Ensuring Secure Communication in Critical Infrastructures

Steffen Fries and Rainer Falk
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

***Abstract*—Critical infrastructures as backbone of the society and economy are increasingly the target of cyber attacks. These infrastructures have been isolated in the past, but are connected more and more also with external systems to allow for new and combined services. This immediately requires the protection of the communication connections to external sites. Legislation and operation have taken this into account and provide the necessary framework for posing specific communication security requirements. From the technical side, different security counter measures exist to cope with the given requirements, but it has to be ensured that these technical means are not only provided, but in fact applied in operation. This paper describes a new approach to ensure that during the setup of a secure communication connection the appropriate security is effectively negotiated with respect to permissible cipher suites for authentication, message integrity, and confidentiality. The application within a Smart Grid is used as example application domain.**

Keywords–security; critical infrastructure; smart energy grid; industrial automation; Internet of Things; secure communication; security policy; security protocol; Transport Layer Security

I. INTRODUCTION

Critical Infrastructures (CI) and especially cyber security in critical infrastructures has gained more momentum over the last years. The term "critical infrastructure" in the context of this paper is used to describe technical installations, which are essential for the functioning of the society and economy of a country, but also globally. Typical critical infrastructures in this context are the smart energy grid (including central or distributed energy generation, transmission, and distribution), water supply, healthcare, transportation, telecommunication services, just to state a few. The increased threat level becomes visible, e.g., through reported attacks on critical infrastructure, but also through legislation, which meanwhile explicitly requires the protection of critical infrastructures and reporting about serious attacks.

Information Technology (IT) security in the past was addressed mostly in common enterprise IT environments, but there is a clear trend to provide more connectivity to operational sites, which are quite often part of the critical infrastructure. Examples for operational sites are industrial automation or energy automation. This increased connectivity leads to a tighter integration of IT and Operational Technology (OT). IT security in this context evolves to cyber security to underline the mutual relation between the security and physical effects.

This paper focuses on the smart energy grid as example for critical infrastructures. The smart energy grid consists of several interworking parts depending on communication in a secure and reliable way. These parts are given through the classical power system elements like a centralized power generation, power transmission (typically high voltage and wide area connections), power distribution (low and medium voltage) and the consumer at the end of the supply chain. In the last years, the usage of renewable energy, e.g., through solar cells or wind power, became increasingly important to generate environmentally sustainable energy and thus to reduce greenhouse gases leading to global warming. Utilizing renewable energy in the power grid can be achieved in basically two ways: replacing classical power plants with renewable power plants likewise connected to the transmission grid. Alternatively, Decentralized Energy Resources (DER) are connected to the distribution network. In both cases, the energy generation through a grid of renewables needs to be monitored and controlled to a similar level as in today's centralized energy generation by power plants, while utilizing widely distributed communication networks. DER may also be aggregated virtually on a higher level to build a virtual power plant (VPP). A VPP may be viewed from the outside in a similar way as a common power plant with respect to energy generation. But due to its decentralized nature, the demands on communication necessary to control the VPP are much more challenging.

The target architecture for this paper is depicted on abstract level in Figure 1 below. It investigates into cyber security requirements from different sources providing specifics for secure communication and utilized technical security measures. Specifically, it proposes technical means to ensure the desired strength of security (given through a security policy) for the communication in the operation environment. The remainder of the paper is structured as follows. Section 2 investigates in cyber security requirements given through regulation, standards and guidelines. Section 3 investigates into Transport Layer Security (TLS) [1] as one common security protocol utilized power systems. Section 4 concentrates on the assurance that this security protocol is used with settings according to a given security policy. The technical proposal to achieve compliance to a given security policy for the communication between different entities of critical infrastructures is the main contribution of this paper. Note that this concept has not been implemented, yet. The conclusion discusses applicability to further security protocols and the necessity for an evaluation to determine the impact of the proposed solution to the overall system.

 ISBN: 978-1-61208-484-8

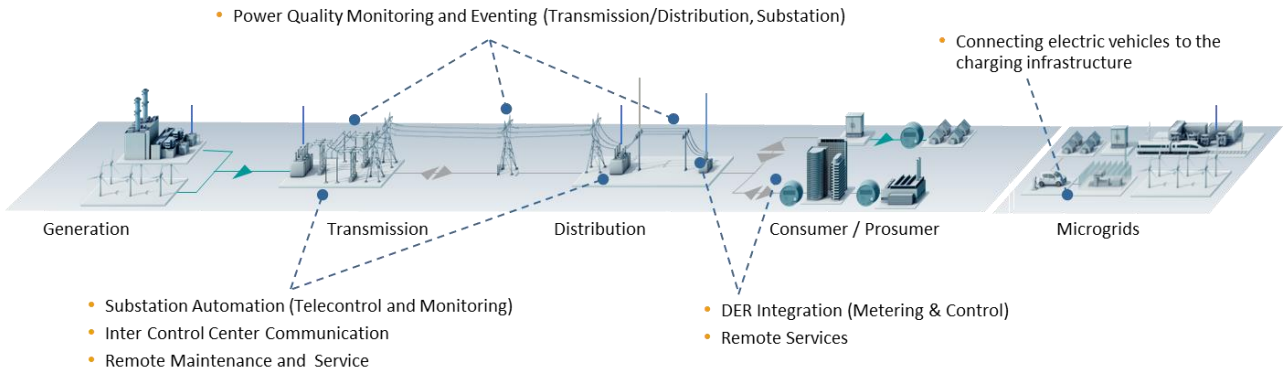

Figure 1. Overview Smart Energy Grid as Example for Critical Infrastructures

II. SMART ENERGY GRID SECURITY REQUIREMENTS

As stated in the introduction, the operational environment of critical infrastructures, in this paper on the example of the smart energy grid, differs from office environments or telecommunication environments in significant aspects. This leads to a different focus of general security requirements, like shown in the following Figure 2.

	Critical Infrastructures	Office IT
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	Up to 30 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	High	Medium

Figure 2. Comparison CI and Office environment

These general security requirements are addressed in regulation, standards, guidelines and further customer specific or operator requirements. Figure 3 depicts example sources for such security requirements.

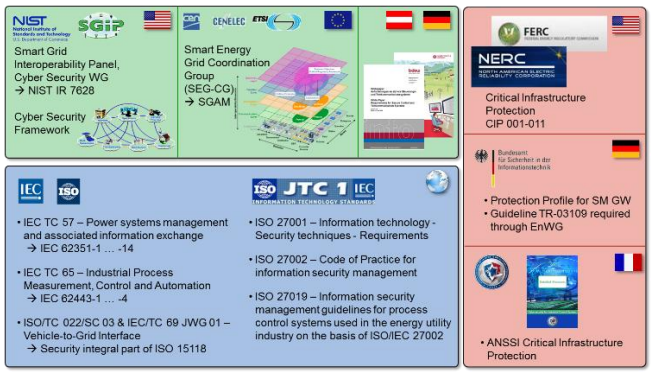

Figure 3. Sources for Security Requirements

As this paper focuses on communication security, the following subsections investigate into specific secure communication requirements in example requirement documents of different sources.

A. Regulative requirements

The regulative environments taken here as example focus on the operation of CI:

– The North American Electric Reliability Council (NERC) has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–011 [2], which are designed as foundation of sound security practices across bulk power systems. They provide a consistent framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional, as well as non-functional requirements. NERC-CIP version 3 is formally controlled and enforced in the U.S. and in Canada. The first version originated in 2006 and has been continuously enhanced.

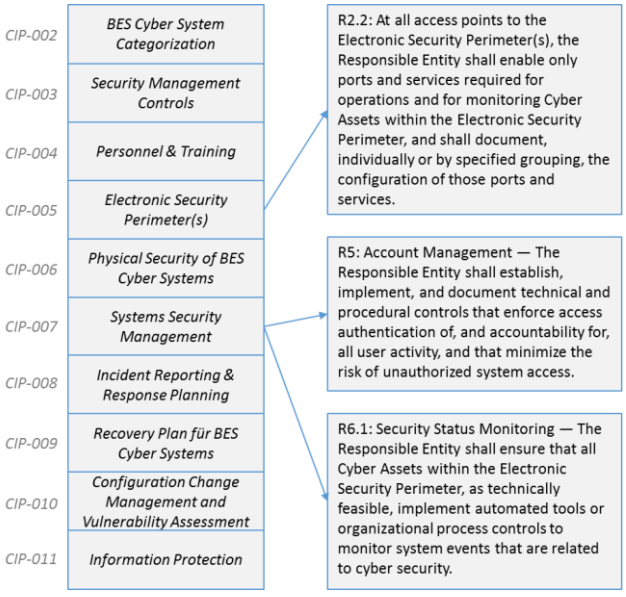

Figure 4. NERC-CIP Security Requirements

– A further example can be given by the legislation in Germany. Here, the IT security law has been finalized in 2015 requiring appropriate protection and monitoring, as well as reporting about security breaches for the operator of CI [3]. A specific regulation is the German Energy Act [4], which regulates in §21 the application of smart meters in facilities depending on the energy consumption/generation rate. The German "Bundesamt für Sicherheit in der Informationstechnik" (BSI) provides the technical guideline TR 03109 [5] to fulfill the requirements from the Energy Act and explicitly, how to ensure secure communication utilizing TLS to protect the communication.
– In France, the "Agence nationale de la sécurité des systèmes d'information" (ANSSI) regulates cyber security. Specifically, for secure communication there exists a guideline for the selection of TLS mechanisms providing appropriate protection [6].

The common approach of these regulations is, that they cover organizational requirements, process requirements and also technical requirements. The examples show that the security of communication is a clear part of the requirements.

B. Standards

Besides legislation, there exists a variety of standards, formulating security requirements or provide specific solutions to secure communication in an interoperable way. The following bullet list builds on the standards stated in Figure 3.

– IEC 62443, especially IEC 62443-3-3 [7]

  IEC 62443 is a security requirements framework defined in the IEC (International Electrotechnical Commission) Council) and can be applied to different automation domains, including energy automation, process automation, building automation, and others. As shown in Figure 5 the different parts are grouped into four clusters covering
  – common definitions, and metrics
  – requirements on setup of a security organization (ISMS related), and solution supplier and service provider processes
  – technical requirements and methodology on a secure system at system-wide level and
  – requirements to the secure development lifecycle of system components, and security requirements to such components at a technical level

  According to the methodology described in IEC 62443-3-2, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits" that map for example to the logical network protocol communication between two zones. Moreover, this document defines Security Levels (SL) that correlate with the strength of a potential adversary. To reach a dedicated SL, dedicated requirements have to be met.

Figure 5. IEC 62443 Overview

Several requirements formulated in IEC 62443-3-3 [7] directly target communication security like:

– Requirement 3.3.1 Communication integrity: "The control system shall provide the capability to protect the integrity of transmitted information".
– Requirement 4.4.1 Communication confidentiality: "The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network."

These requirements are used her as an example that IEC 62443 requires the support of certain functionality. These requirements are linked to different security levels and thus have to be seen in the overall system context.

– IEC 62351, especially IEC 62351-3 [8]

IEC 62351, which is also defined in the IEC, targets security mechanisms applicable to the power systems domain. The standard is split into different parts addressing specific security topics, as shown in Figure 6.

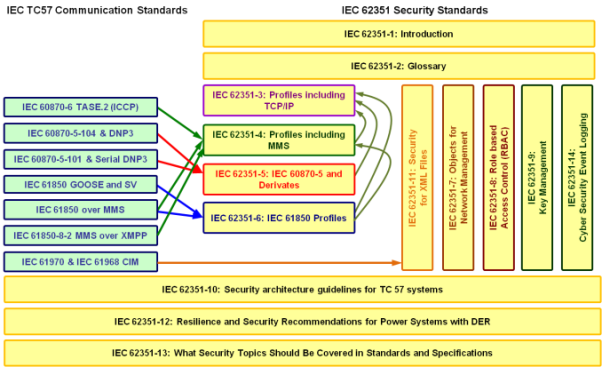

Figure 6. IEC 62351 Overview [8]

Specifically, IEC 62351-3 targets to secure TCP based communication by profiling the use of TLS and is referenced from other IEC 62351 parts. Profiling of TLS relates to narrowing available options in TLS like the requirement to utilize mutual authentication reducing the number of allowed algorithms or the disallowance of utilizing certain cipher suites, not providing sufficient

 ISBN: 978-1-61208-484-8

protection. Moreover, this part also provides guidelines for utilizing options, which depend on the embedding environment. An example is the relation of using session renegotiation and session resumption in conjunction with the update interval of the certificate revocation information.

C. Guidelines

Besides regulations and standards, there also exist guidelines on how to address secure communication in specific application environments.

– The "Bundesverband für Energie- und Wasserwirtschaft" (BDEW) introduced a white paper defining basic security measures and requirements for IT-based control, automation and telecommunication systems for energy and water systems, taking into account general technical and operational conditions [10]. It can be seen as a further national approach targeting similar goals as NERC-CIP, but at a less detailed level. The white paper addresses requirements for vendors and manufacturers of power system management systems by directly relating to ISO 27000. Section 2.3 of this white paper focuses on communication and formulates specific requirements for integrity and confidentiality of connections.

– NISTIR 7628 [11] originates from the Smart Grid Interoperability Panel (Cyber Security WG) of the National Institute for Standards and Technology (NIST). It targets the development of a comprehensive set of cyber security requirements. The document consists of three subdocuments targeting strategy, security architecture, and requirements, and supportive analyses and references. It specifically formulates requirements for smart grid information system and communication protection.

III. TLS TO SECURE TCP COMMUNICATION

As shown in the previous section, there are numerous examples of requirements to secure communication, which leads to the necessity to be able to verify that the appropriate communication security is applied in fact in operational use. This section investigates into technical means to ensure secure communication by taking TLS as example, as it is used widely also in power automation systems (see IEC 62351 in section II.B) , to protect the communication.

TLS in its current version 1.2 defines protection means for TCP-based communication and is defined in Internet standard RFC 5246 [1]. Note, that the standard has a long history and is constantly being evolved to cope with new advances in cryptography and communication security. It supports a variety of authentication options for the communicating peers and allows the negotiation of the protection of the preceding communication in terms of integrity and confidentiality and also key management related options like key updates, etc. The combination of cryptographic algorithms for authentication, integrity, and confidentiality protection is called cipher suite. TLS is build upon several sub protocols that encapsulate the protocol operation in the different phases as shown in Figure 7.

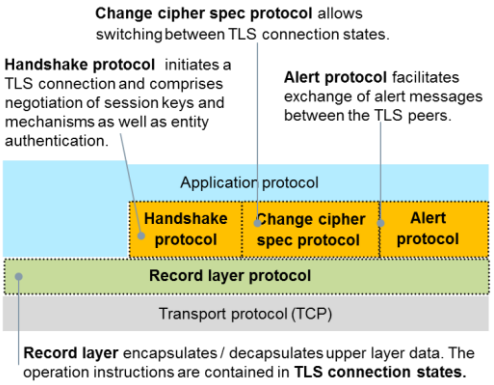

Figure 7. TLS Protocol Structure

For the discussion in this paper the most interesting phase is the TLS handshake, as it is performed in clear and allows the monitoring of the negotiated security options for the following communication session. Figure 8 shows the message exchange during the handshake.

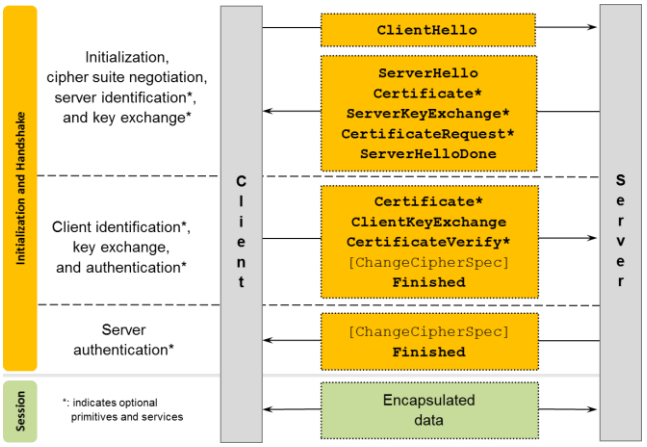

Figure 8. TLS Handshake for TLS Session Setup

Especially, the first phase of the handshake is in focus here, as it conveys the information for the cipher suite negotiation and the authentication of the communicating peers. In the *ClientHello* message, the client passes a list of cipher suites to the server containing the combinations of cryptographic algorithms supported in order of the client's preference. The server will then select a cipher suite and respond with a *ServerHello* message if a matching proposal was found. If no matching proposal was found, the server will issue a failure alert. Assumed that the server will authenticate towards the client, it will send its certificate as part other response. This allows the client to identify the server, validate the server certificate, as well as to utilize the

 ISBN: 978-1-61208-484-8

server certificate during the further session key establishment. If the server additionally requires a client authentication as part of the TLS handshake, it will send a *CertificateRequest* message.

The second phase of the handshake targets the client identification (if requested) and the session key establishment and the authentication of both sides. The *Finished* message from the server to the client concludes the handshake and is the first message encrypted using the negotiated session key. It also contains a hash over the previously exchanged handshake messages to have a delayed verification of the integrity of the performed handshake.

Based on the provided TLS overview the handshake phase can be used to monitor the establishment of a secure communication, which can be audited by an independent component. This can be used additionally to the server security policy configuration to ensure that the negotiated security settings for a communication channel provide a strength required by the security policy. The independent audit option will reveal failures in the configuration of the client or server side or both.

IV. Ensuring Secure Communication

As depicted in the previous section by taking TLS as example, it is possible to monitor the security negotiation of secure communication protocols in a passive way, without interfering with the protocol. To utilize this property, an additional component – a crypto option filter – in a network is defined. This crypto filter may be realized as separate component or may be part of an already existing component handling the data exchange, e.g., a switch.

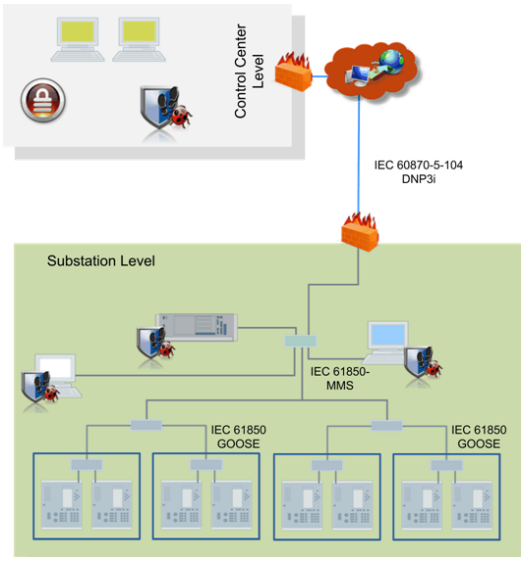

Figure 9. Substation to Control Center Communication

Figure 9 shows the underlying use case targeting the communication between a substation and a control center connected over a public network using a dedicated protocol (here: IEC 60870-5-104) for telecontrol, which is secured by TLS. Both sides are required to authenticate within TLS on the base of X.509 certificates and to provide support for one of the following cipher suites:

– TLS_RSA_WITH_AES_128_CBC_SHA
– TLS_DH_ DSS_WITH_AES_128_SHA
– TLS_DH_DSS_WITH_AES_256_SHA
– TLS_ECDHE_ECDSA_WITH_ AES_128_SHA

The following cipher suites are explicitly forbidden, as they do not provide confidentiality of the data exchange or not even integrity protection (first bullet)

– TLS_RSA_WITH_NULL_NULL
– TLS_RSA_WITH_NULL_SHA256
– TLS_ECDHE_ECDSA_WITH_NULL_SHA

This data is typically contained in a policy configuration data base together with connection specific information to identify the associated security policy.

In the following, two approaches for the realization of a crypto option filter from a network design perspective are described. This also comprises a functionality to utilize the information for ensuring a match to a given security policy, which may then lead to the interruption of communication establishment, if the security policy is not met.

Figure 10 shows a variant, in which the crypto option filter is placed directly into the communication path. This realization may be based on existing network components in the communication path. The data analysis component monitors the connection establishment and the TLS handshake without interrupting the communication channel establishment. The handshake messages *ClientHello* and *ServerHello* carry the specific information about the cipher suite negotiation, which is monitored and compared with the data from security policy database. Additionally the exchange of the server and client side certificate is monitored. As an additional service, the crypto filter may validate the exchanged certificates to ensure that they are not outdated or revoked. Depending on the match of the security negotiation parameter with the security policy, the communication establishment may be terminated through the policy enforcement component.

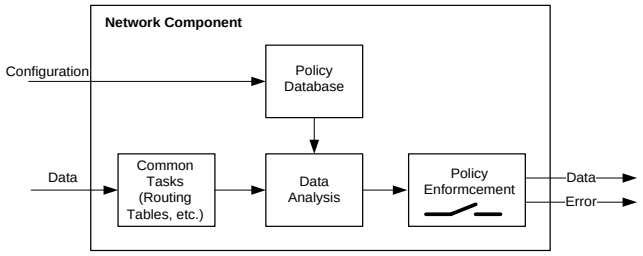

Figure 10. In-path Crypto Option Filter

In contrast to the in-path crypto option filter, Figure 11 shows an off-path filter. The general evaluation is similar to

the in-path filter, with the exception of the data access. As the filter is not directly placed in the communication path, a probe on the network duplicates the traffic and forwards it to the off-path crypto option filter. This probe may be a separate component or a monitoring port on the existing infrastructure component as shown in Figure 11. If it is a separate component, the probe may already preprocess the handshake and extract the information, which can then be provided to the crypto option filter. If the functionality is included in an existing infrastructure component, the complete TLS handshake may be forwarded to the crypto option filter for inspection. Alternatively, the policy enforcement component may integrate the traffic duplication.

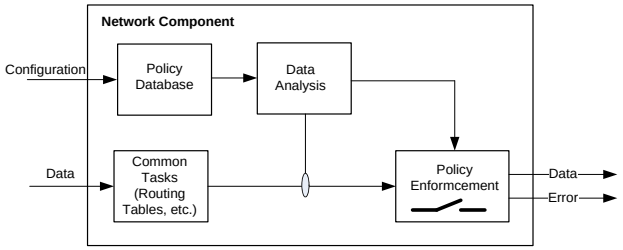

Figure 11. Off-path Crypto Option Filter

The off-path variant has the clear advantage that the policy checking component can be centralized, independent from the actual communication path to be checked.

Note that the description for the crypto option filter focused on the TLS 1.2 version as discussed in Section III. But TLS will be evolved and TLS 1.3 is currently under development. This version will result in simplifications of the meanwhile complex handshake and will reduce the available options and also shorten the handshake phase to three messages. Most importantly, TLS 1.3 will utilize the established key already in the handshake phase to protect messages. The monitoring approach described in the following is still applicable, as the message parts containing the monitoring target are still in clear.

V. CONCLUSIONS AND OUTLOOK

This paper described a solution to ensure that communication between different components of a system is in fact protected according to a dedicated security strength as defined by a given security policy. It ensures that the required level of security is indeed utilized during operation. As shown, requirements for secure communication exist through different guidelines, standards, and also legislation. The proposed solution was shown in the context of substation to control center communication, to ensure mutual authentication and an appropriate protection of the communicated information. As the smart energy grid does increasingly integrate DER systems, the chance of communicating privacy related data increases. And so do the requirements for protected communication.

The example shown related to the protocol TLS, which is used in power system automation to secure the communication. Also other protocols like IPSec or openVPN exist, which are used to provide a secure tunnel for exchanging information. Here, the initial handshake during the connection establishment can be monitored in a similar way as shown for TLS.

Moreover, as the proposed crypto filter verifies the establishment of secure communication channels according to a given security policy, it can also be used to offload further validation tasks from the communication peers, like the validation of the peer certificates utilized during connection establishment.

As stated in the beginning, this paper describes the concept for ensuring the establishment of secure communication channels. The consequent next step is the integration of the proposed approach in a prototype, to validate the effectiveness.

REFERENCES

[1] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, Aug. 2008, http://tools.ietf.org/html/rfc5246 [retrieved: Jan. 2016].

[2] NERC-CIP, North American Electric Reliability Corporation, “CIP Critical Infrastructure Protection Standards”, Version 5, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, [retrieved: Jan.2016]

[3] German IT Security Law, July 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf (German) [retrieved: Jan. 2016]

[4] German Energy Act, EnWG, July 2012, http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf (German) [retrieved: Jan. 2016]

[5] Technical Guideline TR 03109, Technische Vorgaben für intelligente Messsysteme, 2015, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html (German) [retrieved: Jan 2016]

[6] ANSSI Technical Note, Recommandations de sécurité concernant l’analyse des flux HTTPS, October 2015, http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_TLS_NoteTech.pdf (French) [retrieved: Jan. 2016]

[7] IEC62443-3-3:2013, “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”, Edition 1.0, August 2013.

[8] IEC 62351-x Power systems management and associated information exchange – Data and communication security, http://www.iec.ch/smartgrid/standards/ [retrieved: Jan. 2016].

[9] ISO 27000 Series

[10] Bundesverband der Energie- und Wasserwirtschaft, Datensicherheit, BDEW "Whitepaper Requirements for Secure Control and Telecommunication Systems," Version 1.1, 03/2015., http://ldew.de/bdew.nsf/id/52929DBC7CEEED1EC125766C000588AD/$file/Whitepaper_Secure_Systems_Vedis_1.0final.pdf [retrieved: Jan 2016]

[11] NIST IR 7628 Guidelines for Smart Grid Cybersecurity: Vol. 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, Vol. 2 - Privacy and the Smart Grid, Vol. 3 - Supportive Analyses and References, NISTIR 7628 Rev. 1, (Volumes 1-3), http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf [retrieved: Jan 2016]

 ISBN: 978-1-61208-484-8