted
D0.2.1	Workshop Invitations and Minutes Year 1	M12	NCE Smart	Dieter Hirdes	Public
D0.4	Scientific Paper #1	M12	Ifi	Olaf Owe	Public
D0.5	Scientific Paper #2	M12	UNIK	Seraj Fayyad	Public
D0.6	Scientific Paper #3	M12	SIMULA	Yan Zhang	Public
D0.7	Scientific Paper #4	M12	HiG	Einar Snekkenes	Public
D0.8	Scientific Paper #5	M12	Ifi	Olaf Owe	Public
D0.9	Scientific Paper #6	M12	NR	Habtamu Abie	Public
D1.1.1	Semantic Description of Infrastructure	M12	Ifi	Olaf Owe	Public
D1.2.1	Methods for measurable security (draft)	M12	UNIK	Josef Noll	Public
D2.1.1	Technical Report - Privacy Awareness (draft)	M12	NR	Habtamu Abie	Restricted
D2.1.2	Privacy-preservation framework	M12	SIMULA	Yan Zhang	Public
D2.2.1	Anticipatory adaptive security models (draft)	M12	NR	Habtamu Abie	Restricted
D2.2.3	Event-driven adaptive security (draft)	M12	NR	Habtamu Abie	Public
D3.1.1	Multi-metrics analysis of applications on the smart-grid infrastructure (draft)	M12	UNIK	Josef Noll	Public
D3.2.1	Incentives and Usability for IoT Security (draft)	M12	HiG	Einar Snekkenes	Public
D4.2.1	Outline of security centre (pres. and outline)	M12	NCE Smart	Heidi Tuiskula	Public
D0.1.3	Annual Reporting Year 2	M24	UNIK	Josef Noll	Restricted
D0.10	Scientific Paper #7	M24	Ifi	Olaf Owe	Public
D0.2.2	Workshop Invitations and Minutes Year 2	M24	NCE Smart	Dieter Hirdes	Public
D1.1.2	Semantic Description of Infrastructure (final)	M24	Ifi	Olaf Owe	Public
D1.2.2	Methods for measurable security (final)	M24	UNIK	Josef Noll	Public
D2.1.3	Technical Report - Privacy Awareness (final)	M24	NR	Habtamu Abie	Public
D2.2.2	Enhanced event-driven adaptive security	M24	HiG	Einar Snekkenes	Public
D2.2.4	Anticipatory adaptive security report	M24	NR	Habtamu Abie	Public
D2.3.1	Semantic Provability Framework (draft)	M24	Ifi	Olaf Owe	Public
D3.1.2	Application analysis on the smart-grid infrastructure (draft)	M24	Movation	Seraj Fayyad	Public
D3.2.2	Incentives and Usability for IoT Security (intermediate)	M24	HiG	Einar Snekkenes	Public
D4.2.2	Assessment of security models for Smart Grid	M24	NCE Smart	Heidi Tuiskula	Public
D4.3.1	Pres: Roadmap of security modules	M24	NCE Smart	Heidi Tuiskula	Public

Type to enter text

[1] The collaboration platform is drafted on http://IoTSec.no

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

Key perspectives and compliance with strategic documents

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.

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.

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.

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.

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.

Dissemination and communication of results

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

Additional information specifically requested in the call

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

Attachments:

- **List of References**
- **Appendix A: Extended State-of-the-Art**
- **Appendix B: Background of the involved academic institutions**