Verifying the Adherence to Security Policies for 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 (CI) 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 CI-external systems to allow for new and combined services. This immediately requires the protection of the communication connections to CI-external sites but also internally. 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 Digital Grid is used as example application domain.**

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

I. INTRODUCTION

Critical Infrastructures (CI) and specifically cyber security in critical infrastructures have 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 digital 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 IT security and physical effects to the system or environment.

The digital energy grid consists of several interworking parts depending on data exchange 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.

This paper bases on the contribution to IARIA ENERGY 2016 [1] and enhances the base version with more background and technical details. It continues to focus on the digital energy grid as example for a critical infrastructure. The target architecture is depicted on abstract level in Figure 1 below. The paper investigates into cyber security requirements from different sources (like legislation, standardization and guidelines) providing specifics for secure communication and utilized technical security measures. Based on the analysis of security requirements, technical means are proposed to ensure the desired strength of security mechanisms (given through a security policy) specifically targeting the communication in the operation environment.

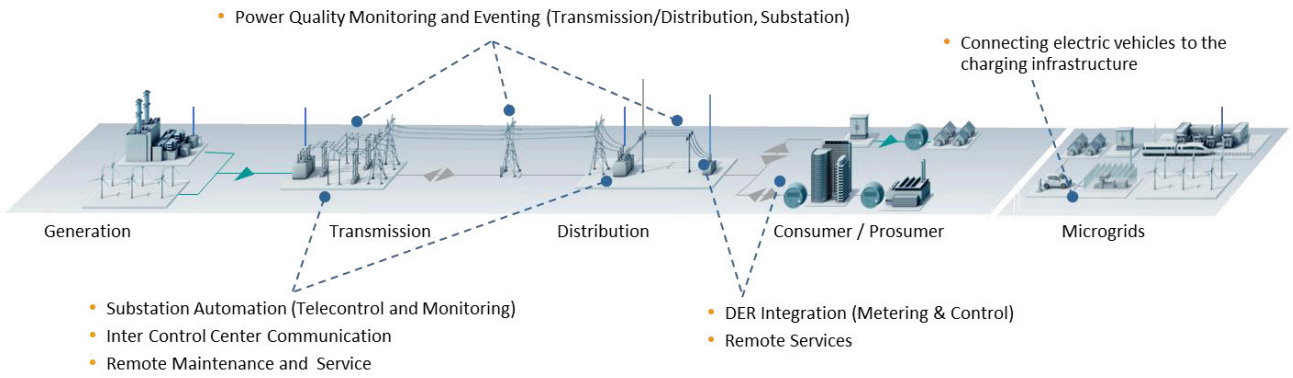

Figure 1. Overview Smart Energy Grid as Example for Critical Infrastructures

The remainder of the paper is structured as follows. Section II investigates in cyber security requirements given through regulation, standards and guidelines. Section III investigates into Transport Layer Security (TLS) [2] and IP Security (IPSec) as two common security protocols utilized in power systems. Section IV 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 using passive monitoring is the main contribution of this paper. Note that this concept has not been implemented, yet. Section V provides a short overview about existing techniques, concentrating on TLS inspection. The conclusion in section VI discusses applicability to further security protocols and the necessity for an evaluation to determine the impact of the proposed solution to the overall system.

II. SMART ENERGY GRID SECURITY REQUIREMENTS

As stated in the introduction, the operational environment of critical infrastructures, as in this paper the smart energy grid, differs from office environments or telecommunication environments in significant aspects. This leads to a different weight 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 (IT Service Center)
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

As visible, integrity and availability have a much higher impact in the critical infrastructure. Moreover, the immediate impact of information security to safety is also more prevalent as in Office IT.

The comparison of general requirements in Figure 2 is used here to underline that solutions, which are typically used in Office IT networks, may not be directly applicable in CI networks. Differences can be explained through the different operating environments and operating conditions. These general security requirements are addressed in a variety of regulation, standards, guidelines and further customer specific or operator requirements. Figure 3 depicts example sources for such security requirements.

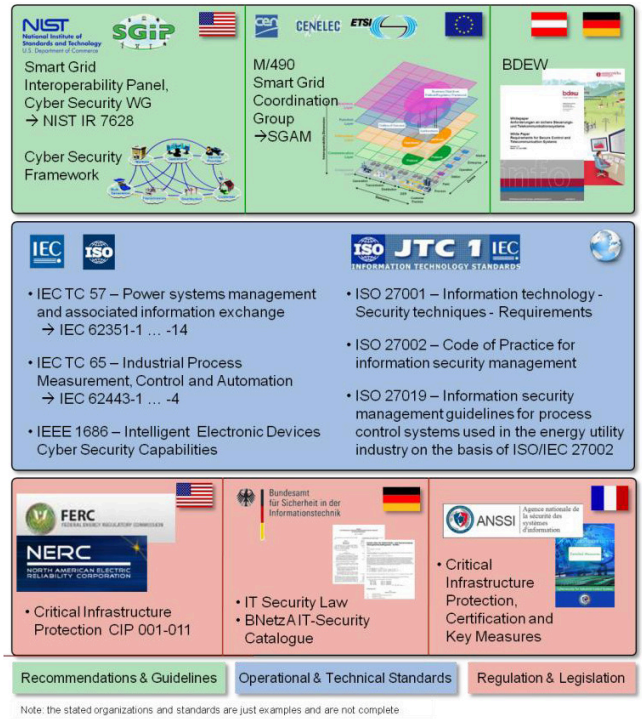

Figure 3. Sources for Security Requirements

As this paper focuses on communication security, the following subsections investigate into specific requirements

targeting secure communication in the example requirement documents of different sources as stated in Figure 3. The overview about these activities is used to underline the ongoing definition of specific security requirements, which will result in specific technical solutions. To ensure the final technical solution copes with given security requirements, a technical solution for security policy verification is proposed in section IV, focusing on communication security. Specifically, passively monitoring is used here to not interfere with the original control communication.

A. Regulative requirements

The regulative requirements taken here as example, focus on the operation of critical infrastructures from a process point of view. To support the security processes technical security controls need to be supported by either the system or the deployment environment. Hence, procedural and technical security requirements cannot be seen independent.

– The North American Electric Reliability Council (NERC) has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–011 [3], 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 applies to asset owners and power system operators and consists of a mixture of organizational, process, and technical 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. Meanwhile work is ongoing on version 6.

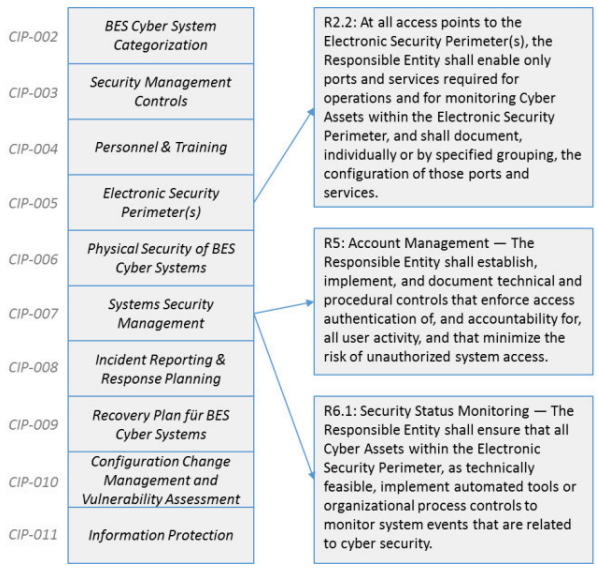

Figure 4. NERC-CIP Example Security Requirements

– A further example can be given by the legislation in Germany. Here, the IT security act has been finalized in 2015 requiring appropriate protection and monitoring, as well as reporting about security breaches for the operator of CI [4]. A specific regulation is the German Energy Act [5], 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 [6] to fulfill the requirements from the Energy Act and explicitly, how to ensure secure communication utilizing TLS to protect the communication. This targets specifically the data exchange of smart meters, either for control or for billing purposes. The protection means for secure communication are specifically defined and comprise the algorithms to be used for authentication, integrity protection, and confidentiality for TLS.
– In France, the "Agence nationale de la sécurité des systèmes d'information" (ANSSI) regulates cyber security. Specifically, for secure communication a technical note has been published providing appropriate protection [7]. This guideline provides recommendations of specific sets of algorithms (cipher suites) to be used for TLS as well as operational modes and extensions of the protocol to address discovered weaknesses.

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 one part of the requirements for which specific technical means are stated.

B. Standards

Besides legislation, there exists a variety of standards, formulating security requirements or provide specific solutions to secure communication in an interoperable way. Standards specify solutions like specific features or protocols in an interoperable way to support the interworking of different vendor's products. The motivation for this investigation is to show that specific security requirements and security counter measures can be directly derived from standards. These security countermeasures in turn can be evaluated in the deployments of critical infrastructures like the digital grid. This motivates the solution, later on described in section IV.

The following bullet list builds on the standards stated in Figure 3 and gives a more detailed overview about the content of the different standards.

– IEC 62443, especially IEC 62443-3-3 [8]

  IEC 62443 is a security requirements framework defined in the IEC (International Electrotechnical Commission) and can be applied to different automation domains, including energy automation, process automation,

building automation, and others. In the set of corresponding documents security requirements are defined, which target the solution operator and the integrator but also the product vendor.

As shown in Figure 5, different parts of the standard are grouped into four clusters covering

- common definitions and metrics
- requirements on setup of a security organization (ISMS related), as well as solution supplier and service provider processes
- technical requirements and methodology for security on system-wide level and
- requirements to the secure development lifecycle of system components, and security requirements to such components at a technical level.

Figure 5. IEC 62443 Overview and Status

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 as shown in Figure 6 below. To reach a dedicated SL, dedicated requirements have to be met.

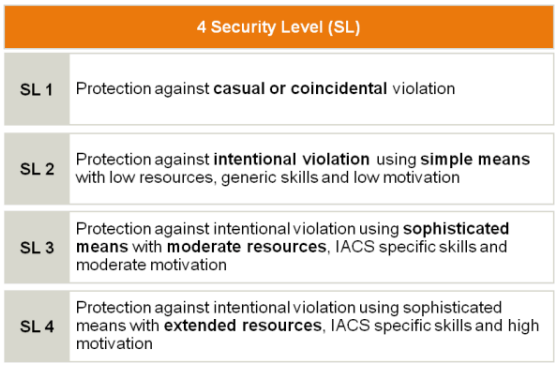

Figure 6. IEC 62443 defined Security Level

For each security level, IEC 62443 part 3-3 defines a set of requirements. Seven foundational requirements group specific requirements of a certain category:

- FR 1 Identification and authentication control
- FR 2 Use control
- FR 3 System integrity
- FR 4 Data confidentiality
- FR 5 Restricted data flow
- FR 6 Timely response to events
- FR 7 Resource availability

For each of the foundational requirements there exist several concrete technical security requirements (SR) to address a specific security level. In the context of communication security, these security levels are specifically interesting for the conduits connecting different zones. The following examples are taken from IEC 62443-3-3 [8] to illustrate some of the foundational requirements:

- FR3, SR3.1 Communication integrity: "The control system shall provide the capability to protect the integrity of transmitted information".
- FR4, SR4.1 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."
- FR5, SR 5.2 Zone boundary protection: "The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk -based zones and conduits model."

These requirements are used here as an example that IEC 62443 requires the support of certain functionality. Also, as seen especially by the last example in the list, the monitoring of the connections is required.

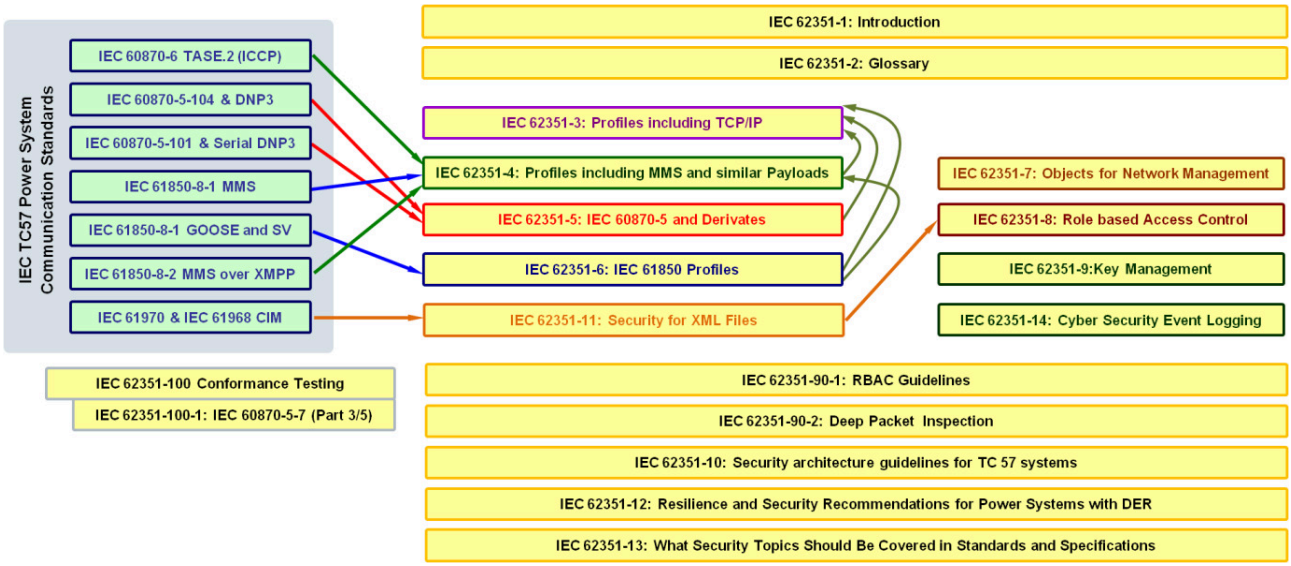

Figure 7. IEC 62351 Overview [9]

– IEC 62351, especially IEC 62351-3 [9]

  IEC 62351, which is also defined in the IEC, targets security mechanisms applicable to the power systems domain specifically. As IEC 62443, the standard is split into different parts addressing specific security topics, as shown in Figure 7.

  Different to IEC 62443, IEC 62351 describes security controls on a very detailed level to achieve interoperability in the utilized security means. Hence, it can be seen as a set of security controls to address some of the security requirements posed by IEC 62443. 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 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. As stated, IEC 62351-3 is always used in conjunction with other parts of IEC 62351 like part 4, addressing substation automation communication from a control center or communication between control center or part 5 for telecontrol.

– IEEE 1686 [10] specifies the expected security capabilities for Intelligent Electronic Devices (IED) regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Also addressed is the encryption of communications with the IED. It serves as a procurement specification for new IEDs or analysis of existing IEDs.

  Beyond others, there are specific requirements for communication security. These address for instance:

  – File transfer is only allowed using Secure File Transfer Protocol
  – Network management shall be provided with SNMPv3.
  – Secure tunneling using cryptographic VPNs.

  Specific cryptographic algorithms are not required, but the support of the stated functionality.

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 27002 [11]. Section 2.3 of this white paper focuses on communication and formulates specific requirements for integrity and confidentiality of connections.

– NISTIR 7628 [12] 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.

– SGIS Report: The security subgroup of the European Smart Grid Coordination Group (SG-CG) targeted the European Commission mandate M/490 [13] and addressed cyber security in the (European) smart grid. Smart Grid services shall be enabled through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, down to connected properties. The report describes an analysis framework applied to different use cases and mapped to standards work to address identified security requirements. The investigation into security was closely connected to Smart Grid Architectural Model (SGAM) developed by a different working group. The final report of the security subgroup (see [14]) provides recommendations of security means, to be applied in the different zones and domains of SGAM. Secure communication has been specifically referenced through the IEC 62351 series and general security protocols like TLS, which will be investigated in the next subsection.

III. SECURE COMMUNICATION PROTOCOLS

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 example protocols to ensure secure communication by taking TLS and IPSec as example, as they are widely used, also in substation automation. The goal is to analyze the protocol session establishment phase and specifically into options to monitor the negotiation of security parameters to ensure the compliance to a given security policy. This information shall be used afterwards to discuss options to monitor the session establishment passively. As it will be shown in the following subsections, only in case of TLS passive monitoring of the security parameter establishment can be performed. Therefore, for the discussion of a technical solution, TLS is used further on as example.

A. TLS to Secure TCP Communication

TLS is widely used in power automation systems (see IEC 62351 in section II.B), to protect the communication for automation control and monitoring, but also for remote management.

TLS in its current version 1.2 defines protection means for TCP-based communication and is defined by the Internet Engineering Task Force (IETF) in RFC 5246 [2]. Protection here relates to different security services like unilateral or mutual authentication, message integrity, or message confidentiality, which can be negotiated during the initial handshake. Note, that the standard has a long history and is constantly being evolved to cope with new advances in cryptography and communication security. Currently there is work ongoing on version TLS 1.3, which will provide more radical changes compared to the enhancements in the previous version iteration. TLS 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.

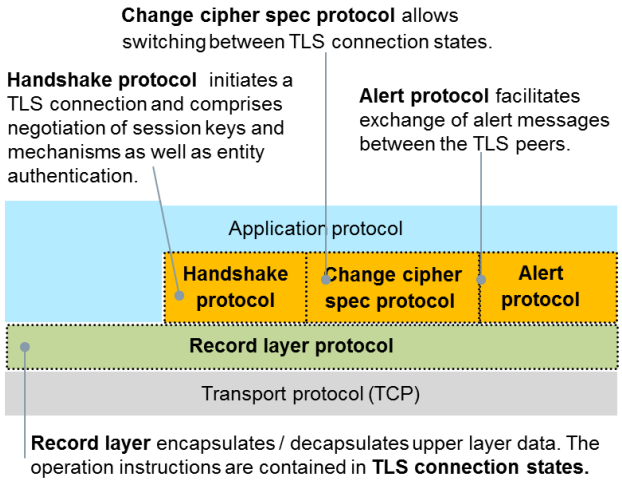

Figure 8. TLS Protocol Structure

TLS is built upon several sub protocols that encapsulate the protocol operation in the different phases as shown in Figure 8. For the discussion in this paper the most interesting phase is the TLS v1.2 handshake, as it is performed in clear and allows the monitoring of the negotiated security options for the following communication session. Figure 9 shows the message exchange during the TLS v1.2 handshake.

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

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. In this step, the client will provide its certificate if requested in the *Certificate* message. 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.

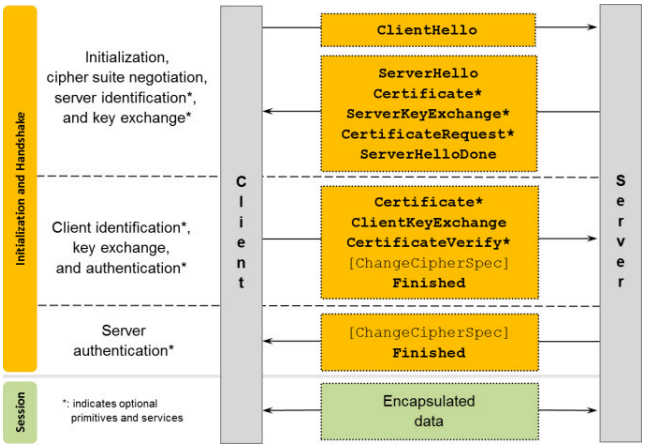

Figure 9. TLSv1.2 Handshake for TLS Session Setup

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.

Besides TLS protection of TCP based communication there exists also a derivation of TLS for UDP based communication. This security protocol is called Datagram Transport Layer Security – DTLS and is defined in RFC 6347 [15]. The handshake is similar to TLS, but is enhanced with a cookie mechanism to cope with the missing reliability of TLS. Hence, the message context during the handshake of DTLS can be analyzed in the same way as for TLS.

Besides the initial handshake, TLS supports further session management operations to support session key renegotiation or the resumption of previously closed sessions. Session renegotiation is essentially the performance of a complete handshake during an ongoing TLS session. It is performed to establish a new session key and also to verify the credentials used for authentication. Especially the latter is becoming necessary for long lasting connections between devices. This is due to the fact, that the certificates used during the handshake have a limited validity period. Additionally, they may be revoked if the corresponding private key has been compromised. To ensure that this is detected, the certificates used for authentication are re-evaluated during session renegotiation. Session resumption is different as it reuses the already established pre-master secret from a previous session to either negotiate a new session key during the still ongoing session or to resume the previous session, if it was closed before. This enables a much faster session startup as the asymmetric operation is omitted. Note that session resumption is at maximum allowed 24 hours after the original session has been closed. Session renegotiation and session resumption during a still running session are both performed over the already existing TLS session. This makes a passive monitoring of the handshake impossible, if encrypting cipher suites have been negotiated during the initial handshake. Session resumption of a session that has been closed before will perform the TLS handshake on a "fresh" TCP connection. In this case, the handshake is performed in clear text, as the TLS connection needs to be reestablished. Hence, the resumption can be passively monitored for security policy compliance.

As stated before, TLS is a protocol that is under constant development. Over the years it has become more versatile also due to its extensibility. This extensibility has been used to enhance the feature set but also to address discovered weaknesses. Currently TLS v1.3 is under development with the goal to redesign the handshake to offload some of its complexity and also to be able to have a more performant session setup. This version is currently in draft status [16] but expected to be released as RFC during 2017.

In contrast to TLS v1.2 the new handshake can be performed in one message less, resulting in a 1.5 roundtrip handshake as shown in Figure 10. Also new is the option to already encrypt part of the information in the TLS server response message. The *Client.Hello and the Server.Hello* messages are till sent in clear text, allowing the inspection regarding compliance to a given security policy regarding the utilized cipher suites. Also, the server certificate is visible. A different approach has been taken for the client side authentication. In TLS v1.3, the *Certificate.Request* message from the server and the *Certificate* message from the client are sent encrypted. This hinders the inspection of the certificate by simply monitoring the TLS handshake. On the other hand, it increases the privacy of the client side, as eavesdropping by an adversary on path may not expose the client identity.

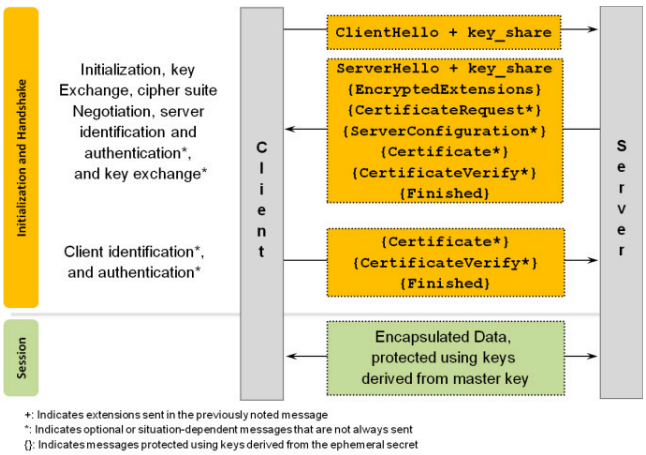

Figure 10. TLSv1.3 Handshake for TLS Session Setup

Based on the session establishment analysis, the initial handshakes of a TLS connection can be passively monitored to verify the adherence to a given security policy.

B. *IPSec and IKE to to support secure tunneling*

IPSec is a protocol typically being used to build secure communication tunnel, so-called Virtual Private Networks (VPN). The advantage of an IPSec based VPN is the option to tunnel different protocols either TCP-based or UDP-based. Therefore, this approach is often used to connect two distinct zones or sites. An example is the application to connect a substation and a control center, for which the IPSec VPN is used to protect IEC 61850 control communication or IEC 60870-5-104 telecontrol communication and additionally voice-over-IP (VoIP) communication to enable a direct interaction from the control center with a service technician located in the substation.

In contrast to TLS, IPSec describes the protocol protecting the bulk communication without an integrated key management. The key management for IPSec can be done manually or automated. For an automated key management the Internet Key Exchange (IKE) is available in version 1 and version 2. In both versions, IKE distinguishes two phases:

– In phase one, a secure key management channel between the involved IKE peers is established.
– In phase two, Security Associations for security protocols (e.g. IPSec) are established on request via the secure key management channel.

While IKEv1 supports a variety of authentication modes and also different modes for the phase one key exchange, IKEv2 has been specified to reduce this complexity. IKEv2 is defined by the IETF in RFC 4306 [17]. Figure 11 below shows the message exchanges for both phases including the different parameter contained in these messages. It becomes immediately visible, that within phase 1, after the first roundtrip the remaining communication is encrypted. Therefore, only the first handshake of the phase 1 key exchange can be passively monitored.

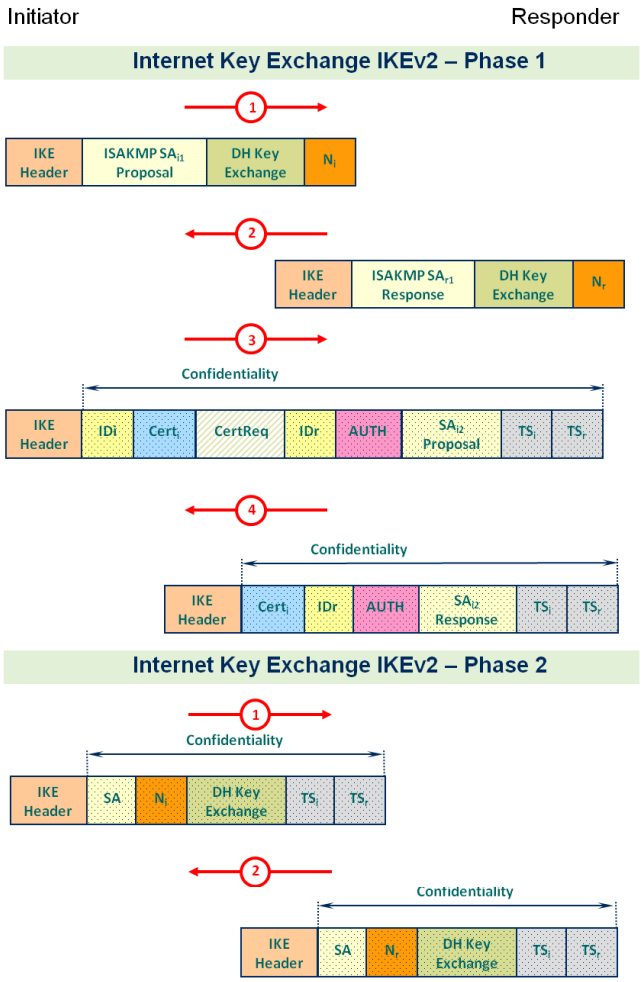

Figure 11. IKEv2 Phase 1 and Phase 2 Key Exchange

These messages negotiate cryptographic algorithms (contained in the security association payload SA), exchange nonces (N), and perform a Diffie-Hellman key agreement (DH) for the second phase of IKE. The security association parameters for the actual IPSec session are negotiated in IKE phase 2, which is encrypted using the negotiated parameter from IKE phase 1. As shown, this key management cannot be monitored passively to verify the negotiation of IPSec parameter according to a security policy. Here, an investigation at either side of the VPN tunnel would be necessary, e.g., by verifying the negotiation of the security association based on the settings and the system security log.

IV. ENSURING SECURE TCP 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 and by a component not involved in the actual communication. 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 of the message exchange (not the actual data processing), e.g., a switch. This allows for inpath and also for offpath monitoring. Offpath monitoring specifically enables monitoring options without an influence to the control communication in terms of delay. The task of the crypto filter is essentially the monitoring of clear text session establishment phases of cryptographic protocols to evaluate the adherence of a given security policy. The crypto filter is defined as part of this paper; an evaluation of the approach has not been done, yet.

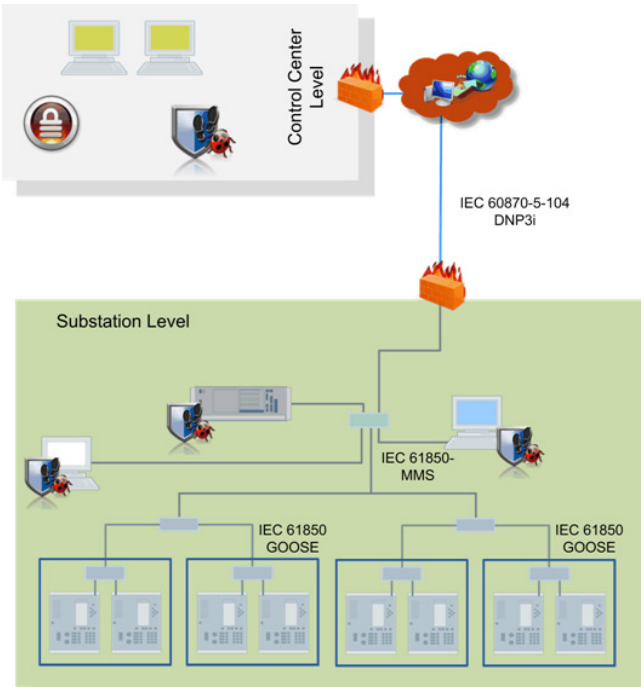

Figure 12. Substation to Control Center Communication

Figure 12 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 13 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.

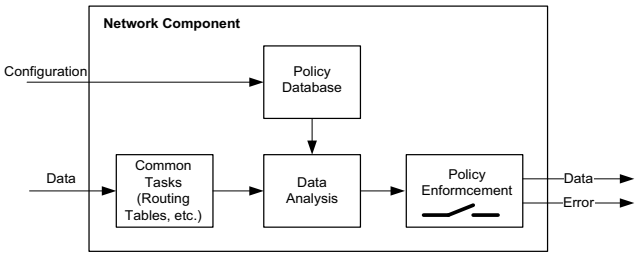

Figure 13. In-path Crypto Option Filter

In contrast to the in-path crypto option filter, Figure 14 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 14. 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.

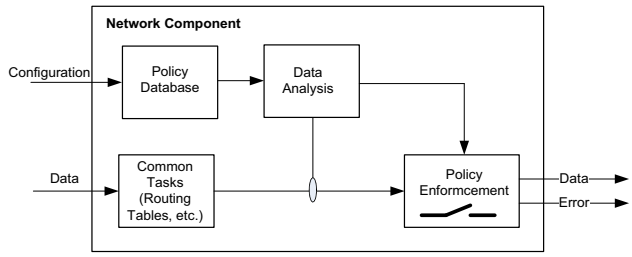

Figure 14. Off-path Crypto Option Filter

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.A. TLS 1.3 will result in simplifications of the current more 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 as described is not completely possible. While the negotiation of cipher suites can still be followed as it proceeds in clear, the client certificate exchange is encrypted. Hence, the certificate may not be checked anymore.

V. EXAMPLES FOR EXISITING SOLUTIONS

Monitoring of communication protocols for specific content can be done on-path (as part of the immediate communication path) or off-path as also stated in the previous section. Off-path techniques may involve for instance the monitoring port of switches, which allow direct access to the routed data and thus to analyze these data. This is only possible for communication protocols, which perform the data exchange in clear, without applying encryption. If encryption is applied, access to the utilized session key would be necessary. On-Path techniques insert a new component (middlebox) into the communication path, which terminates the communication connection to both sides and allows for the inspection of the data exchange. Examples are deep packet inspection modules, which can be operated on Firewalls to inspect the data for viruses, malware or also malformed protocol messages. Utilizing these components to ensure adherence to a session security policy are not know. The described solution in section IV for TLS can be seen as enhancement to packet inspection. In the specific case, the clear text handshake of TLS is leveraged to allow for the application of both techniques, on-path and off-path.

Alternatively to the described solution for TLS, there is ongoing research on changing the handshake of TLS to allow middleboxes to inspect traffic on-path as described in [18] without breaking end-to-end security called mcTLS (Multi Context-TLS). The basic principle here is to perform an enhanced handshake involving middleboxes into the handshake phase of TLS. Specifically, the middleboxes are authenticated during the handshake and thus know to both communicating ends. Moreover, each side is involved in the generation of the session key, which is also provided to the middlebox. There is also additional keying performed for the exchange of pure end-to-end keys, allowing the application of key material known to the middlebox to encrypt the traffic and for integrity protection, while the end-to-end based keys are used to provide an end-to-end integrity. The latter approach ensures that the middlebox can read and analyze the content of the communication in the TLS record layer, but any change done by the middlebox is detected by a violation of the end-to-end integrity check value. This approach has the advantage that it provides an option to check the associated security policy during the session setup and at the same time monitor traffic as an authorized component. The drawback is that the solution focuses solely on TLS and cannot be applied to other protocols without changes. Also, it is always included as an in-path component, which may result in unwanted performance influences. This shows another approach, which requires also requires more effort for the realization as it requires changing the utilized security protocol.

VI. 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. Besides that, it has been shown, that the approach has its limits on the example of IPSec as here, the main information about the bulk data exchange protection are already negotiated in an encrypted manner and therefore not visible to a passive monitoring component.

In the investigated case of TLS, 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. Also shown have been limitations for TLS, in the context of renegotiations of the session parameter. As in the case of IPSec, the renegotiation of session parameter is performed over an encrypted connection and can therefore not be monitored passively. If there is a requirement to also monitor these exchanges, classical proxy solutions terminating the secure channel can be used, with the influence on session setup and potential additional components.

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

REFERENCES

[1] S. Fries and R. Falk, "Ensuring Secure Communication in Critical Infrastructures," Proceeding IARIA ENERGY 2016, pg. 15-20, June 2016, ISBN: 978-1-61208-484-8,

[2] 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].

[3] 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]

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

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

[6] 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]

[7] ANSSI Technical Note, Security Recommendations for TLS, February 2017, https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf [retrieved: Mar. 2017]

[8] 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.

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

[10] IEEE 1686, "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities," Mai 2013Bundesverband 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] ISO 27002, "Information technology - Security techniques - Code of practice for information security controls," 2013

[12] 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 2017]

[13] Mandate M490, http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=475# [retrieved: Jan 2017]

[14] CEN/CENELEC/ETSI Smart Grid Reports: www.cencenelec.eu/go/SmartGrids/ [retrieved: Jan. 2017]

[15] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, January 2012, https://tools.ietf.org/html/rfc6347, [retrieved: Jan. 2017]

[16] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Draft, https://tools.ietf.org/html/draft-ietf-tls-tls13-18, October 2016, [retrieved: Jan. 2017]

[17] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306, December 2005, https://tools.ietf.org/html/rfc4306, [retrieved: Jan. 2017]

[18] D. Naylor et al., "Multi-Context TLS (mcTLS), Enabling Secure In-Network Functionality in TLS," http://mctls.org/, [retrieved: Jan. 2017]