Project:

Smart Metering Cyber Security

An analysis of cyber security in the smart metering of electricity consumption in Finland

By the end of year 2013, while many European countries are only agreeing on the technical standards and cyber security practices, in Finland the settlement of over 80% of electricity consumers must be based on real, hourly interval-metered consumption. Consequently the smart metering penetration is reaching 100% of the consumption sites. Based on this situation in the field, an analysis was committed among the AMM system stakeholders, to clarify the cyber security position in the emergence of full-scale smart metering and to create a roadmap for its further development.

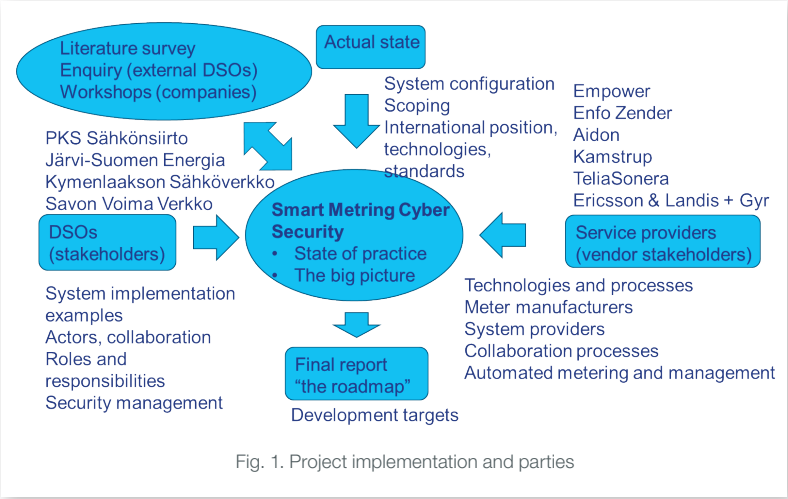

Fig. 1. Project implementation and parties

Project

The project, Smart Metering Cyber Security, was run by VTT during 2013 and actively supported by experts from the participating companies. The starting point was that in 2009, the Council of State decreed on rolling out smart metering, and now, consequently, the coverage is reaching 100% of consumption sites. No smart metering specific detailed cyber security requirements were given, but the common security and privacy protection acts apply. The goal of this project was to analyse the cyber security of smart metering and to provide the following outcome:

- The big picture of cyber risks in smart metering
- Analysis of the risks in the context of the Distribution System Operators (DSOs)
- Development of a target proposal, a roadmap with company-specific objectives for the project stakeholders.

Approach

The project scope was smart metering (or AMI Advanced Metering Infrastructure) in Finland. The cyber security analysis focused on a threat and vulnerability analysis, and the driving method of work was organised workshops with the project parties. The project parties and the viewpoints they brought into discussion are presented in Fig. 1. A synthesis of the results was made, and analysed in a joint closing workshop, to estimate the sizes of the risks. Different types of development targets were listed on the basis of the analysis work.

Smart metering in Finland

The Finnish smart-metering systems are run as business networks by DSOs, as depicted in the logical reference model of the smart-metering system in Fig. 2. The DSO is legally responsible for providing customer usage data, which is managed in the subsequent refining steps by the DSO or the providers of the energy services. The data, initiating in the smart meter, is first transferred via a mobile operator's network into the AMI Headend system, and then on into other information systems. The data is processed, stored, refined, combined with other data – like customer and invoicing data – and eventually delivered to the given market participants. The cyber security challenge originates in the variety of stakeholders, roles, and interfaces. The security management and requirement implementation practices vary among the parties, hence security in collaboration is hard to manage, and if one party

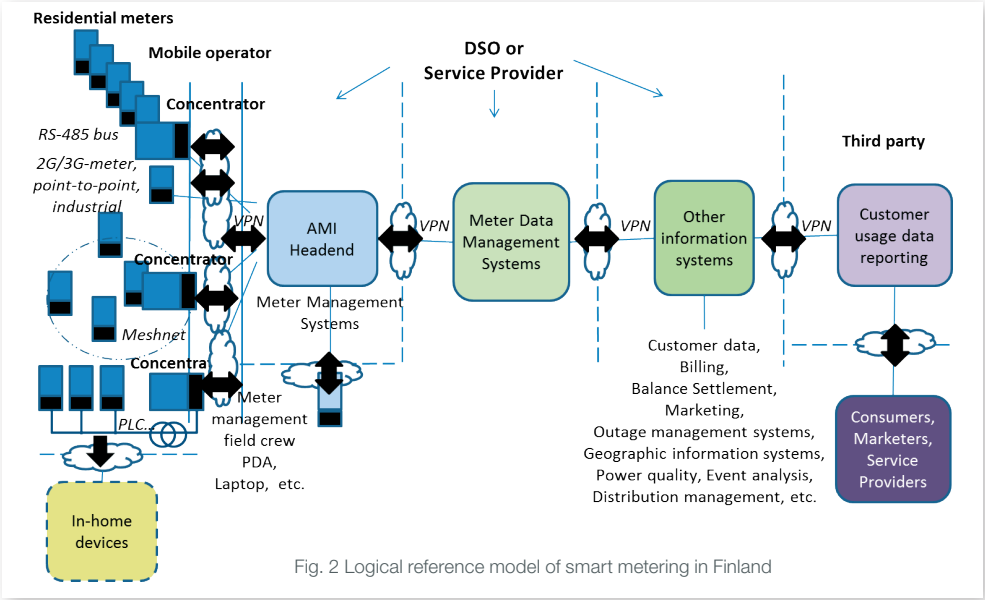

Fig. 2 Logical reference model of smart metering in Finland

fails, all have to bear the consequences. The interfaces are also challenging at the technical level, with a variety of interfaces, proprietary communication protocols and several versions complicating security analysis and remedies.

Based on this analysis, the critical smart-metering functions are as follows:

Function	***Related threats***
Public web server providing customer consumption data	DDOS attack (DMZ and beyond) Customer data exposure
Update over the air	Malfunction en masse
Remote management functions	Erroneous remote switching off and on, individually or en masse
Local meter administration and communication	Preventing meter communication or operation through tampering.

Recommendations for development targets

Based on the project analysis, recommendations for cyber security improvement are given as follows:

- Cyber security awareness should be raised in subcontracting, especially in cases of nested development outsourcing cross the borders.
- Consumption data management and storage must be asserted to be secure, especially in relation to device installation and maintenance operations in the field, and automated customer data reporting services on the Internet. Customer service representatives must be aware of the security and privacy constraints.
- Widely accepted and independently well analysed and tested cyber security standards must be utilised in system development (rather than dedicated security solutions).
- The security of customer data communication and user/device authentication protocols must be asserted.
- The company networks and systems must be divided into appropriately separate security zones: such as zones for communication, critical AMM, data management, data provision, grid management, and critical grid automation.
- Set up intrusion detection systems (IDS) at relevant points in the company networks.
- Carefully secure all software updates to the meters and smart-metering systems.
- Develop measures to prevent insider attacks, limit their impact, and prepare to deal with them.
- Secure remote switching and load management operations against accidental or malicious mass operations, including ciphering the messaging, authentication of the parties, and sanity-checking the command sequences.
- Secure the energy market information interchange with third parties, including ciphering the communications and providing the data with a demilitarised zone separated, with firewalls, from the internal networks.
- Provide common cyber security guidelines – instructions, requirements and recommendations – to support system development and new system procurement.
- Exploit auditing and certification in the projects, using external services as needed.
- Create and join business networks in cyber security management, to jointly and continuously monitor the development of threats and countermeasures.
- Prepare for breaches with plans for communications, as well as loss limiting and corrective actions.
- Secure operations to the new standards by continuous cyber security development.

Conclusions

In the project analysis, no serious vulnerabilities or major problems in cyber security arose; targets for development are listed above. The project's participating organisations embody a significant part of the national energy market technology developers. The parties were not aware of any attacks targeted at smart metering comparable with the Finnish set up. But then again, smart metering is only now gaining momentum in Finland and internationally. Hence, malicious interest in smart metering and related information systems is likely to increase.

Contacts

Pekka Savolainen tel. +358 20 722 2489
Jukka Rautava tel. +358 20 722 2120
Pekka Koponen tel. +358 20 722 6755

VTT TECHNICAL RESEARCH CENTRE OF FINLAND
P.O. Box 1000
FI-02044 VTT, FINLAND