ENCS

Agentschap NL
Ministerie van Economische Zaken

CYBER SECURITY:
A FUNDAMENTAL BASIS FOR SMART GRIDS

EINDRAPPORT TOPSECTOREN TKI PROJECT

Authors: Rob van Bekkum, Maarten Hoeve

Date: 29-07-2014

Version: v1.0 Final

Reviewed: Ed Engelschman, Victor van der Stoep

UNIVERSITEIT TWENTE. KEMA DNV ENCS SECURITY MATTERS alliander kpn TNO innovation for life

Table of Contents

1. General Project Information 3
2. Project End-report 4
   2.1. Summary 4
      2.1.1 Monitoring: 4
      2.1.2 Privacy Enhancing Technologies 5
      2.1.3 Testing 5
      2.1.4 Requirements 6
   2.2. Introduction 7
      2.2.1. Monitoring 7
      2.2.2. Privacy Enhancing Technologies (PET) 10
      2.2.3. Testing 12
      2.2.4. Requirements 14
3. Execution of the Project 17
   3.1. Problems Encountered 17
   3.2. Changes in the project against the original project-plan 18
   3.3. Planned versus actual hours, costs and subsidy 18
   3.4. Dissemination 19
      3.4.1 Monitoring 19
      3.4.2. Privacy Enhancing Technologies 19
      3.4.3. Testing 19
      3.4.4. Security requirements: 19
   3.5. Thanks Participants 20

1. General Project Information

The general project information is as follows:

Project number:	TKISG02020
Project title:	Cyber Security: a fundamental basis for Smart Grids
Project-coordinator:	ENCS, European Network for Cyber Security
Project participants:	Alliander, DNV GL, TNO, KPN, Security Matters, University Twente

This project was executed with subsidy from the Dutch Ministry of Ecomic Affairs, for the TKI Topsectoren Smart Grids that is coordinated by Agentschap NL. The project was aimed at the program line virtual infrastructure, sub-line security and privacy. According to the innovation contract Smart Grids one of the two focus areas in this sub-line is Security by Design. This project aimed to make a substantial impact in this area. It also contributed to the sub-line security of the program line Physical Energy Infrastructure and to the program line Social & Institutional Innovation.

2.1. SUMMARY

Smart grids are a crucial to support the use of more sustainable energy sources. More automation in electricity networks will be needed to integrate increasing amounts of decentralized generation, electric vehicles and heat pumps and encourage consumers to actively manage their energy demand.

Unfortunately, more automation also make the electricity grid more vulnerable to cyber threats. The TKI project *"Cyber Security: A Fundamental Basis for Smart Grids"* has worked on improving the cyber security of smart grids in four areas, described below - starting with Monitoring.

2.1.1 MONITORING:

For a DSO it is vital to have situational awareness of the security status of their smart grid network, and DSOs should continuously monitor the security status of Smart Grids

Objectives

1. Find efficient strategies for placing sensors.
2. Develop methods to detect attacks in network traffic.
3. Develop a proof-of-concept monitoring solution based on currently available technology.

Results

- A strategy to place intrusion detection sensors in substation automation systems was developed. Placing sensors to monitor inside the control center will catch most intrusions, but some intrusions can only be detected by sensors inside substations.
- Algorithms were developed to detect man-in-the-middle-attacks that abuse network management protocols (ARP, ICMP, DHCP).
- Algorithms were developed to detect intrusions in encrypted traffic between control centers and substations. The algorithms can detect abnormal sequences of network packets in a periodic stream, or abnormal amounts of traffic. Tests on real traffic show they will even detect subtle attacks while raising few false alarms.
- A proof-of-concept monitoring solution was constructed in a substation automation test bed. It was tested on fifteen realistic use cases defined by a grid operator. All cases could be detected with the solution.

2.1.2 PRIVACY ENHANCING TECHNOLOGIES

Another area researched was Privacy Enhancing Technologies (PET). When reading out Smart Meters, DSOs want to both preserve the privacy of consumers, and get the information they need for advanced Smart Grid services such as demand side management. New protocols are needed for the communication between Smart Meters and the grid operator to ensure the privacy of consumers.

Objectives

1. Test in a realistic test bed the robustness and scalability of the privacy-preserving meter reading protocol.
2. Identify additional use cases in smart grids that require privacy-preserving-technologies and develop cryptographic protocols for these cases.

Results

- The protocol performed well in a realistic test set up with 100 meters. The encryption caused no significant delays in reading the meters, and could easily be integrated into the DLMS/COSEM communication protocol. The protocol was robust under meters or communication lines malfunctioning.
- Six new use cases were identified: grid management, fraud and loss detection, e-mobility, benchmarking, retailer and consumer engagement, and distributed energy resources. The existing protocol covers most cases. For the other cases protocols were found in the literature.

2.1.3 TESTING

DSOs need a way to test that the whole system, from the Smart meters in people's homes, to the sensors and controllers in the field, and finally their own control rooms is resilient to cyber attacks.

Objectives

1. Develop a security testing framework for smart grid.
2. Develop a method for penetration testing.
3. Develop tools for vulnerability discovery.
4. Develop infrastructure and procedures to connect test labs.

Results

- A testing framework was developed that describes when to apply which tests and how to deal with critical but fragile systems.
- A systematic penetration testing method was developed for smart grid systems.
- Fuzzers were created to find vulnerabilities in the implementations of the IEC 60870-5-104 and 61850 communication protocols, used in substation automation.
- Several experimental tests were run in which labs at different locations were connected. The lessons learned were written down in a report.

2.1.4 REQUIREMENTS

Security requirements are the foundation on which security is built. A balanced set of security requirements is crucial both in the design-stage and when assessing and/or testing the security of existing systems.

Objectives

1. Create a set of workable cyber security requirements for grid operators.
2. Gather best practices in improving smart grid security.

Results

- An overview of vulnerabilities and threats to substation automation systems was made.
- A strategy to specify smart grid security requirements was developed. The strategy is based on jointly developing the use cases, requirements, and architecture, so that feedback on the feasibility of choices can be used.
- Best practices on smart grid security were gathered from experts in the project and the literature.

For more information about these research activities please send an e-mail to info@encs.eu.

2.2. INTRODUCTION

To support more sustainable energy sources, such as solar or wind power, electricity networks will need to be more automated. To integrate increasing amounts of decentralized generation, electric vehicles and heat pumps and encourage consumers to actively manage their energy demand, grid operators need to be able to better and monitor the electricity grid.

Unfortunately, more automation will make the grid more vulnerable to cyber attacks. Every controller or network component added to the grid can be abused by attackers. Information systems are being connected to each other and to the internet, to make it easier to share data. But this also makes it easier for attackers to reach critical systems that were isolated before.

A comprehensive approach to improving the cyber security of the grid is needed. Now that the way the grid works is being redesigned, future-proof security mechanisms and architectures should be selected based on clearly defined requirements and thorough testing. As smart grid components have a long lifetime in the field, and replacement is economically almost infeasible, it is vital to adopt security-by-design principles now before mass deployment happens.

The TKI innovation contract Smart Grid recognized the urgent need for better cyber security as a prerequisite for a reliable electricity grid, and made security by design one of the focus areas of 2012. To work on these areas, ENCS gathered in the project *"Cyber Security: A Fundamental Basis for Smart Grids"* strong parties which could make a high quality contribution. The project brought together academic research with the University of Twente and a DSO - Alliander. Both TNO and KPN brought specialist with years of experience in ICT security to the consortium. DNV GL brought extensive experience in testing. Security Matters, an enterprise focused on network security, brought specialized monitoring technology. Together these partners worked on improving cyber security in four workstreams: monitoring, privacy-enhancing technologies, testing, and requirements. These workstreams are described below.

2.2.1. MONITORING

Not all security incidents can be prevented by designing and implementing smart grids well. There is always a risk that attackers get past the defensive measures. For this reason a grid operator should monitor what is going on in its data networks. It needs to know if systems are configured according to security policy, and if there are systems in it that are vulnerable to known attacks. Even more it needs to know about security incidents and intrusions.

Better tools are needed to monitor the most critical parts of the data networks, the Supervisory Control And Data Acquisition (SCADA) networks that oversee and control electrical substations. Commercially available tools used to monitor ICT networks only cover a part of such networks. They often can only detect known attacks, of which there are still few. Research has up to now been restricted by the limited availability of data from operational networks.

Objectives

The research in the monitoring workstream aimed to contribute to a cost-effective security monitoring in smart grids in three ways:

1. *Find efficient strategies for placing sensors.* The layout of smart grid data networks is different from ICT networks. Devices are deployed in electrical substations or in peoples homes. Placing sensors to get the data needed to detect most intrusions, could become expensive. Hence, a strategy to efficiently place security monitoring sensors is needed.
2. *Develop methods to detect attacks in network traffic.* Network intrusion detection systems developed for ICT networks will miss many attacks in smart grid network traffic. Both the attacks and the normal traffic are different in smart grids. Hence, new detection techniques are needed. In particular, researched focused on methods to detect attacks in encrypted traffic, without sharing the encryption key with the sensor.
3. *Develop a proof-of-concept monitoring solution based on currently available technology*. A lot of tools are available for ICT systems, and some special-purpose tools are now becoming available for SCADA systems. No single existing sensor exists can however detect and prevent all of the identified threats. Multiple technologies must be combined to create an effective security monitoring solution.

At the beginning of the project the choice was made to focus for all three objectives on SCADA systems that oversee and control electrical substations. These systems are probably the most critical system grid operators are using now. A lot of work on smart grids is going in to improving and extending these systems.

Approach

To find sensor placement strategies the approach was to gather information about SCADA architectures from experts at Alliander and come up with a list of data sources that sensors could monitor. A list of attack scenarios was compiled from the literature and conversations with SCADA security experts, and an analysis was made of which attacks would be visible in which data sources. Based on this analysis a sensor placement strategy was developed.

The development of methods to detect attacks in non-encrypted traffic focused on man-in-the-middle attacks. Such attacks are a serious threat in SCADA systems, because the communication protocols are unauthenticated. They involve the attacker placing himself in the communication stream between the control center and devices in the field. Attackers can do this by abusing network management protocols, such as the Address Resolution Protocol (ARP). An algorithm was developed to detect unusual amount of messages in network management protocols that could be an indication of a man-in-the-middle-attack.

To develop methods to detect attacks in encrypted traffic two approaches were investigated. The first approach is based on the periodicity of SCADA traffic: SCADA systems often poll values in a repeating cycle. Hence, the sizes of network packets and their timing are largely periodic. Packets that do not fit into this periodic pattern can be detected. They do not if in the normal traffic, and could be signs of an attack. This approach was tested with data from an emulated SCADA system in the ENCS lab.

The second approach looks at the volume of traffic. Because of the periodicity, the volume of traffic is expected to be close to constant. This assumption was checked on traffic collected from an operational SCADA system. A model was developed for the deviations from the average

volume seen in such traffic. A system was developed that can detect abnormal traffic volumes, which could be caused by attacks.

For the proof-of-concept intrusion detection system for SCADA systems based on currently available technologies first a threat analysis was made, describing the sources of threats, vulnerabilities, and the resulting attack scenarios. Next, monitoring technologies were examined that can detect the identified attacks. A threat-technology matrix was developed that shows the capabilities of each monitoring technologies against the identified threat scenarios. Using the matrix a mix of monitoring technologies was chosen that can detect all anticipated attack scenarios.

The selected mix of technologies was set up in the ENCS test-bed. To evaluate the proof-of-concept fifteen realistic attack scenarios, chosen together with Alliander, were worked out in detail. Tests were conducted to see if and how these scenarios were detected.

Results

The work on placing sensors in substation automation SCADA systems showed that most types of attacks can be detected by placing sensors centrally, at the control center. Some types of attacks can however only be seen by sensors inside the substation. Due to the highly critical nature of some substations it may be justified to place sensors there in the future. (See deliverable 1.)

The work on detecting attacks in unencrypted network traffic led to algorithms to detect man-in-the-middle attacks in the ARP, DHCP, and ICMP protocols. These will be further developed and evaluated in future research (See deliverable 3, 10.).

The work on encrypted network traffic has led to prototypes of several algorithms. These were evaluated on network traffic captured in an operational SCADA network. The two most successful algorithms were written down in conference papers. (See deliverables 2, 7, 8, 9.)

The proof-of-concept detection solution for combining multiple intrusion detection sensors was built in the ENCS lab. It successfully detected all 15 use cases defined together with Alliander. Demonstrations of these use cases were given to the project team and other interested parties. (See deliverables 4, 5.)

Deliverables – Work-stream Monitoring
Reports
1. Placement of Intrusion Detection Sensors in Substation Automation (ENCS, SM)
2. Intrusion Detection on Encrypted Data for Smart Grids (ENCS) (Incl. Annex A: Experiment on Modbus data)
3. Monitoring non-encrypted traffic in ICS networks (SM)
4. Threats Overview (ENCS, SM)
5. Network Security Monitoring & Use Cases (ENCS, SM, Alliander)
6. Security monitoring in substation automation (TNO)
Scientific papers:
7. Detecting Intrusions in Encrypted Control Traffic (ENCS)
8. Volume-based Intrusion Detection in SCADA Systems (ENCS)
Software prototypes:
9. Tool to monitor encrypted traffic (ENCS)
10. Tool to monitor non-encrypted traffic (SM)
Other:
11. Hard drive with recorded network traffic data (Alliander)
12. Monitoring test environment (POC) (KPN, ENCS, SM)
13. SOC environment (KPN)

Deliverables Workstream Monitoring

2.2.2. PRIVACY ENHANCING TECHNOLOGIES (PET)

Many regulations protect the privacy of consumers, such as the Dutch Data Protection Act (NL WBP). When reading out Smart Meters, grid operators want to both preserve the privacy of consumers, and get the information they need for advanced Smart Grid services such as demand side management.

The PET workstream continued work started in an academic conference paper published in 2011 at the Privacy Enhancing Technologies Symposium. In that paper protocols were developed that would allow distribution grid operators to read out the aggregate power use of a group of homes, without disclosing privacy sensitive information about individual homes.

A key step to getting these protocols accepted into a real system is to show (in a realistic setting, not only on paper) that they scale well, are robust, and integrate with existing systems. Due to the limited computational resources on meters and the low bandwidth in the network between the meter and head-end, grid operators are wary of using encryption in smart metering systems. They will only consider it if it has been convincingly shown that it does not impede the normal functionality.

A small-scale implementation test on 4 meters was carried out with Elster in 2012 to test the feasibility of the PET protocol on actual smart meters. Based on the success of the small-scale implementation, in the PET workstream ENCS, Alliander, and Elster collaborated to conduct more in-depth integration and scalability tests on a set of 100 smart meters.

Objectives

The PET workstream has two objectives:

1. *Test in a realistic test bed the robustness and scalability of the privacy-preserving meter reading protocol.* The tests aimed to identify and resolve management, robustness, and performance issues and to minimize the effort to migrate to such a solution.
2. *Identify additional use cases in smart grids that require privacy-preserving-technologies and develop cryptographic protocols for these cases.* Example use cases would be electric vehicle charging or fraud detection using smart meters.

Approach

To demonstrate how easy the PET protocol would be to integrate, it was implemented with minimal changes to the DLMS/COSEM protocol, the most common communication protocol for smart meters in Europe. The PET protocol was implemented in the smart meter firmware by the meter manufacturer.

Systematic tests were conducted to determine the effect of the protocol on performance and robustness. A test bed with 100 smart meters was build in the ENCS test lab to conduct tests. The meters were connected to head-end software that could read them out using a serial protocol.

The performance tests considered different operations, such as creating the encryption keys required and sending the encrypted values. Performance was measured through CPU and memory usage, and the time the operations took. The effect of the size of the aggregation groups was also measured.

Robustness was tested by simulating communication errors and power failures. The goal was to test if the failure of some meters did not affect reading from other meters, and if the meter reading could recover after some failed readings.

Besides testing the already developed protocol, ENCS also worked with Alliander to identify existing and potential use cases for privacy enhancing technologies, and to investigate alternative privacy approaches that are business-enabling. Interviews were held with smart grid experts from Alliander to understand their needs and requirements.

Results

The results of integration and scalability tests on 100 meters showed that the PET protocol adds no significant extra costs and easily fits within the DLMS/COSEM protocol. Detailed results from the tests and the use case analysis were presented at the SEGS Workshop on November 8 in Berlin. As such this project was the first to bring a privacy enhancing technology from a prototype to a scalable and deployable solution and it showed how to implement “Privacy by Design” in a real setting. (See deliverables 1 to 11 and deliverable 14.)

ENCS is currently working to get the PET protocol standardize as an annex to the DLMS/COSEM protocol standard. Efforts are also under way to include it in national smart meter privacy and security requirements.

Six new use cases were identified together with Alliander: grid management, fraud and loss detection, e-mobility, benchmarking, retailer and consumer engagement, and distributed energy resources. The PET protocol supports a large majority of these use cases. For use cases not covered by the existing approach, other protocols were found in the literature. (See deliverables 12 and 13.)

Deliverables - workstream PET
PET Test plans:
1. ENCS PET Master Test Plan (ENCS)
2. ENCS PET Component Phase Test Plan (ENCS)
3. ENCS PET System Phase Test Plan (ENCS)
4. ENCS PET System Setup (ENCS)
5. ENCS PET Requirements Traceability Matrix (ENCS)
Test results:
6. ENCS PET Component Results (ENCS)
7. ENCS PET System Results (ENCS)
8. ENCS PET Test Closure Report (ENCS)
9. Enhancements (ENCS)
10. Scalability and Integration (ENCS)
11. Log Files - PET Results: 452 MB. Available on request. (ENCS)
Reports:
12. PET Use Cases (ENCS, Alliander)
13. Additional Privacy-Preserving Protocols (ENCS)
Scientific papers:
14. Implementation of Privacy-Friendly Aggregation for the Smart Grid (ENCS)

Deliverables Workstream PET

2.2.3. TESTING

Security testing is a crucial step in improving the cyber security of smart grids. Many components and systems are still installed without being tested for security. Operational systems are rarely tested. Grid operators fear that testing them will disrupt their operation. Consequently, there are many vulnerabilities in smart grid systems. Only systematic testing can improve this situation.

Objectives

The objective of the testing workstream are:

1. *Develop a security testing framework for smart grid.* The framework should specify which test methods should be applied to which components and systems and when. It should also describe the steps in performing test to produce repeatable results. Finally it should describe how to deal with testing critical but fragile systems.
2. *Develop a method for penetration testing.* In penetration testing the tester assumes the role of an attacker. He tries to use the same tools and methods to compromise the tested system. This approach is very powerful. There is a risk however that the results depend too much on the skills and approach of the tester. A systematic method is needed to ensure repeatable results.
3. *Develop tools for vulnerability discovery.* A lot of tools to find vulnerabilities have already been developed for ICT systems. Some tools are also available for industrial control

systems. Some communication protocols are however specific to smart grids. Tools are needed to find vulnerabilities in the application of such protocols.

4. *Develop infrastructure and procedures to connect test labs.* Skills and expertise for smart grid security testing are spread thin over many labs. People with specific knowledge are often hard to find locally. Hence, tests will often need to be performed by testers from external labs, possibly located far away. Also, testing critical systems often involves rebuilding the system in a test bed. The software and equipment needed for this are also often located in many different test beds. Some equipment may be even installed in the field, either installed but not yet operational or as part of a test environment (e.g. the Alliander LiveLab). For both reasons there is a need to connect test labs at different location to create a virtual test lab.

Approach

To develop the testing framework, first an overview was made of existing test technologies. Both technologies for smart grids and general methods from the ICT domain were considered. The ICT technologies were evaluated for their applicability in smart grids. The results from the review of existing technologies and the standards reviewed in the requirements work-package were combined into a general cyber test framework.

The framework was then evaluated both in pilot tests conducted in this project and in commercial testing projects performed by ENCS. Base on these test, the testing steps and reporting formats were further improved.

The penetration testing framework was developed by KEMA based on their testing experience, and the best practices in penetration ICT systems and industrial control systems.

For the vulnerability discovery tools, fuzzers for the IEC 60870-5-104 and IEC 61850 communication protocols were developed. These protocols are commonly used in SCADA systems used to monitor electrical substations. These tools were evaluated in pilot tests on embedded devices used in substations.

To gain experience with connecting test labs, experimental tests with the partners were conducted during this project. Different technical solutions to connect labs, e.g. via virtual private networks (VPNs), were tried. Procedures to work together were set up and refined. The experiences were written down in a report based on interviews with the people involved in these experimental tests.

Results

The review of the test methods resulted in a testing framework that described which tests are applicable in which situations. (Deliverable 1.) The test framework was used in two pilot tests (deliverables 6 and 7). This framework is currently being used as the basis for tests conducted in the ENCS test lab. It is being further developed in projects at ENCS.

A penetration test method was developed and documented (deliverable 2).

Mutation based fuzzers were built for the IEC 104 and 61850 protocols. (Deliverable 3 and 5). Both were applied to devices in the ENCS test lab. They were able to find several vulnerabilities that would not have been found with commercially available testing tools. (See deliverable 8.)

A lot of experienced was gained in connecting test labs and collaborating with multiple partners in a test. The lessons learned were written down in a report (deliverable 4). They are being applied in commercial testing projects and will be applied in FP7 research projects (SEGRID, AMADEOS).

Deliverables - workstream Testing
Reports
1. Framework for End-to-End Security Testing in Smart Grids (ENCS, Alliander)
2. Test methodology for vulnerability assessment and penetration test (KEMA)
3. Report on security testing tools (UT)
4. Lessons Learned on Virtual Test Labs (ENCS, TNO, UT)
Software prototypes:
5. Fuzzer & Client development (104 & 61850) (UT)
Pilot test reports:
6. Smart RTU Robustness Test (ENCS)
7. Smart Device Robustness Test (ENCS)
8. Report on vulnerability assessment (UT)

Deliverables Workstream Testing

2.2.4. REQUIREMENTS

Security requirements are the foundation on which security is built. They may be derived from an investigation of stakeholder expectations, regulatory constraints, analysis of the threat landscape and impact assessments. A balanced set of security requirements is crucial both in the design-stage (to allow informed design decisions about which security measures to adopt and which residual risks to accept) and when assessing or testing the security of existing systems. The level of digitalization in smart grids is new to the Energy sector. Suppliers need to develop new components based on requirements derived by grid operators, including the security requirements.

Many high level guidelines are available from for example government bodies, but the advice they give is at too high a level for grid operators to use them. More detailed requirements are needed to support grid operators in their decisions to purchase Smart Grid equipment or organize their security processes.

Objectives

The objectives for this workstream are:

1. *Create a set of workable cyber security requirements for grid operators*. The requirements should be based on an analysis of the security risks in smart grids. As no good threat analysis is available, this should be produced.
2. *Gather best practices in improving smart grid security*. Not all advice to grid operators to improve security can be formalized in requirements. Sometimes detailed technical

advice is only applicable in some situations. Sometimes new technologies to improve security are in development but still to immature to include in the requirements. Advice of this type is recorded as best practices.

Approach

This work stream started with an analysis of the technical reference architecture for smart grids prepared under Mandate 490. This architecture was combined with the architecture used by the IEC technical committee 57, which represents the functional information data flows between many important smart grid domains main domains and integrate many systems and subsystem architectures.

As the approach was to choose requirements based on an risk analysis, an overview of risk analysis methodologies for the smart grid infrastructure was made.

Following this the common threats and vulnerabilities of the smart grid infrastructure were determined. Systematically the attacks on assets that are within scope of this project were gathered and listed, including the identified common vulnerabilities in these assets. The threats were structured according to the different domains identified in the reference architecture. The overview of vulnerabilities common in smart grid systems include both vulnerabilities inherent to the nature of industrial control systems, and vulnerabilities that might be easily avoidable but are still frequently encountered in today's smart grid implementations.

A review of the existing security standards was carried out. In recent years many new standards relevant to smart grids were proposed. The project analyzed these existing security standards as well as studies from working groups and competence centers like CEN/ CENELEC / ETSI , ENISA, DKE, IEC Strategic Group 3, ITU-T Smart Grid Focus Group, NIST, JISC Japanese Industrial Standards Committee, SGCC, The State Grid Corporation of China

Originally the plan was to select from these standards a workable set of requirements to mitigate the risks found in the risk analysis. The risk analysis was however not available on time. Also, the reference architecture contained insufficient information on smart grid use cases to develop requirements in the level of detailed originally envisioned. Therefore, the choice was made to change the approach and pick a more modest objective.

A strategy was developed to develop smart grid requirements based on use cases. The strategy was designed to address the difficulties found in the smart grid domain. It was based on the experiences with smart meter requirements.

Best practices were gathered from a wide collection of sources. Many were based on the experience of the experts participating in the project. Others were based for instance on the recommendations published by the US government through their ICS-CERT.

Results

An report on threats and vulnerabilities was compiled. It gives an overview of well known issues with SCADA systems. (Deliverable 3.)

A method to develop security requirements for the smart grid was developed. The main feature is that the uses cases, requirements, and architecture are developed together. In this way it is possible to adjust use cases or requirements if implementing security becomes too costly. (Deliverable 1.)

Best practices were developed in four areas: developing secure components, designing a secure smart grid architecture, organizational security, and security monitoring. (Deliverable 2.)

Deliverables - workstream Requirements
Reports:
1. Security Requirements for the Smart Grids Infrastructure (ENCS)
2. Best Practices on Security Measures for the Smart Grids Infrastructure (ENCS)
3. Smart Grid Threats and Vulnerabilities (TNO)
4. Reference Architecture (Alliander, TNO)
5. Framework to support cyber security risk analysis on smart grids infrastructure, services and components (KEMA)
Summaries:
6. Security Standards for Smart Grids (Alliander, ENCS)
7. Security Assessment Methodology for the Smart Grids Infrastructure (Alliander, ENCS)

Deliverables Workstream Requirements

3.1. PROBLEMS ENCOUNTERED

Problems were encountered in three areas:

1. *Alignment of expectations between the partners.* Taking one look at the consortium, it is obvious that the partners have very different background and objectives. All are interested in smart grid security. But they differ in the role they see for themselves in achieving it, as well as a different motivation (including vendors, research, and end-user).

   During the project the partners found it difficult to formulate a common goal they could all get behind. They did not manage to work out the objectives and deliverables so that all partners could benefit from them. While all partners (as organisations) have participated in similar research activities, it seems that the expectations on the outcome of the Topsectoren program where misaligned from the start, and difficult to align during the running project.

   Consequently, many partners chose to work more independently than they should have. Many deliverables where following too much a single partners interest rather than supporting the overall project storyline, and project results were not always promptly shared.

2. *Timely delivery of results.* The project proposal defined deadlines for deliverables and milestones spread over the year. Unfortunately many of these intermediate deadlines were missed. Because of this, it was difficult to build on previous results. For instance, in the requirements workstream, the requirements could not be chosen based on the threat analysis.

   The project manager felt he did not have sufficient authority to enforce deadlines. Intermediate reviews by externals would have helped to put more pressure on timely delivery.

3. *Quality control.* All participants were very enthusiastic about giving input on documents. Only a small group however felt responsible for the quality of the final deliverables. Having a better quality control process could have helped to distribute the responsibilities more evenly. In particular, setting clear quality criteria for deliverables and agreeing on a review process in advance would have helped. Quality control was also affected by late deliveries, leaving insufficient time for feedback loops (this was one of the reasons why the project asked for an extension).

3.2. CHANGES IN THE PROJECT AGAINST THE ORIGINAL PROJECT-PLAN

In 2012 the original project proposal was submitted to Agentschap-NL, the organization responsible for the Dutch subsidy tender called TKI Topsectoren Smart Grids. The main change against this original project plan is about the end-date. We requested Agentschap.NL to move the end-date form 1-2-2014 to 1-5-2014 and this request was approved by Agentschap.NL

Original start-date	Original end-date	New end-date
1-1-2013	1-2-2014	1-5-2014

Table with dates project

3.3. PLANNED VERSUS ACTUAL HOURS, COSTS AND SUBSIDY

This paragraph provides the overview of the planned hours, planned costs and planned subsidy per participant versus the actual hours, actual costs and subsidy per participant.

		Proposal			Actual			Delta		
	Participant	**Planned costs**	**Planned hours**	**Planned subsidy**	**Actual costs**	**Actual hours**	**Actual subsidy**	**Actual - Planned costs**	**Actual - Planned hours**	**Actual - Planned subsidy**
P1	ENCS	€ 239.040	3984	€ 167.548	€ 267.495	4429	€ 167.548	€ 28.455	445	€ 0
P2	TNO	€ 218.720	1544	€ 144.003	€ 214.627	1497	€ 143.443	-€ 4.093	-48	-€ 560
P3	Alliander	€ 262.715	3284	€ 122.499	€ 168.300	2805	€ 104.631	-€ 94.415	-479	-€ 17.868
P4	KPN	€ 144.000	2400	€ 72.240	€ 116.520	1942	€ 58.454	-€ 27.480	-458	-€ 13.786
P5	UTwente	€ 93.765	960	€ 60.947	€ 102.093	889	€ 56.440	€ 8.328	-71	-€ 4.508
P6	Security Matters	€ 112.800	1880	€ 84.288	€ 112.800	1880	€ 84.288	€ 0	0	€ 0
P7	DNV KEMA	€ 14.400	240	€ 11.520	€ 14.400	240	€ 11.520	€ 0	0	€ 0
	TOTAAL:	€ 1.085.440	14292	€ 663.045	€ 996.235	13682	€ 626.324		-610	

Table with the planned costs, hours, and subsidy per participant versus the actual costs, hours and subsidy.

3.4. DISSEMINATION

For each of the four workstreams the dissemination is described in this section.

3.4.1 MONITORING

The report on sensor placement will be distributed to ENCS' members through the trusted platform. The problem of placing sensors in SCADA systems proved to be not challenging enough to lead to scientific publications. Hence, work focused more on monitoring encrypted data. The results on monitoring encrypted data were written down in two scientific papers. One has been published in the SEGS 2013 workshop attached to ACM CCS. The other paper has been submitted to a conference.

The outcomes of the proof-of-concept were written down in two reports, that are being distributed to ENCS's members and other interested parties. To promote the reports, a short summary will be distributed to ENCS's contacts. Demonstrations of the proof-of-concept were given to interested stakeholders in the project, and to external parties such as Rijkswaterstaat.

3.4.2. PRIVACY ENHANCING TECHNOLOGIES

The test results from the PET workstream were published in a scientific paper presented at the SEGS 2013 workshop. The test reports themselves have been shared with interested parties within Alliander. Work is currently ongoing to get the protocol standardized as an annex of the DLMS/COSEM communication standard for smart meters. This standard is the most widely used standard of its type in Europe. If the protocol gets accepted, it will enable wide employment. Up to now the user group that governs the standard has reacted positively to the proposed annex.

3.4.3. TESTING

The testing framework is the basis of all commercial test that are performed in the ENCS test labs. ENCS is advising several gird operators on how to set up a testing program for smart meters and substation automation equipment. The testing framework and the review of existing testing methods are the basis for these discussions.

3.4.4. SECURITY REQUIREMENTS:

Although the strategy developed is not applied directly, the knowledge acquired is actively used by ENCS and partners in developing smart grid security requirements. ENCS has been contracted to set up smart meter security requirements for Austria and in Portugal (with TNO). Work will start soon to developed substation automation security requirements. The best practices are shared to ENCS's Advanced Cyber Security Course (ACSC). The ACSC teaches employees of asset owners about control systems security. More than 150 people have already attended it. It has been substantially updated based on the outcomes of this project, and in particular the best practices.

3.5. THANKS PARTICIPANTS

On this project specialists worked together from Alliander, KPN, TNO, DNV GL, Security Matters, University Twente and ENCS:

- ENCS: Klaus Kursawe, Maarten Hoeve, Benessa Defend, Rafal Leszczyna, Andres Perez Garcia, Fred Streefland, Rafael Barbosa, Victor van der Stoep, Christiane Peters, Hamid Rahmouni
- TNO: Bert Jan te Paske, Hiddo Hut, Johanneke Siljee, Gerben Broenink, Harm Schotanus, Peter Heskes, Wendy Ellens, Erik Meeuwissen, Daniel Worm, Thomas Attema, Piotr Zuraniewski
- Alliander: Sander Jansen, Johan Rambi, Frans Campfens, Martijn van Braak, Martijn Kamerling, Eric van Aken, Berrie Staring, Ron Sandwijk , Wilfred Smith, Raymond Hallie, Rob van Bekkum
- University Twente: Emmanuele Zambon, Sandro Etalle
- Security Matters: Christina Hoefer, Chris Schade, Damiano Bolzoni
- DNV GL: Robin Massink, Hans Baars
- KPN: Pascal de Koning, Marco Leenen, Humphrey James

On behalf of ENCS we would like to thank all these people for the pleasant collaboration during this project.