SMART GRID PROTECTION AGAINST CYBER ATTACKS

Contract No 608224

Deliverable D3.3
Smart Grid Security Standards Recommendations

AIT Austrian Institute of Technology • Fraunhofer AISEC • The Queen's University Belfast
Energieinstitut an der Johannes Kepler Universität Linz • EMC Information Systems International Ltd
Kungliga Tekniska högskolan (KTH) • Landis + Gyr
United Technologies Research Centre • SWW Wunsiedel GmBH

Document control information	
Title	Smart Grid Security Standards Recommendations
Editor	Paul Murdock
Contributors	Ivo Friedberg, Robert Griffin, Paul Murdock
Description	This document presents a view on standards recommendations for Smart Grid security.
Requested deadline	31-Mar-2016

Executive Summary

This document, the third deliverable for SPARKS Work Package 3 (WP3), provides recommendations regarding existing and new standards relevant to securing Smart Grid environments.

We begin by describing the Smart Grid security standards landscape, referencing major surveys of this landscape that have been created by the European Union Agenda for Network and Information Security (ENISA), by CEN/CENELEC/ETSI, including recommendations in that survey related to the Smart Grid security standards landscape, and by the US National Institute of Standards and Technology (NIST).

In the sections that follow, we look at standards related to each of the major areas covered in the SPARKS project work packages. For each of these areas, we identify what we believe are the most significant gaps in the relevant standards and provide recommendations for addressing these gaps. In some cases, such as in the discussion of the need for standards related to Smart Grid resilience, we also provide detailed explanation of an approach that we believe would be helpful in terms of addressing those gaps.

In the appendices, we provide a list of the recommendations that are made in the body of the document. We also provide the report submitted to NIST by the SPARKS team during the public comment period for NIST 1180R3.

Table of Contents

Table of Figures

Preface

In the first deliverable for SPARKS Work Package 3 (WP3), D3.1, we focused on assessing of Smart Grid reference architectures. In the second deliverable, D3.2, intended for individuals directly involved in Smart Grid implementations, we provided guidance related to best practices, technologies and processes intended to help organizations create secure Smart Grid environments and solutions. In this document, D3.3 Smart Grid Security Standards Recommendations, the third deliverable for WP3, we propose changes to existing standards relevant to Smart Grid security and some additional standards that would be of value in achieving security for Smart Grid.

Many valuable resources are available to help understand the Smart Grid security standards landscape. Given these resources, we do not intend to provide yet another compendium. Rather, we have focused on areas where we believe there are gaps in the standards that should be addressed. Further, we provide recommendations related to the update and synthesis of existing resources that we believe will benefit Smart Grid security.

In developing this document, we have drawn on all of the deliverables of the SPARKS project to date. These include:

- Deliverables available on the SPARKS project website at
  https://project-sparks.eu/publications/deliverables/
- Materials developed for the SPARKS 1st Stakeholder Workshop and 2nd Stakeholder Workshop available at
  https://project-sparks.eu/events/1st-sparks-stakeholder-workshop/
  https://project-sparks.eu/events/2nd-sparks-stakeholder-workshop/
- Materials developed by SPARKS project consortium members as contributions to conferences, technical journals and other publication vehicles, available at
  https://project-sparks.eu/publications/publications/

1 Introduction

1.1 Purpose of this Document

This document expands on the insights from the previous SPARKS Work Package 3 (WP3) deliverables to provide guidance to Standards Development Organizations (SDO) regarding areas in which action should be taken by the wider Smart Grid security community 1) to revise existing standards and guidance related to Smart Grid security, 2) to create new standards and/or guidance, and 3) to increase the visibility and adoption of existing and future standards and guidance. In order to accomplish this goal, we begin by discussing in more detail the standards landscape for Smart Grid security, drawing particularly on comprehensive surveys of Smart Grid security standards from NIST SP 1180R3 (1), ENISA Smart Grid Security: Smart Grid related standards, guidelines and regulatory documents (2) and CEN/CENELEC/ETSI Smart Grid Information Security (3) to identify critical gaps in existing standards and in standards under development. These gaps include concerns regarding technical standards related to processes such as risk management, technology certification and security simulation, as well as to technologies such as device identification, protocol specification and security analytics. Gaps are also identified in guidance, such as in architectural recommendations related to hybrid architectures that include both traditional centralized grids and microgrids.

We draw on the two previous WP3 deliverables to provide important context for this document. D3.1 Assessment of Smart Grid Reference Architectures (4) discussed a range of issues that are important in establishing an effective security architecture for a Smart Grid environment; these included the role of architecture within a secure development life cycle, as well as the importance of technologies such as security analytics and device identification. D3.2 Guidance for Smart Grid Security (5) built on D3.1 to discuss the process of establishing a security architecture for Smart Grid environments, as well as introducing aspects of this process that are not yet well-developed in industry standard references such as NISTIR 7628 (6).

We also draw on deliverables from other SPARKS work packages, all of which provide context for the identification of gaps in Smart Grid standards and approaches for addressing those gaps. This is especially true in D2.2 Threat and Risk Assessment Methodology, in which the SPARKS team has proposed a methodology that addresses the significant gaps in existing Risk Assessment and Management methodologies in terms of their application to Smart Grid security (7).

In this deliverable, as we identify gaps in existing standards we provide recommendations on how to address these gaps, including steps that can be taken by the SPARKS project team. For each recommendation, one or more organizations to which that recommendation should be presented have been identified.

A number of our recommendations echo those from other organizations, particularly from CEN/CENELEC/ETSI, ENISA and NIST. However, to the best of our knowledge, the guidance presented here goes beyond that currently published by the respective organizations.

Given the world-wide importance of Smart Grid security and the important work that is being done in this area not only in the European Union but also in North America and Asia, we reference resources from all these geographies as appropriate to the discussion of the standards landscape and the gaps that we see as significant. For example, in our D3.1 deliverable, we suggested that the US Smart Grid security framework documented in NISTIR 7628 is an important architectural resource for organizations developing, reviewing or regulating Smart Grid solutions; in this deliverable, therefore, we touch on several gaps in the NISTIR 7628 resources that we called out in D3.1 and D3.2.

However, we have addressed our recommendations to EU organizations, rather than to organizations in other geographies, seeing these EU organizations as most appropriate to our project.

The remainder of this section describes our gap analysis and recommendations at a high level. Subsequent sections explore specific gaps and recommendations in more detail.

1.2 The Role of Standards in Smart Grid Security

Before presenting the gap analysis and recommendations, it may be helpful if we define what we means by standards, as the term is used in this document. We have taken a broad definition of the term, reflecting the large body of diverse resources that are or can be discussed as standards:

A number of kinds of standards are typically called “De Jure” standards:

- Documents approved and published by recognized government and/or industry standards bodies that specify protocols, application programming interfaces, XML schemas, ontologies, architectural models, security frameworks and other technical descriptions of functionality, interfaces and so on. There are many such standards relevant to Smart Grid in general and Smart Grid security in particular, including such core standards as the NIST, M/490 and micogrid reference architectures, IEEE standards and IEC standard discussed in D3.1.

- Documents approved and published by recognized standards bodies that specify processes for risk management, application development, testing, certification and so on. Again, there are many such standards relevant to Smart Grid security, including the risk management standards discussed in D2.2 and the reference architecture methodologies discussed in D3.1, mentioned above.

- Documents approved and published by recognized standards bodies that provide guidance regarding best practices for technology and process implementation relative to standards, interpretation and explanation of standards, interpretation and explanation of regulatory requirements underlying standards, and so on. Such guidance from NIST and ENISA is discussed in D3.2.

- Resources from recognized standards bodies such as function libraries, constant definitions, test harnesses, sample code, navigation tools and other capabilities that can be used by implementations to achieve or demonstrate conformance with a standard and/or with regulatory requirements

In contrast, “De facto” standards include all of the above kinds of standards, but are provided by vendors or organizations that do not qualify as standards organizations. Many vendor-defined interfaces and protocols that achieve widespread use fall into this category. Best practices and other kinds of guidance, from academic sources as well as from industry, can also become de facto standards; for example, the “Laws of Identity” from Kim Cameron of Microsoft (8).

Given the range of artefacts that can justifiably be called standards, it is clear that the roles and audiences of standards vary widely. We believe the purposes of this deliverable can best be met by considering de jure standards relevant to Smart Grid security and, in particular, by concentrating on those that we believe can or should have the highest impact on improving the security of Smart Grid implementations. We also focus on those aspects of Smart Grid security technology, process and governance that are central to our SPARKS project. Our goal in the gap analysis and recommendations is to show concrete steps that can be taken to improve the content and impact of Smart Grid security-related standards, recognizing that the success of any standard is a reflection not just of the content of that standard, but also of the significance of the issue addressed and the commitment of stakeholders to realizing that standard in their solutions.

1.3 Smart Grid Security Standards Landscape

An exhaustive and authoritative description of the Smart Grid security standards landscape is beyond the scope of the SPARKS project, especially since a number of organizations have already invested considerable effort in such descriptions, documented in comprehensive surveys of Smart Grid standards (including security-related standards):

- ENISA provides a detailed overview of Smart Grid standards in the 2013 document Smart Grid security: security-related standards, guidelines and regulatory documents (9) as well as guidance related to Smart Grid standards in the 2011 document Protecting Industrial Control Systems: Recommendations for Europe and Member States (10).
- CEN/CENELEC/ETSI surveys Smart Grid standards in the "Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids" (11) and the extract of recommendations in "Standards for Smart Grids". (12)
- NIST recently updated their list of Smart Grid security standards in NIST SP 1180R3. (13) This is complemented by an online tool for navigating Smart Grid standards. (14)
- IEC provides a survey of Smart Grid security standards in "A List of Cybersecurity for Smart Grid Standards and Guidelines". (15) This is also complemented by an online tool. (16)

There are a number of other resources that provides lists and/or explanation of Smart Grid standards, in most cases including at least some security-related standards. Some examples of these other resources are:

- Smart Grid Standards by Takura Sato et al. (17)
- China "State Grid Framework and Roadmap for Smart Grid Standards" (18)
- SGEM project D1.3.1 "Smart Grid Standardization Analysis" (19)
- IEEE list of existing and proposed standards (20)
- STARGRID project recommendations on Smart Grid standards (21)

Such resources are valuable to many organizations that are concerned with standards:

- Government organizations interested in ensuring a secure and resilient energy supply
- Energy suppliers interested in state-of-the-art, cost-effective implementation of Smart Grid security
- Vendors interested in providing technology and expertise for Smart Grid security solutions
- Standards Development Organizations (SDO) interested in ensuring the relevance and effectiveness of their standards efforts

All the resources mentioned above, however, have significant gaps. Although the resources by ENISA, CEN/CENELEC/ETSI, IEC and NIST point to many of the same standards, the differences between the lists in these documents indicates that there is no single authoritative resource. Further, there are a number of standards directly relevant to Smart Grid security that are not mentioned in any of the documents listed above, for example:

- Sandia Microgrid Reference Architecture (22)
- OASIS Cyberthreat Intelligence Technical Committee standards (23)
- OASIS Energy Interoperation Technical Committee standards (OpenADR) (24)
- EPRI/NESCOR Smart Grid Failure Scenarios (25)

There are also many standards that are less directly required for a secure Smart Grid but that should nonetheless be evaluated within a survey of the landscape, such as key management and cryptographic standards for encryption of AMI data, substation status information and so on.

The gaps in existing descriptions of the Smart Grid security standards landscape provide the context for the first of our recommendations regarding Smart Grid security standards:

Recommendation 1-1: ENISA should revise the existing EU-focused survey of Smart Grid security standards to provide information regarding all existing Smart Grid security standards applicable to the range of interests of EU Smart Grid stakeholders.

We believe the mandate for such a resource was given to ENISA by EU regulation 526/2013 Article 3.1d and can be effectively done in cooperation with CEN/CENELEC/ETSI (26). Although such a survey could be done jointly with NIST, given the work already done in NIST SP 1180R3, it is important that such a document should reflect the needs of an EU Smart Grid constituency and should therefore be separate from NIST SP 1180R3.

This recommendation will be discussed directly with ENISA by the SPARKS team. We should note that the SPARKS team has already provided feedback to NIST about gaps in SP 1180R3 as part of the review process for that document in May 2015; this feedback is provided in Appendix C of this document.

1.4 Gaps in Smart Grid Security Standards, Guidance and Tools

In reviewing existing standards (as we defined this term above) related to Smart Grid security, we have identified gaps in several areas:

- **Clarifications** regarding using standards related to Smart Grid security
- **Specification** of security-related aspects of processes, protocols, or interfaces
- **Guidance** regarding effective risk management, architecture, design, implementation and validation of Smart Grid security
- **Adoption**, implementation and use of standards, or sub-sets of standards, related to Smart Grid security

As already indicated by the documents referenced in the previous section, the standards landscape relevant to Smart Grid in general and to Smart Grid security in particular is extensive and extremely diverse. In order to help the Smart Grid community understand and make use of these standards, documents and on-line tools have been developed by various organizations that provide standards-related **clarifications**.

For example, the CLUSIF document "Cyber Security for Industrial Control Systems" provides a table of recommended standards for implementation and other purposes, shown in Figure 1 (27).

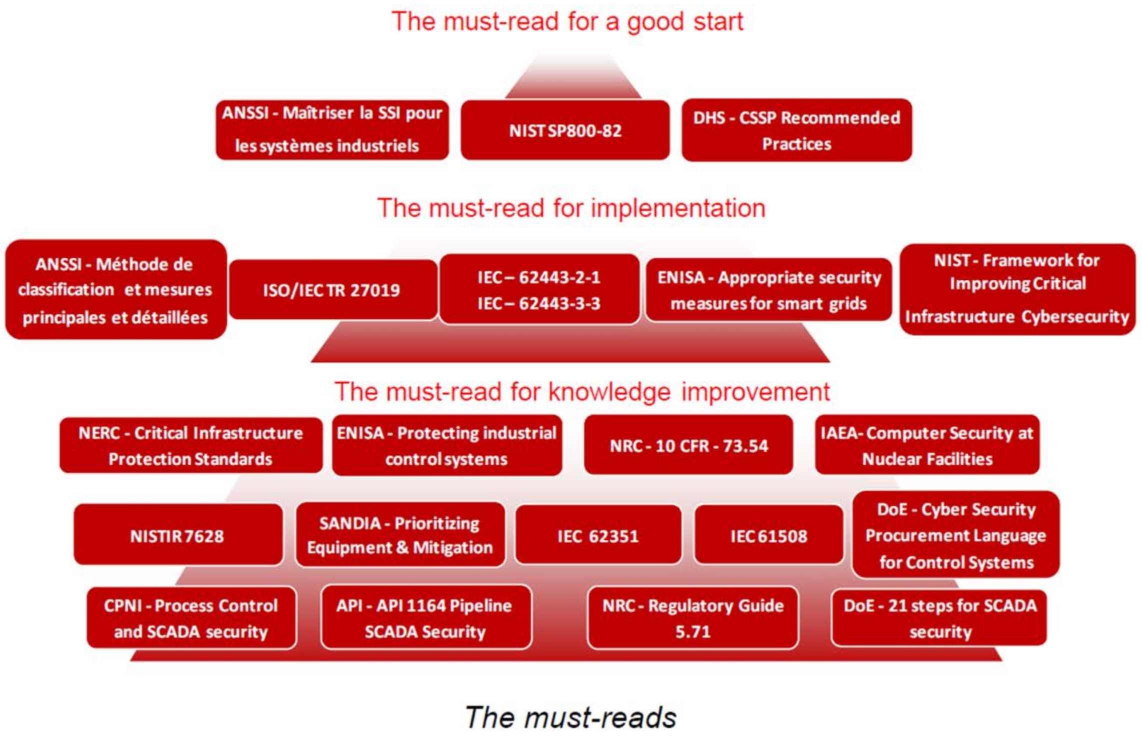
The must-read for a good start
ANSSI - Maîtriser la SSI pour les systèmes industriels
NIST SP800-82
DHS - CSSP Recommended Practices
The must-read for implementation
ANSSI - Méthode de classification et mesures principales et détaillées
ISO/IEC TR 27019
IEC – 62443-2-1
IEC – 62443-3-3
ENISA - Appropriate security measures for smart grids
NIST - Framework for Improving Critical Infrastructure Cybersecurity
The must-read for knowledge improvement
NERC - Critical Infrastructure Protection Standards
ENISA - Protecting industrial control systems
NRC - 10 CFR - 73.54
IAEA- Computer Security at Nuclear Facilities
NISTIR 7628
SANDIA - Prioritizing Equipment & Mitigation
IEC 62351
IEC 61508
DoE - Cyber Security Procurement Language for Control Systems
CPNI - Process Control and SCADA security
API - API 1164 Pipeline SCADA Security
NRC - Regulatory Guide 5.71
DoE - 21 steps for SCADA security
The must-reads

Figure 1 CLUSiF List of Standards

The Chinese roadmap for Smart Grid standards lays out a specific program for addressing gaps in standards relevant to Smart Grid across a broad range of technology areas, from design methodology to power line transmission, substation design and operational control of large generation systems (28). Though security is discussed only briefly, with reference to ISO 27000 and IEC 15048, the roadmap shows the need for recommendations regarding what standards are relevant and how best to take advantage of them.

In Recommendation 1-1 above, we suggested a comprehensive documentation of the Smart Grid security standards landscape. Given the need for guidance related to Smart Grid security standards indicated by the resources discussed in this and the preceding section, we believe that first recommendation should be complemented by the following in support of clarifications of the Smart Grid security standards landscape:

Recommendation 1-2: Either as part of or as companion volume to the Smart Grid security standards survey, ENISA should provide comprehensive and usable recommendations regarding the relevance and effective use of the various standards to the various EU Smart Grid security stakeholders.

We believe that D3.2 of the SPARKS project is a useful example of how such recommendations can be provided. This recommendation, like Recommendation 1-1, will be discussed directly with ENISA by the SPARKS team.

As is immediately apparent from the CEN/CENELEC/ETSI, ENISA, IEC and NIST documents referenced in the preceding section, a very large body of standards already exist that provide technical **specifications** of protocols, interfaces and so on, including technical specifications for security. IEC 61850, for example, includes capabilities for authentication of entities participating in SCADA communication.

In reviewing Smart Grid security-related standards, we identified some technical specifications that exist but are not yet included in the ENISA or other documents, such as the OASIS CTI standards related to security information exchange mentioned earlier. We also identified what we believe are several areas in which existing technical standards should be reviewed and potentially revised. These gaps and the recommendations related to them are discussed in Section 5 of this document, relative to our SPARKS research on PUFs.

Many of the most important Smart Grid security-related standards provide **guidance** on how to manage risk, how to architect Smart Grid solutions and how to implement Smart Grid capabilities. As in D3.2, this guidance is sometimes related to effective use of standards. In other cases, take SGAM as an example, the standard itself is best viewed as a guide or a framework rather than a technical specification. In reviewing Smart Grid security-related standards, we saw a number of instances in which technologies such as security analytics are not yet mature enough for technical specification but which are important enough to warrant guidance in other resources.

Most of the sections in this document recommend enhancing a few core EU Smart Grid standards, such as SGAM, with guidance related to various processes and technologies of importance in SPARKS. Most importantly, we view guidance regarding architectural approaches to Smart Grid resilience as the single most critical gap; this issue is discussed in detail in Section 3.

Finally, some of the most important gaps related to Smart Grid security standards pertain to the **adoption** and implementation of existing standards. Many of the recommendations in the 2011 ENISA report "Protecting Industrial Control Systems: Recommendations for Europe and Member States" (29) pertain to this gap in adoption, rather than to gaps in specification or guidance. For example, the recommendations call for the creation of national and pan-European Industrial Control Systems (ICS) security strategies, the development of a Good Practices Guide on ICS security and the establishment ICS-computer emergency response capabilities – all of which are facilitated and supported by adoption and implementation of existing standards.

Subsequent sections of this document will identify several areas in which adoption of security-related aspects of existing standards is the critical gap, particularly in the discussion of IEC 61850 in Section 4 of this document. More importantly, we believe that adoption is one of the critical issues relative to Smart Grid related standards, along with effective risk management, which is discussed in the next section.

2 Risk Assessment and Management Standards for Smart Grid

2.1 Critical Issues and Gaps in Existing Risk Assessment and Management Standards

As discussed in the deliverables for SPARKS Work Package 2 (WP2), the SPARKS team sees risk assessment and management as essential to cybersecurity for the Smart Grid: "It is important to understand the cybersecurity risks to the Smart Grid, so that well founded security requirements and controls can be identified and implemented" (30). In developing these deliverables, the SPARKS team began by reviewing existing risk assessment and management standards, to enable building on the substantial work that has already been done in the area of risk assessment management for Smart Grid. That review, however, found a number of significant gaps with respect to risk assessment and risk management for Smart Grid. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment identified five significant challenges in Smart Grid risk assessment:

1. *Juxtaposing safety and security risks*. "Although these two classes of analysis methods are mature, their combined use to understand the safety related incidents that could emerge from cyber-attacks is still in its infancy." (31)

2. *Recognizing cyber-physical risks*. "The fact that smart grids are cyber-physical systems has two major implications for risk assessment: In addition to the cyber threats and vulnerabilities that must be considered, physical risks must also be assessed. … Furthermore, the physical impact of a cyber-attack must be assessed in terms of disturbance to the energy supply." (32)

3. *Addressing risks to legacy systems*. "Collaboration of old and new [systems] should be taken into account while assessing risks on Smart Grids. … limited passive tests [may be] the only means of risk assessment … the impact of the introduction of new systems on legacy ones and [vice versa] must be assessed." (33)

4. *Accommodating complex organizational dependencies*. "Determining which organization shoulders the responsibility of the risk burden can be difficult." (34)

5. *Perceiving cascading effects*. "Incidents in one subsystem of a Smart Grid have the potential to cause cascading effects resulting in failures in the other subsystems."(35)

The SPARKS team determined that no existing risk management methodology and tool set addressed these challenges. D2.2 Threat and Risk Assessment Methodology, therefore, defines an effective Smart Grid Threat and Risk Assessment Methodology (abbreviated as SGTRAM in this document), tailoring the ISO/IEC 27005 information security risk management framework to the specific challenges of risk management for the Smart Grid. It also adapts the approach of consequence identification and impact assessment advocated by the SGIS working group, complementing that approach with other capabilities that address the challenge of identifying security requirements, recommendations and controls.

A methodology is most effective when supported by tools that automate, simplify and standardize the efforts of practitioners of that methodology. Consequently, WP2 also plans to deliver development tools which provide the requisite support. In addition, many aspects of the methodology are now supported through Governance, Risk and Compliance (GRC) vendor tools (36).

We believe the SGTRAM methodology addresses the challenges and gaps we have identified in standards related to risk assessment and management for the Smart Grid. We do not propose, therefore, enhancements to standards such as ISO/IEC 27005.

2.2 Recommendations regarding Smart Grid Risk Management Standards

One very significant challenge remains, however, the *widespread* use of a Smart Grid risk management methodology such as the one we have defined. Such use is necessary for the refinement of the methodology and related tools, the creation of a community of experts in the methodology and tools, and the development of a body of knowledge regarding the methodology and tools as they become more widely used. We have taken a number of actions to encourage the use of SGTRAM, including:

- Public availability of the D2.2 deliverable on the SPARKS project web site (37)
- Presentation of the methodology at SPARKS stakeholder workshops and project reviews (38)

- Discussion of the approach taken in SGTRAM in the Smart Grid Security book written by the SPARKS project team (39)
- Presentation of the approach taken in SGTRAM at industry conferences (40)

The SPARKS team will continue these kinds of dissemination activities. However, there are several actions that can be taken by ENISA and by ETSI/CEN/CENELEC that can significantly contribute to the widespread use of an effective Smart Grid risk assessment and management methodology, whether it is SGTRAM or another.

ENISA provides very useful online information regarding risk management and assessment methodologies (41). As already discussed, however, Smart Grids entail particular challenges that are not necessarily of concern in all risk management domains. Over the long term, it may be that profiles for applying risk management methodologies may be needed in order to help practitioners in various domains (telecommunications, process engineering, transportation, financial services, smart grid and so on) leverage well-established approaches such as ISO/IEC 27005 effectively. (The use of profiles to encourage adoption of technical standards is discussed in Section 4 of this document.) In the near-term, however, we suggest including SGTRAM in the list of risk assessment / management methodologies maintained by ENISA and pointing to it from the ENISA web pages related to Smart Grid.

Recommendation 2-1: ENISA should accept submission of SPARKS SGTRAM to the online inventory of risk management / assessment methods

One important mechanism for encouraging the use of methodologies such as SGTRAM is to provide mechanisms by which organizations can be certified in their use of a methodology and individuals can be certified in their expertise in a methodology. The need for certification schemes related to Smart Grid security, including risk assessment and management, has been discussed in ENISA's Smart Grid Security Certification in Europe: Challenges and Recommendations (42). Recommendations in that document include the creation of a steering committee to coordinate Smart Grid certification activities. Smart Grid risk assessment and management certification, at least at the organizational level, should be on the agenda for such a steering committee.

Recommendation 2-2: ENISA should consider SGTRAM as one of the requirements for future Smart Grid Security certification

Such consideration will likely identify areas for improvement of SGTRAM, both in methodology and tools, beyond the scope of the SPARKS project. It is our hope that this recommendation will encourage the adoption of further development of SGTRAM by an organization such as ETSI.

Over and above organizational certification, development of processes for certification of individual expertise is desirable. As has been the case with organizational certification schemes for ISO/IEC 9001, we believe the existence of such an organizational scheme for SGTRAM will serve as impetus for the development of programs for developing and certifying SGTRAM expertise at the individual level.

3 Security Architecture Standards for Smart Grid

3.1 Critical Issues and Gaps in Existing Security Architecture Standards

In the earlier deliverables for WP3, we focused on three families of resources as particularly valuable for developing a security architecture for a particular Smart Grid solution:

- NISTIR 7628 "Guidelines for Smart Grid Cybersecurity" (Volumes 1-3) and related resources (43)
- M/490 Smart Grid framework, including the Smart Grid Architecture Model (SGAM) and related resources (44)
- Sandia National Laboratories "Microgrid Security Reference Architecture" (MSRA) and related resources (45)

The first two of these sets of resources are widely recognized as essential tools in understanding Smart Grid security issues and tools, and then developing, evaluating or revising the security architecture for a particular Smart Grid environment. However, in reviewing these three sets of resources, we identified several important gaps in both the NISTIR 7628 resource family and the M/490 resource family. These gaps included concerns regarding 1) insufficient attention to alternatives for cryptographic identification of devices across a Smart Grid environment and 2) insufficient attention to security analytics as an essential capability for Smart Grid security, particularly in the light of targeted attacks that by-pass perimeter-based defensive mechanisms, as was the case in the recent cyberattack on electric grid in the Ukraine (46). Later sections of this document will discuss recommendations related to device identification (Section 5) and security analytics (Section 7).

We identified a more comprehensive gap in both NISTIR 7628 and M/490 resources, however, related to insufficient discussion of and consideration of microgrids, particularly as they relate to the critical issue of the resilience of the electric grid at local, national and international levels. As discussed in Section 2 above, in WP2 we have developed a risk management methodology that extends both the ISO 27000 risk management framework and the concepts of the SGIS Toolbox (though not employing the SGIS Toolbox directly) in order to assess risk not just in terms of threats, assets, vulnerabilities and impacts, but also in terms of the events that result from specific threats against specific assets using specific vulnerabilities that result in specific impacts. Among the most important of the events are those that result in disruption or destruction of power, potentially also in damage to property, financial loss and loss of life. We have also paid particular attention to these issues in WP5, as we look at the societal impact of attacks on the cyberphysical world of the Smart Grid.

As a result of our efforts across these and the other work packages, the consideration of cyber security for Smart Grid has led us to identify a critical need to address resilience in the architectural standards and related resources that are essential tools for developing effective Smart Grid security solutions in the EU. We therefore make the following general recommendation:

Recommendation 3-1: CEN/CENELEC/ETSI should incorporate resilience into SGAM through definition of resilience approaches, technologies, issues and trade-offs, including in terms of the use of microgrids in support of resilience in national and international grids.

The remainder of this section explores this recommendation in more detail, such as establishing a more comprehensive understanding of and approach to resilience, and in terms of including a specific exploration of microgrids and their relationship to resilience. This recommendation will be discussed with ENISA and appropriate next steps determined for discussion with CEN/CENELEC/ETSI.

The same issue with regard to resilience applies to NISTIR 7628. Though there is some discussion of continuous operation and of microgrids in NISTIR 7628 and related documents, it is not at sufficient depth to provide in-depth understanding of the issues, strategies and technologies related to Smart Grid resilience. The SPARKS team will draw this issue to the attention of NIST.

3.2 Defining Resilience for Smart Grid

One of the most prominent motivations for the development of a modern Smart Grid is to increase the resilience of the grid infrastructure. NISTIR 7628 mention power system availability (defined as *the power system resiliency to events potentially leading to outages*) and Microgrids (which introduce *increased resilience by aggregation and interconnection of independent microgrids*) as two out of four key concepts for the presented logical security architecture defined in section 2.2.1 of the standard document. Although the resilience of the grid infrastructure is predominantly used to motivate and structure the future Smart Grid architecture, all relevant standards lack a formal definition of resilience in cyber-physical systems in general and the Smart Grid specifically. Also more general standard documents like the ISO/IEC/IEEE 24765:2010 (47) that defines vocabulary for systems and software engineering disciplines does not include a formal definition of resilience in engineering domains.

This seems like a major shortcoming in existing standard documents as it is a source of ambiguity when domain experts interpret resiliency differently (e.g. resilience in ICT infrastructure could be understood differently than resilience of traditional power grids). We think that this shortcoming should be addressed in the existing standards and make Recommendation 3-2, relevant to the SPARKS project insofar as cybersecurity issues have a direct impact on resilience:

Recommendation 3-2: CEN/CENELCT/ETSI should include resilience, like interoperability, as a well-defined dimension that intersects with all SGAM domains and zones, incorporating this dimension into a revision of the CEN/CENELEC/ETSI Smart Grid Coordination Group's Smart Grid Reference Architecture document.

Existing literature has defined resilience in various domains. It was first defined by C. S. Hollings (48) for ecological systems and was later adapted for use in psychology (the ability to recover from trauma) and for the analysis of entities such as businesses or communities (e.g. their ability to recover from natural disaster). It was only more recently that resilience was also defined for classical engineering domains. Hollnagel et. al (49) define resiliency engineering in terms of an ability to change behaviour in response to the changing shapes of risk. Sterbenz et. al (50) define resilience for communication networks and provide a framework to manage resilient operation in networks as well as a metric to measure resilience as a function in a two dimensional space.

This research shows that the term *resilience* is applied in various domains and while the general interpretation is similar, a clarification of the exact interpretation in each domain is necessary. Today we can see that an exact definition of resilience is needed for cyber-physical systems.

Some approaches have been made toward defining resilience for cyber-physical systems. Rieger et. Al (51) defined resilient control systems as follows:

Definition 1: *A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.*

Another definition is given by Wei and Ji (52). They define resilient industrial control systems as follows:

Definition 2: *A resilient industrial control system (RICS) is the one that is designed and operated in a way that:*

1. *The incidence of undesirable incidents can be minimized;*
2. *Most of the undesirable incidents can be mitigated;*
3. *The adverse impacts of undesirable incidents can be minimized, if these incidents cannot be mitigated completely;*
4. *It can recover to normal operation in a short time.*

This definition is illustrated in the Resilience Curve diagram from Wei et al shown in Figure 2 (53). We use these definitions as a starting point to a more detailed discussions about the requirements of a standardized definition of resilience for the Smart Grid as well as the difficulties that we identified.

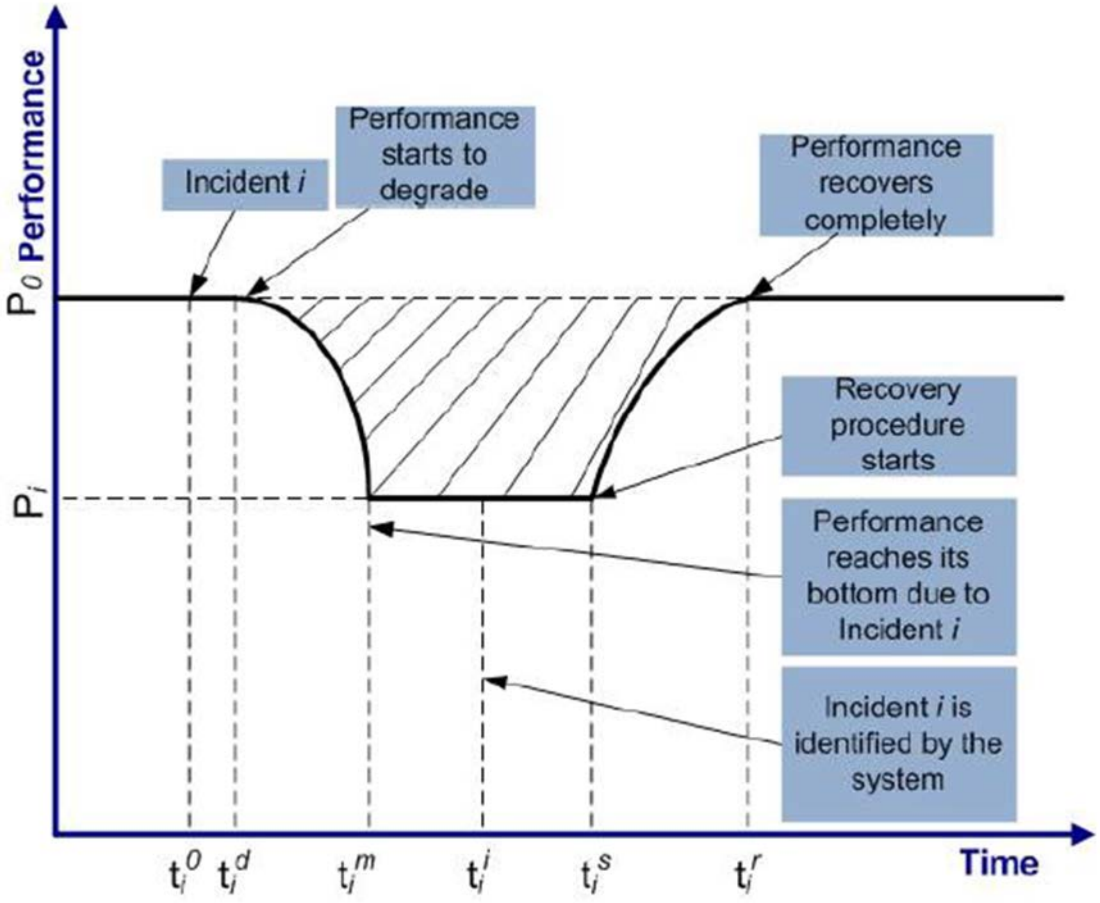

Figure 2 Resilience Curve

Figure 2 shows resilience as a function of system performance. The resilience is shown as the area between the performance curve and the nominal system performance P_0. Here a smaller area indicates higher system resilience. Based on Definition 2, the figure shows two main aspects of resilience. First, we define *robustness* as the ability of the system to withstand and mitigate disturbances. From Definition 1 we see that disturbances include unexpected (often random) as well as malicious (often intentional) threats to the system. The second aspect of resilience is *adaptability* which we define as the ability to gracefully degrade and recover in the face of disturbances.

Based on the previous definitions of resilience, improvements in those two system aspects are sufficient to improve system resilience. This does not, however, clarify what is meant by *performance*.

How is the performance of a Smart Grid measured? NISTIR 7628 identifies seven domains that build a modern Smart Grid. Is it a valid assumption that we can choose the performance in one domain to measure the overall system performance? Arguably the performance of the Transmission Domain cannot be used to measure the performance of Markets. Considering the SGAM model, the previous definitions of resilience seem even less meaningful as we have to consider interactions between all three dimensions of the model. We have already argued that performance in different domains is not comparable. But resilience is also an issue which slices through all five SGAM layers; how, for example, does the resilience of the Communication Layer influence the resilience of either the Component or the Information Layer?

Further, are *adaptability* and *robustness* equally relevant for all zones? It seems intuitive that robustness has more effect on resilience in the more isolated Process and Field zones, while resilience is more dependent on adaptability in the higher level Enterprise and Market zones. But this intuitive interpretation has still to be shown to be valid.

Considering the complexity of current efforts in standardizing security models for the Smart Grid, it becomes clear that the current definitions of resilience in this domain are too simple to be applied to these models. This is a problem not only for the security of the future Smart Grid but also for its motivation. As we can see in NISTIR, one main motivation behind the roll-out of Smart Grid technology is the assumption that these technologies increase the resilience of the infrastructure. This motivation is used, although no applicable definition of resilience exists for this new type of system.

Finally, it is not sufficient to consider resilience solely from a technical perspective. We have to extend our definition of events that may impact system performance by considering not only technical and environmental threats but also the socio-technical dimensions of the operational environment. As pointed out by Hollnagel in Resilience Engineering (54), complex cyber-physical systems are not static. The socio-technical context of the system introduces non-technical challenges that tend to transform the system into a state of higher risk over time. A resilient system needs to manage these challenges alongside the technical challenges.

Given these challenges, we make the following recommendation regarding the incorporation of resilience into SGAM:

Recommendation 3-3: Given the critical importance of resilience, CEN/CENELEC/ETSI should create a new SGAM Resilience Guide that provides best practices for resilience across traditional grid, hybrid grid and federated microgrid models for Smart Grid environments.

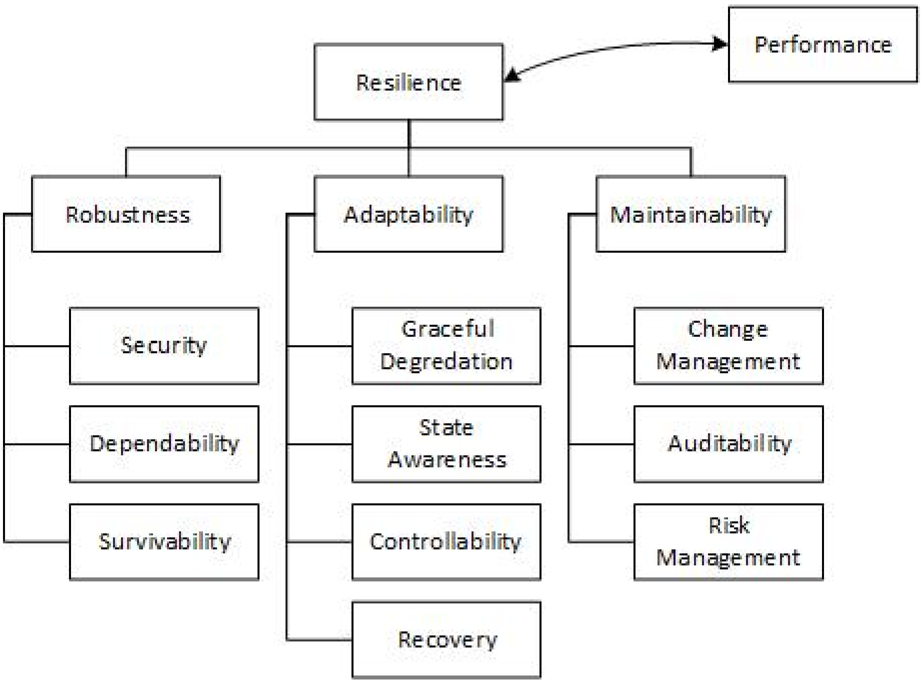

Figure 3 Aspects of resilience as proposed by SPARKS

Based on this analysis, we have identified three aspects of resilience that need to be considered in the D3.1 Smart Grid Reference Architecture document. These are:

1. **Robustness,** which deals with the diminishment of unwanted effects resulting from random or malicious challenges to the system. It is a property that is statically built into the system as part of the architecture and is the first layer of resilience.
2. **Adaptability,** which deals with the dynamic mitigation of unwanted effects resulting from random or malicious challenges to the system. This includes limiting the effects to a minimum while maintaining state awareness and controllability. It further includes the ability to recover to nominal operation once a challenge is mitigated.
3. **Maintainability,** which deals with long-term challenges to the system which can include both technical and social challenges to the resilience of the system.

Further, we agree with the widely accepted notion that resilience is a function of performance. But a widely accepted understanding of different flavours of performance in cyber-physical systems needs to be established. We believe that the three dimensional SGAM model is a good starting point to establish such an understanding across domains, zones and layers. Therefore we also make this recommendation with reference to defining resilience as a dimension in SGAM:

Recommendation 3-4: CEN/CENELEC/ETSI should provide clarification on robustness, adaptability, and maintainability as aspects of resilience, and should provide guidance on the intersection of cybersecurity and resilience, and the intersection of performance and resilience.

One such intersection is in the use of microgrids with Smart Grid solutions, discussed in the next section, in which the scale efficiencies of larger generation and distribution capabilities are balanced against the flexibility and resilience benefits that microgrids can provide.

3.3 Standardizing Microgrid Security Architectures for Smart Grid

There is a rapidly-growing body of information regarding microgrid architecture, much of which also covers, to varying extent, security concerns and capabilities. Of these resources, The Sandia Microgrid Security Reference Architecture (55) is the most security-focused, but many others, including the recent book on Microgrids: Architecture and Control by (56), provide significant discussions of security, particularly as a factor in the resilience of a microgrid.

Because of the insufficient consideration of microgrid capabilities in SGAM and NISTIR 7628, particularly as they relate to security and resilience requirements, we suggested using the Sandia document as a resource to complement the SGAM and NISTIR 7628 in our D3.2 publication. We have also followed-up on those suggestions in this document with Recommendation 3-3.

Although consideration of microgrids within the context of resilience is essential, it is not sufficient. As is indicated by the Sandia and Hatziargyriou texts, however, microgrid architecture is a challenging area, more so when aspects related to security and resiliency are considered core parts of the framework. Smart Grid practitioners in the EU need effective guidance for architecting and implementing microgrids, specifically within European environments, so that they can embrace microgrid approaches with confidence.

Therefore we recommend that, like resilience, microgrids should be the subject of a new resource provided as part of the SGAM family of resources.

Recommendation 3-5: CEN/CENELEC/ETSI should develop a new SGAM Microgrid Guide to provide detailed guidance regarding the architecture and implementation of microgrids, including considerations related to security and privacy.

Such guidance does not constitute a standard.

Given the relative immaturity of microgrids, there is still substantial discovery to be done. That development will help identify existing standards that are relevant, standards that should be evolved, and standards which may be required.

4 Protocol-Related Standards for Smart Grid Security

4.1 Critical Issues and Gaps in Existing Protocol-Related Standards

As already mentioned earlier, the SPARKS 2nd Stakeholder workshop in March 2015 included the demonstration of a cyber-attack on a Smart Grid system in which attackers used phishing to introduce malware into the IT infrastructure and then moved laterally into the SCADA environment (57). The malware then used a man-in-the-middle attack to manipulate messages being sent between a photovoltaic (PV) inverter and the SCADA human-machine interface (HMI) in order to change control values and to hide the actual PV output values from the HMI.

The communications between the HMI and PV used configurations of the protocol and communication services that are in very common usage in both older grid implementations and newer Smart Grid solutions. As called out by Kim et al (58), “many electric sector infrastructures were designed and installed decades ago with limited cybersecurity consideration”. Unfortunately, that is still very often the case today. As our SPARKS consortium members from Wunsiedel have experienced, all too often security capabilities that are available in or for use with standard protocols are not implemented by SCADA devices and HMI environments.

The standards community has worked toward addressing this problem, particularly in the case of ISO/IEC 61850, through the development of profiles. The “Security Profile for Advanced Metering Infrastructure”, for example, specifies PKI-based authentication of the communications channel used for 61850 messages in order to mitigate the risk of man-in-the-middle attacks (59).

A discussion of Smart Grid standards by the STARGRID Project (60) in January 2015 identified the ongoing need for profiles specifying secure operation of interface standards, calling out especially the extensive family of IEC standards specific to or relevant to Smart Grid. From the perspective of that report, coverage of standards across the technology landscape is not a problem; rather, the issue is in the effective application of standards, particularly because of the lack of profiles that provide the necessary guidance regarding the effective use of standards.

Development of such profiles was also a key recommendation in the Smart Grid standards guidance of the Standards Council of Canada (recommendation T&D2) (61). The report also called out the importance of the IEC 62351 and IEC 61850 standards and underlined the significant work to be done in maturing standards related to Smart Grid security. In that regard, the report recommended that Canadian Smart Grid stakeholders participate in the NIST Smart Grid Interoperability Panel (SGIP) in order to contribute to the standards being developed by NIST (recommendation P&S1).

An example of the implementation guidance required in order for standards to be effective is the Open Automated Demand Response Standard (OpenADR) conformance development process (62). OpenADR identifies standards that describe application programming interfaces to support interoperable communication between Smart Grid service providers and consumers, and also instantiates a process for certification of implementation conformance to these standards. OpenADR (see Figure 4) is developed under the auspices of the OpenADR Alliance (63).

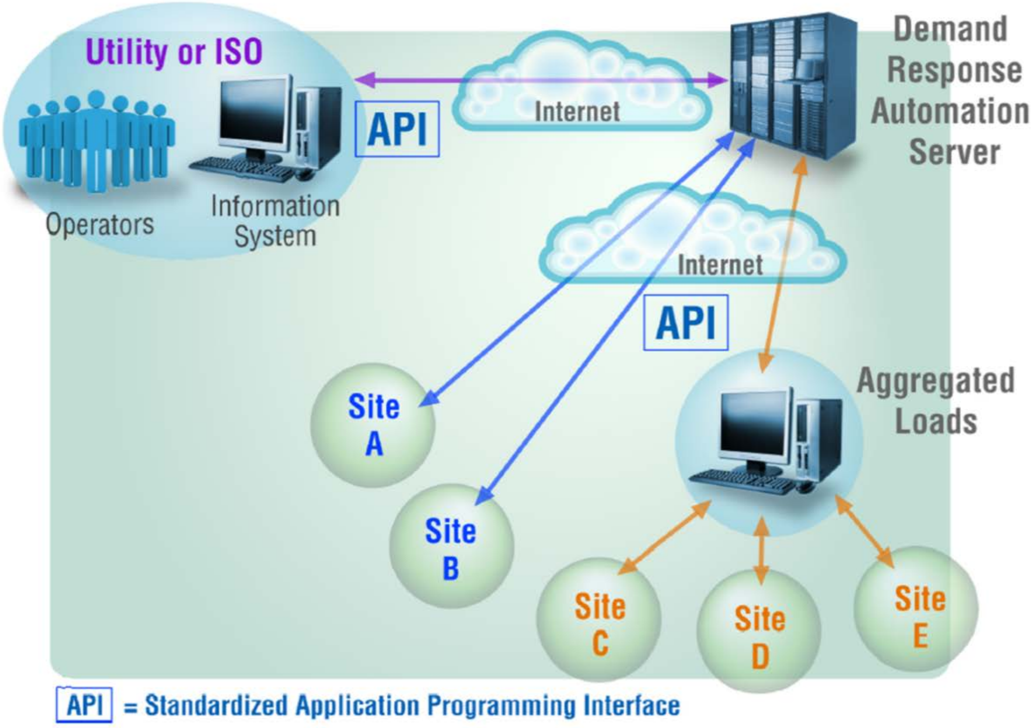

Figure 4 OpenADR

OpenADR provides a good illustration of what we believe is the most significant gap with regard to Smart Grid protocol standards; that is, the need for definition, adoption and certification processes for security-related profiles for these protocols. We certainly applaud the recommendations in the IEC Smart Grid Standardization Roadmap regarding enhancement of existing standards and development of new standards, including those related to security. But, as the IEC roadmap itself says, the issue of ensuring Smart Grid security is not just a question of protocol standards, but of the secure use of those standards within the Smart Grid: “technical requirements will not be sufficient to address the complexity of the Smart Grid” (64). We believe security-related profiles are an essential tool in the secure use of the protocols that have been and will be standardized.

4.2 Recommendations regarding Protocol-Related Standards

The SPARKS team believes that ENISA can play a major role in addressing the significant gaps in the secure use of protocol-related standards. First, there is a need to establish comparable guidance related to security profiles as has already been established for such areas as risk management methodologies. A similar inventory and guidance regarding security profiles for Smart Grid could be created by ENISA and made available within the framework of their current online environment.

Recommendation 4-1: ENISA should provide an online inventory and guidance regarding profiles for secure use of Smart Grid protocols such as the IEC 61850 family.

We believe that such an inventory and guidance can be created effectively by ENISA and made available within the framework of their current online environment.

Such an inventory will result in the identification of profile gaps, however this will provoke subsequent improvement cycles. Further, the guidance will drive certification processes that will encourage adoption of the best practices enabling organizations developing Smart Grid solutions to evaluate vendor components in terms of their security posture. We therefore suggest the following:

Recommendation 4-2: Based on the results of the above inventory, ENISA (potentially in collaboration with other organizations such as ISO/IEC) should include recommendations regarding profile and certification process development in an updated roadmap for Smart Grid security.

5 PUF-Related Standards for Smart Grid Security

5.1 Critical Issues and Gaps in Existing PUF-Related Standards

The SPARKS T4.2 mini-project is focused on investigating novel smart meter authentication and key management approaches based on Physical Unclonable Functions (PUF). Although there is significant research on PUFs and some instances of implementation (65), there is very little standards effort focused in this area. One such effort is the ISO/IEC project NP 20897 (66), approved as a project but not yet in draft, focused on security requirements, test and evaluation methods for PUFs. Such a standard for the evaluation of PUF security is important and the SPARKS consortium will monitor the progress of this standard.

A second gap in current standards is the definition of a reference architecture for the use of PUFs as a mechanism for generating device identifiers based on the inherent properties of a physical device, rather than on arbitrary identifiers associated with the device. Both symmetric and asymmetric key technology are widely used in Smart Grids for identification of physical and logical devices, including smart meters, sensors and controllers. The architecture described for Automated Metering

Infrastructure (AMI) in Ju et al (67) provides one such instance; PUFs can be readily integrated into such an architecture as the mechanism for key generation, as described in the SPARKS 1st Stakeholder Workshop (68). Once the feasibility of PUFs as a component of Smart Grid device authentication has been demonstrated, existing Smart Grid reference architectures will need to be updated with best practices for the use of PUFs for this purpose.

A third area of standards relevant to the use of PUFs in Smart Grid relates to key generation, distribution and management. Key management is an important topic in ISO/IEC 62351, including a specific discussion of device identification (69). ETSI has also provided an extensive discussion of key management standards relevant to Smart Grid in Technical Report 103118 (70). Though many of the standards mentioned are relevant to device identification using PUFs, none of the standards listed there, to our knowledge, discuss how PUFs can or should be used. Key distribution protocols from other standards organizations, such as the OASIS Key Management Interoperability Protocol (KMIP) (71), are applicable to the use of PUFs; for example, as a part of architectures in which information from PUFs is propagated to a key generation component. Within a reference architecture that includes the use of PUFs for device authentication, best practices and profiles will be needed relative to the key generation, distribution and management protocols that the architecture includes.

5.2 Recommendations regarding PUF-Related Standards

Based on the gaps discussed above, the SPARKS team makes the following recommendations regarding standards relevant to the use of PUFs within the Smart Grid environment.

Recommendation 5-1: The SPARKS team should monitor and, if appropriate, participate in the development of the IEC standard for PUF security requirements, test and evaluation that is the focus of ISO/IEC NP 20897.

Recommendation 5-2: ENISA should monitor the research on the use of PUFs for device authentication in Smart Grid environments and, if and when appropriate, work with standards organizations to include PUF-based approaches in security standards such as ISO/IEC 62351.

6 Smart Grid Security Standards Related to Security Analytics

6.1 Critical Issues and Gaps in Existing Analytics-Related Standards

There is increasing recognition of the importance of applying data analytics to the Smart Grid in order to detect and respond to cyber threats, evidenced by the publications and technology being developed in this area. The long history of applying analytics for operational purposes certainly contributes to the development of security analytics. But as discussed in SPARKS D3.1 Assessment of Reference Architectures, the standards landscape to security analytics in general, and to security analytics for Smart Grid in particular, remains relatively under-developed.

As called out in that deliverable, the first and most important gap is in the lack of discussion of security analytics in the various Smart Grid reference architectures. The CEN/CENELEC/ETSI model for Smart Grid security described in the Smart Grid Information Security (SGIS) standard does not include security analytics, though there is indication of the importance of analysis in the discussion of incident response (72). NISTIR 7628 mentions analytics for anomaly detection as a reason for log collection, but does not otherwise provide guidance regarding the role of security analytics in the framework described in that standard; security analytics is not included in the list of security technologies in Appendix B of that document (73). The Sandia Microgrid Security Reference Architecture mentions security analytics as part of a defence-in-depth strategy, but does so only in the context of forensic analysis, not anomaly detection (74). This neglect of security analytics in Smart Grid security reference architectures and guidance on Smart Grid security likely reflects the continuing dominance of a perimeter-based, preventative model for cyber security, as well as the relatively recent development of security analytics in general. Whatever the cause, this gap is the most important one in terms of security analytics and Smart Grid security standards.

Standards related to algorithms and methodologies for security analytics constitute a second important gap. ISO TC 69 has created a significant set of standards that provide guidance regarding the appropriate and effective use of statistical analysis techniques (75). For example ISO/TR 18532:2010 provides guidance on the application of statistical analysis methods to quality management in industrial systems (76). To our knowledge, no such guidance has been created by ISO or other standards organizations in the area of effective application of statistical methods or algorithmic approaches (such as clustering and segmentation) in security analytics, though there are certainly very valuable texts on this subject both from the academic community, such as the recent book by Carol Stimmel, (77) and from industry (78).

In SPARKS D3.2 Guidance for Smart Grid Security, the SPARKS team discussed the importance of the human-machine interface (HMI) to effective security for Smart Grid and identifies a number of existing standards related to HMI design, such as ISO11064-5. There is also guidance regarding HMI design, such as EEMUA Publication 201 (79). HMI is particularly important for security analytics; one of the most common problems with security analytics capabilities is flooding security personnel with unmanageable lists of potential security issues and incidents. As discussed in Stimmel (80), visualization capabilities are critical to making the results of security analysis actionable and effective. A CEN/CENELC presentation from 2014, for example, calls out a cybersecurity dashboard as an example of the Information Layer Mapping for SGAM (81). However, unlike the work being done in ISO EN13606 (82) regarding visualization for health information, no standards organization is currently addressing best practices for visualization of Smart Grid security information.

Finally, there continues to be significant issues caused by differences in formats of and interfaces for accessing the diverse data sets that are useful in security analytics for Smart Grid. The work being done by the OASIS Cyber Threat Intelligence Technical Committee on the TAXII, STIX and CYBOX standards is an important step in standardization of data format, particularly with regard to threats and incidents (83). However, the divergence in formats across the range of information useful for security analytics continues to be an issue. The Common Information Model (CIM) defined in ISO/IEC 61968 (84) may help ease this issue, although the impetus for this standard is to reduce the complexity of operational interfaces. The Multispeak Security specification (85), included in the 2014 version of the SGIP Catalog of Standards, is already widely used for interoperability related to operational interfaces, but specifies the format of the message, not the format of the message content.

6.2 Recommendations Regarding Security Analytics-Related Standards

As indicated above, the most immediate issue in the area of security analytics standards is the inclusion of security analytics within the most important reference architectures and guidance:

Recommendation 6-1: ENISA should work with CEN/CENELEC/ETSI to determine when and how to include security analytics within a revision of the Smart Grid Information Security (SGIS) standard and other relevant materials.

Although the standardization of the Human-Machine Interface for Smart Grid security is not yet feasible (and perhaps not desirable, given the importance of tailoring HMI to a particular environment), guidance regarding HMI for Smart Grid security would be valuable, particularly in terms of particular concerns in Europe relative to privacy. Given the role CEN/CENELEC/ETSI has taken with regard to Smart Grid architecture, they would also be an appropriate organization to provide guidance related to this area.

Recommendation 6-2: CEN/CENELEC/ETSI should develop a guidance related to Smart Grid security HMI.

At this time, security analytics is probably not yet sufficiently mature for consideration by ISO TC 69 or other organizations in terms of analytics methodologies and visualization techniques. However, the importance of sharing security information across and within organizations leads to a second recommendation:

Recommendation 6-3: The SPARKS team should continue to participate in the OASIS CTI Technical Committee and should include guidance regarding cyber threat and incident intelligence in future SPARKS deliverables related to security analytics.

7 Smart Grid Security Standards Related to Resilient Systems

7.1 Critical Issues and Gaps in Resilience-Related Standards

The importance of resilience as a consideration related to Smart Grid security has been discussed earlier in this document. The SPARKS T4.4 mini-project explores a particular aspect of this topic: the use of virtual sensors as a mechanism for improving the resilience of Smart Grids in the face of cyber-attacks.

Few publications related to virtual sensors in the academic and research community (other than by the SPARKS project participants) have called out the relevance of virtual sensors to Smart Grid; Kabadayi et al (86) are among the exceptions.

There is some standards activity related to virtual sensors. The Open Geospatial Consortium (OGC) have published the SensorML (87) standard which is a valuable resource in terms of enabling sensor webs. However, very little development has been done so far on the specification of profiles for the use of SensorML in various environments, including Smart Grid (88).

The potential use of virtual sensors as part of a larger Smart Grid resilience strategy has not yet been addressed in existing reference architectures and guidance from CEN/CENELC/ETSI or other standards organization. The opportunity for virtual sensors and sensor networks to contribute to resilience should be included in such standards, drawing on existing experience in such environments as the OGCNetwork (89).

7.2 Recommendations Regarding Resilience-Related Standards

As discussed in Section 2, resilience is of such importance to Smart Grid that it should be considered as a dimension of SGAM. Virtual sensors have the potential for a significant contribution in this area and should be included as a potential element of the resilience dimension.

Recommendation 7-1: In the resilience dimension of SGAM domains (recommended above to be included in a revision of the CEN/CENELEC/ETSI Smart Grid Coordination Group's Smart Grid Reference Architecture document and/or the SGAM Resilience Guide proposed above), CEN/CENELCT/ETSI should provide guidance regarding the use of virtual sensors in achieving resilience.

The SPARKS team can contribute to the acceptance of virtual sensors for Smart Grid not only through the SPARKS project deliverables and related publications, but also through engagement in the standards community.

Recommendation 7-2: The SPARKS team should consider engagement with OGS or other standards organizations addressing the use of virtual sensors in Industrial Control Systems in general and Smart Grid in particular.

8 Smart Grid Security Standards Related to Simulation and Modelling

8.1 Critical Issues and Gaps in Existing Simulation-Related Standards

In section 3 above, we discussed gaps and recommendations related to architectural models such as SGAM, including the need for significant enhancements related to resilience and microgrids. In this section, we consider standards related to the activities of modelling and simulation for the purposes of evaluating technological capabilities, understanding the impact of different cyber-attacks, demonstrating the effectiveness of particular design approaches, and so on. These kinds of activities have been discussed in a number of SPARKS results, including the presentation on "Modelling the Impacts on Microgrid Systems" and the simulation of a cyber-attack at the SPARKS 2nd Stakeholder Workshop (90).

Though there are many examples of modelling and simulation in academic literature, government-funded projects, vendor capabilities and industry publications, there is very little attention to Smart Grid simulation with the standards community. No standards specifically related to simulation and modelling (in the sense we are using in this section) are listed in NIST 1108R3 (91), the CEN/CENELEC/ETSI SGIS standards landscape (92), the ENISA survey of Smart Grid standards (93) or the ISO/IEC 62351 family of standards (94).

There are, however, several standards that are directly relevant to Smart Grid security simulation and modelling. The EPRI NESCOR description of Smart Grid failure scenarios is extremely valuable in providing a comprehensive set of scenarios that can be used as the basis for simulation and modelling of the impact of various attacks and of the effectiveness of different security-related processes and technologies (95). The SPARKS team has used the NESCOR scenarios in defining the simulated attack presented at the 2nd Stakeholder Workshop and has referenced the scenarios in a number of other deliverables. Valuable as the scenarios are, however, they have not yet achieved general adoption. Moreover, even these standard descriptions of security-related scenarios have gaps, particularly in terms of more complex attack scenarios that involve multiple inter-related impacts and cascading failures.

A second area in which standards exist relative to security-related simulation and modelling is in the specification of test environments, such as the NIST Smart Grid in a Room Simulator (SGRS) project (96). The ENISA Security Related Working Group, Standards and Initiatives report (97) provides an extensive list of standards organizations and activities related to test beds, simulation and modelling of cyberphysical systems, including Smart Grid. As indicated in the ENISA Smart Grid Certification in Europe: Challenges and Recommendations report (98), however, there does not yet exist an European specification for test beds related to Smart Grid security that would assist researchers in creating effective simulations and assist Smart Grid organizations in evaluating the results of simulation and modelling activities.

A third area in which standards exist relative to Smart Grid security are those sections of technical specifications that describe the testing requirements for demonstrating conformance. ISO/IEC 61850, for example, specifies not only the metrics to be applied, but also testing techniques that should be used (99). These specifications are extremely important in terms of evaluating not only the conformance of particular implementations to a standard, but also in the design of simulations that are analysing vulnerabilities and modelling attack scenarios. Most well-established technical standards, especially in areas such as protocols, have well-defined conformance specifications, though there may, nonetheless, be issues in terms of the implementation of the security aspects of these standards in vendor products.

8.2 Recommendations regarding Simulation-Related Standards

The EPRI NESCOR scenarios have proved invaluable to the SPARKS project in terms of both modelling and simulation. Though there are gaps that need to be addressed in the scenarios, we believe that they constitute the best resource for definition of simulation and modelling scenarios. Unfortunately they are not mentioned in important resources related to Smart Grid security simulation and modelling such as the ENISA report on Smart Grid certification mentioned above.

Recommendation 8-1: ENISA should consider adopting the EPRI NESCOR Smart Grid failure scenarios as a standard and reference it in guidance related to Smart Grid security testing, simulation, modelling and certification.

The SPARKS team fully supports the efforts that ENISA has already begun in terms of certification processes, including the inventory of simulation and modelling capabilities. We also fully support the definition of conformance requirements, metrics and techniques in all technical specifications related to Smart Grid security.

9 Conclusion

This document provides recommendations for improving standards related Smart Grid security across the major areas of focus in the SPARKS project, including recommendations both to ENISA and CEN/CENELEC/ETSI and also to the SPARKS project team. These recommendations are based on the gaps that have been identified so far in the course of the SPARKS project.

We have focused on those aspects of Smart Grid security standards that we believe have not been explored adequately in other discussions of Smart Grid standards. Our primary audience for this guidance is the individuals and organizations directly involved in Smart Grid standards development, as well as organizations (such as ENISA and CEN/CENELEC/ETSI) responsible for recommendations in this area for Europe.

Appendix A: Summary List of Recommendations

This section provides a list of recommendations made in this document.

Recommendation 1-1: ENISA should revise the existing EU-focused survey of Smart Grid security standards to provide information regarding all existing Smart Grid security standards applicable to the range of interests of EU Smart Grid stakeholders.

Recommendation 1-2: Either as part of or as companion volume to the Smart Grid security standards survey, ENISA should provide comprehensive and usable recommendations regarding the relevance and effective use of the various standards to the various EU Smart Grid security stakeholders.

Recommendation 2-1: ENISA should accept submission of SPARKS SGTRAM to the online inventory of risk management / assessment methods

Recommendation 2-2: ENISA should consider SGTRAM as one of the requirements for future Smart Grid Security certification

Recommendation 3-1: CEN/CENELEC/ETSI should incorporate resilience into SGAM through definition of resilience approaches, technologies, issues and trade-offs, including in terms of the use of microgrids in support of resilience in national and international grids.

Recommendation 3-2: CEN/CENELEC/ETSI should include resilience, like interoperability, as a well-defined dimension that intersects with all SGAM domains and zones, incorporating this dimension into a revision of the CEN/CENELEC/ETSI Smart Grid Coordination Group's Smart Grid Reference Architecture document.

Recommendation 3-3: Given the critical importance of resilience, CEN/CENELEC/ETSI should create a new SGAM Resilience Guide that provides best practices for resilience across traditional grid, hybrid grid and federated microgrid models for Smart Grid environments.

Recommendation 3-4: CEN/CENELEC/ETSI should provide clarification on robustness, adaptability, and maintainability as aspects of resilience, and should provide guidance on the intersection of cybersecurity and resilience, and the intersection of performance and resilience.

Recommendation 3-5: CEN/CENELEC/ETSI should develop a new SGAM Microgrid Guide to provide detailed guidance regarding the architecture and implementation of microgrids, including considerations related to security and privacy.

Recommendation 4-1: ENISA should provide an online inventory and guidance regarding profiles for secure use of Smart Grid protocols such as the IEC 61850 family.

Recommendation 4-2: Based on the results of the above inventory, ENISA (potentially in collaboration with other organizations such as ISO/IEC) should include recommendations regarding profile and certification process development in an updated roadmap for Smart Grid security.

Recommendation 5-1: The SPARKS team should monitor and, if appropriate, participate in the development of the IEC standard for PUF security requirements, test and evaluation that is the focus of ISO/IEC NP 20897.

Recommendation 5-2: ENISA should monitor the research on the use of PUFs for device authentication in Smart Grid environments and, if and when appropriate, work with standards organizations to include PUF-based approaches in security standards such as ISO/IEC 62351.

Recommendation 6-1: ENISA should work with CEN/CENELEC/ETSI to determine when and how to include security analytics within a revision of the Smart Grid Information Security (SGIS) standard and other relevant materials.

Recommendation 6-2: CEN/CENELEC/ETSI should develop a guidance related to Smart Grid security HMI.

Recommendation 6-3: The SPARKS team should continue to participate in the OASIS CTI Technical Committee and should include guidance regarding cyber threat and incident intelligence in future SPARKS deliverables related to security analytics.

Recommendation 7-1: In the resilience dimension of SGAM domains (recommended above to be included in a revision of the CEN/CENELEC/ETSI Smart Grid Coordination Group's Smart Grid Reference Architecture document and/or the SGAM Resilience Guide proposed above), CEN/CENELCT/ETSI should provide guidance regarding the use of virtual sensors in achieving resilience.

Recommendation 7-2: The SPARKS team should consider engagement with OGS or other standards organizations addressing the use of virtual sensors in Industrial Control Systems in general and Smart Grid in particular.

Recommendation 8-1: ENISA should consider adopting the EPRI NESCOR Smart Grid failure scenarios as a standard and reference it in guidance related to Smart Grid security testing, simulation, modelling and certification.

Appendix B: Additional Notes on National Guidelines in Germany

In addition to the recommendations in Figure 1, further “must-reads” in Germany include publications from the Federal Office for information Security, known as the BSI (Bundesamt für Sicherheit in der Informationstechnik) – see https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

Note also

- Selected BSI publications in English can be found at https://www.bsi.bund.de/EN/Publications/publications_node.html
- A link to the full publication BSI catalogue (in German) can be found at https://www.bsi.bund.de/DE/Home/home_node.html

Appendix C: Comments on NIST Special Publication 1108R3

Comments on NIST Special Publication 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

Submitted by the SPARKS Project team
30-May-2014

Contact:
Dr. Robert W. Griffin (Scientific and Technology Manager, SPARKS Project)
Robert.griffin@rsa.com
+41 79 196 4893

C.1 Executive Summary

The SPARKS (Smart Grid Protection against Cyber Attacks) project, a research initiative in Smart Grid security funded under the European Union FP7 program, offers the following comments and suggestions on draft NIST SP 1108R3. We would welcome the opportunity for discussion of these recommendations with NIST.

Release 3 of NIST SP 1108R3, like the preceding versions, contains very valuable and useful information. Identification of relevant standards and guidance regarding these standards has been identified as a clear priority by SPARKS stakeholders; the information in in NIST SP 1108R3 continues to extremely important is enabling Smart Grid constituencies not only in the USA but also in Europe to make informed and appropriate decisions regarding technical strategies for achieving Smart Grid security. The high-level discussions of Smart Grid architecture and risk management methodology are also very helpful for constituencies concerned about Smart Grid security. The SPARKS team appreciates the work represented by NIST SP 1108R3 and other NIST contributions to Smart Grid security and will be referencing and encouraging our stakeholders and constituencies to benefit from these resources.
However, the SPARKS team sees several areas that we hope you will consider addressing in your revision of NIST SP 1108R3:

- Additional relevant standards. There are several standards that do not appear to have been considered for this version of the special publication. We have included a list of several standards that we see as worth consideration.

- Additional standards to be developed. In addition to the areas identified in the special publication as requiring development of standards, there are several areas in which standards would be beneficial. We have included a list of these areas.

- Consideration of additional risk management methodologies. Although probability-based risk assessment and management approaches, such as in the RMP methodology referenced in section 6.3.3 and elsewhere in this draft of NIST SP 1108R3, is the most widely accepted approach in, there are a number of limitations in these approaches. We suggest at least referencing other approaches, as well consideration of supporting the development of these alternatives, particularly STAMP/STPA, into standards.

- Consideration of additional architectural components. In particular, the complementary role of security analytics to defensive mechanisms should be considered not only in terms of possible standards efforts but also as part of the high-level architecture referenced in SP 1108R3 and developed more fully in other NIST publications.

- Consideration of privacy concerns. Although privacy is referenced a number of times in the special publication, concerns regarding the intersection of privacy and security should be explicitly addressed both at a high level in SP 1108R3 and in detail in other NIST publications.

- Consideration of microgrids within the recommendations regarding testing and certification. The document calls out the importance of microgrids in Smart Grid solutions. We concur with this assessment and encourage NIST to give further attention to the role of microgrids in testing and certification.

Though some of these areas may represent areas of particular sensitivity in the European Union, we believe that addressing them will make this special publication of enhanced value to all its readers.

C.2 Recommendations

The SPARKS team offers the following recommendations regarding the framework and roadmap in NIST SP 1108R3.

C2.1 Additional Relevant Standards

There are several standards that do not appear to have been considered for this version of the special publications, particularly in terms of guidance related to analysing and responding to threats. Though they are not specifically Smart Grid standards, we see the following standards as worth consideration for inclusion in NIST SP 1108R3

- NIST SP 800-92: Guide to Computer Security Log Management
- NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations
- IEEE Foundation for Intelligent Physical Agents SC00097B http://fipa.org/specs/fipa00097/SC00097B.pdf

C2.2 Additional Standards to be Developed

In addition to the areas identified in the special publication as requiring development of standards, there are several areas in which standards would be beneficial.

- Information-sharing for Smart Grid. SP 1108R3 references several standards efforts related to on information sharing, particularly related to interoperation among meters However, there are a number of other areas in which information sharing is of critical importance, particularly regarding common formats for sharing of Smart Grid security incident information. Efforts such the IODEF effort in IETF, can serve as starting points for information-sharing efforts specific to Smart Grid. The TCG IF-MAP standard may also be worth consideration as a starting point for standardization regarding ingestion of information from a broad range of devices.

- Security Analytics for Smart Grid. To our knowledge, there are no standards efforts currently underway for security analytics, comparable (for example) to those provided by ASTM in areas such as chemical analysis. Leadership by NIST in the area of standards related to security analytics use cases, methods, algorithms and so on would be very valuable for security in general and for Smart Grid security in particular.

C2.3 Risk Management Methodology for Smart Grid

Draft Special Publication 1108R3 reinforces the focus on probability-based risk assessment and management methodologies, particularly RMP, as the recommended approach for Smart Grid. Section 6.3.3 contains the most detailed references to RMP and related documents. Neither in that section nor elsewhere, however, does 1108R3 mention alternative risk assessment and management methodologies.

We feel that there are important limitations in approaches such as RMP, and that consideration should be given to alternatives, particularly those derived from operational risk assessment, such as the STAMP/STPA methodology that is being developed under the leadership of Dr. Nancy Leveson of MIT (http://sunnyday.mit.edu/STAMP-publications.html). This top-down approach to risk assessment and management has significant benefits in terms of ensuring the broadest recognition of all loss, disruption and destructive impacts that should be understood and evaluated. NIST engagement in maturing this methodology should be considered in 1108R3.

C2.4 Smart Grid Security Architecture

Although NIST SP 1108R3 is not intended as a specification of Smart Grid architecture, the inclusion of the architectural framework within the document is very useful both as context for the standards recommendations and as high-level guidance towards achieving resilient, reliable and robust Smart Grid implementations. Although the intent of the architecture is clearly not to explore specific technologies, there are a number of places in which the omission of security considerations in general and of critical security capabilities in particular may set the wrong expectations regarding the role of security in Smart Grid. For example, the discussion of the legacy model in Figure 5.7 does not, to our knowledge, touch on the critical role of security within the Operations domain.

Similarly, the discussion of cybersecurity in section 6 dos not touch on the challenges related to employing security analytics within Smart Grid, including in the list of future activities. Though it is not the function of SP 1108R3 to discuss particular technologies, it appears to us that the identification of research and development in this area by NISTIR 7628 Vol. 3 (p 76) as a significant priority should be reflected in SP 1108R3.

C2.5 Smart Grid Privacy

Privacy is a major concern in European Union countries and increasingly in the USA as well. Although privacy is referenced a number of times in SP 1108R3, there is no discussion of even the highest-level regarding the architectural approach to ensuring privacy, for example Concerns regarding the intersection of privacy and security should be explicitly addressed at least at a high level in SP 1108R3.

C2.6 Expanding the Role of Microgrids in Testing and Certification

SP 1108R3 calls out the importance of microgrids in Smart Grid solutions. We concur with this assessment. That being the case, we encourage NIST to give further attention to the role of microgrids in testing and certification, as is indicated by the references to microgrid interoperability and testing in the Executive Summary (line 347 ff) which should be expanded in Section 7.

C3. The SPARKS Project

The SPARKS (Smart Grid Protection against Cyber Attacks) project is a research initiative in Smart Grid security funded under the European Union FP7 program, The technical activities that will be carried out in these work packages are focused on a number of key areas, with respect to securing the future smart grid: smart grid security analysis, including risk assessment; security architectures and standards for smart grids; and key smart grid security technologies, including resilient control systems, the use of Physically Unclonable Functions (PUFs) for smart meter (gateway) authentication; intrusion detection in SCADA systems, and the use of security analytics in smart grids. Associated with these technical aspects will is a socio-economic cost-benefit analysis, which indicates their ability to be deployed on real systems. Furthermore, European regulatory and legal requirements will be considered when developing the security solutions in the project. More information on SPARKS is available at https://project-sparks.eu/.

References

This section lists the citations in this document.

1. National Institute of Standards and Technology (NIST). Special Publication 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. 2014. Retrieved from http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf
2. ENISA Smart Grid Security: Smart Grid related standards, guidelines and regulatory documents. 2013. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view
3. CEN/CENELEC/ETSI Smart Grid Coordination Group. Smart Grid Information Security. 2014. Retrieved from ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf
4. SPARKS. D3.1 Assessment of Smart Grid Reference Architectures. 2015. Retrieved from http://project-sparks.eu/wp-content/uploads/2014/04/SPARKS-Smart-Grid-Reference-Architecture-White-Paper.pdf
5. SPARKS. D3.2 Guidance for Smart Grid Security. September 2015. Retrieved from http://project-sparks.eu/wp-content/uploads/2014/04/D-3-2_SmartGridSecurityGuidance.pdf
6. NISTIR 7628, Revision 1. “Guidelines for Smart Grid Cybersecurity, Volumes 1 – 3”. 2014. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
7. SPARKS. D2.2 Threat and Risk Assessment Methodology. 2015. Retrieved from http://project-sparks.eu/wp-content/uploads/2014/04/D2_2_Threat_and_Risk_Assessment_Methodology.pdf
8. Kim Cameron. “The Laws of Identity.” 2005. Retrieved from https://msdn.microsoft.com/en-us/library/ms996456.aspx
9. ENISA. Smart Grid Security: Smart Grid related standards, guidelines and regulatory documents. 2013. (see #2 above)
10. ENISA. Protecting Industrial Control Systems: Recommendations for Europe and Member States. 2011. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport
11. CEN/CENELEC/ETSI Smart Grid Coordination Group. Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. 2011. Retrieved from http://www.etsi.org/images/files/Report_CENCLCETSI_Standards_Smart_Grids.pdf
12. CEN/CENELEC/ETSI Smart Grid Coordination Group. Smart Grid Information Security. 2014. (see #3 above)
13. NIST Special Publication 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. 2014. (see #1 above)
14. http://www.nist.gov/smartgrid/catalog_of_standards.cfm
15. ISO/IEC. A List of Cybersecurity for Smart Grid Standards and Guidelines. 2013. Retrieved from http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf
16. http://www.iec.ch/smartgrid/mappingtool/
17. Sato, Takura et al. 2015. Smart Grid Standards: Specifications, Requirements, and Technologies. Wiley.

18. China SGCC. Framework and Roadmap for Strong Smart Grid Standards. 2012. Retrieved from http://esci-ksp.org/publication/sgcc-framework-and-roadmap-for-strong-smart-grid-standards/
19. SGEM project D1.3.1 "Smart Grid Standardization Analysis". 2010. Retrieved from http://clicinnovation.fi/publication/d1-3-1-smart-grid-standardization-analysis-version-2-0/
20. http://smartgrid.ieee.org/resources/standards/ieee-approved-proposed-standards-related-to-smart-grid
21. STARGRID. Standardization Recommendations. 2013. Retrieved from http://stargrid.eu .
22. Sandia National Laboratories. Microgrid Security Reference Architecture. 2012. Retrieved from http://prod.sandia.gov/techlib/access-control.cgi/2013/135472.pdf
23. https://www.oasis-open.org/committees/cti
24. https://www.oasis-open.org/committees/energyinterop
25. Electric Power Research Institute (EPRI). "National Electric Sector Cybersecurity Organization Resource (NESCOR)". 2015. Retrieved from http://smartgrid.epri.com/NESCOR.aspx
26. Discussed in ENISA. Securing Data in Cyberspace. 2014. Retrieved from https://www.enisa.europa.eu/publications/flash-notes/securing-data-in-cyber-space
27. CLUSIF. Cyber Security of Industrial Control systems. 2014 p 14. Retrieved from https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Cyber-Security-of-Industrial-Control-Systems.pdf
28. China SGCC. Framework and Roadmap for Strong Smart Grid Standards. 2012. (see #18 above)
29. ENISA. Protecting Industrial Control Systems: Recommendations for Europe and Member States. 2011. (see #10 above)
30. SPARKS. D2.2 Threat and Risk Assessment Methodology. 2015. P.6. (see #7 above)
31. SPARKS. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment. 2015. P.11.
32. SPARKS. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment. 2015. P.11.
33. SPARKS. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment. 2015. P.12.
34. SPARKS. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment. 2015. P.12.
35. SPARKS. D2.5 Preliminary Smart Grid Vulnerability and Risk Assessment. 2015. P.12.
36. For example, see RSA Archer 6.0 Operational Risk management. http://www.emc.com/security/rsa-archer-governance-risk-compliance/index.htm
37. http://project-sparks.eu/wp-content/uploads/2014/04/D2_2_Threat_and_Risk_Assessment_Methodology.pdf
38. https://project-sparks.eu/publications/deliverables/
39. Skopik, Florian et al. Smart Grid Security. 2015. Elsevier.
40. http://project-sparks.eu/wp-content/uploads/2014/04/comforen-cameraready-2015.pdf
41. https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods
42. ENISA. Smart Grid Security Certification in Europe: Challenges and Recommendations. 2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification/smart-grid-security-certification-in-europe/at_download/fullReport
43. NISTIR 7628, Revision 1. "Guidelines for Smart Grid Cybersecurity, Volumes 1 – 3". 2014. (see #6 above)

44. CEN-CENELEC-ETSI Smart Grid Coordination Group, "CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture". 2012. http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

45. Sandia National Laboratories. Microgrid Security Reference Architecture. 2012. (see #22 above)

46. Wired. "Everything we know about Ukraine power plant Hack". 2016. http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ and http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

47. Systems and software engineering -- Vocabulary. (2010). ISO/IEC/IEEE 24765:2010(E), 1–418. doi:10.1109/IEEESTD.2010.5733835.

48. C. S. Holling, Resilience and stability of ecological systems, Annual review of ecology and systematics (1973) 1-23.

49. Hollnagel, E., Woods, D. D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

50. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8), 1245–1265. doi:10.1016/j.comnet.2010.03.005

51. Rieger, C. G., Gertman, D. I., & McQueen, M. A. (2009). Resilient control systems: Next generation design research. In Human System Interactions, 2009. HSI '09. 2nd Conference on (pp. 632–636). doi:10.1109/HSI.2009.5091051

52. Wei, D., & Ji, K. (2010). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. In Resilient Control Systems (ISRCS), 2010 3rd International Symposium on (pp. 15–22). doi:10.1109/ISRCS.2010.5603480

53. Wei, D., & Ji, K. (2010). Resilient industrial control system (see #52 above).

54. Hollnagel, E., Woods, D. D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

55. Sandia National Laboratories. Microgrid Security Reference Architecture. 2012. (see #22 above)

56. Nikos Hatziargyriou. Microgrids: Architecture and Control. 2014. Wiley.

57. https://project-sparks.eu/events/2nd-sparks-stakeholder-workshop/

58. Kim, Jin et al. Implementation of Secure 68150 Communication. 2014. Retrieved from http://www.cired.net/publications/workshop2014/papers/CIRED2014WS_0322_final.pdf

59. The Advanced Security Acceleration Project. Security Profile for Advanced Metering Infrastructure. 2009. Retrieved from http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v2_0.pdf

60. STARGRID. Standardization Recommendations.2013 (see #21 above)

61. Standards Council of Canada. The Canadian Smart Grid Standards Roadmap. 2012. Retrieved from https://www.scc.ca/en/about-scc/publications/roadmaps/canadian-smart-grid-standards-roadmap

62. http://www.openadr.org/specification

63. Ghjalikar, Girish et al. Smart Grid Standards and Systems Interoperability: A Precedent with OpenADR. 2011. p. 1. Retrieved from http://drrc.lbl.gov/sites/all/files/LBNL-5273E.pdf

64. SMB Smart Grid strategic Group. IEC Smart Grid Standardization Roadmap. 2010. P. 35. Retrieved from http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf

65. Example of using PUFs for Smart Meter security by NXP https://www.intrinsic-id.com/nxp-strengthens-smartmx2-security-chips-with-puf-anti-cloning-technology/

66. ISO IEC NP 20897. Security requirement, test and evaluation methods for physically unclonable functions for generating nonstored security parameters http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=69403

67. Ju, Scongho et al. "Security Architecture for Advanced Metering Infrastructure". 2013. Retrieved from http://www.acsij.org/documents/v2i3/ACSIJ-2013-2-3-167.pdf

68. Dr. Martin Hutle. "Smart meter (gateway) authentication and key management using hardware PUFs". 2013. Retrieved from https://project-sparks.eu/wp-content/uploads/2014/04/sparks-smart-meter-gateway-puf.pdf

69. ISO/IEC 62351-9. 2012. Retrieved from http://www.iec.ch/smartgrid/standards/

70. ETSI, Technical Report 103118: Machine to Machine Communications (M2M); Smart Energy infrastructures security; Review of existing security measures and convergence investigations. 2015. Retrieved from https://www.etsi.org/deliver/etsi_tr/103100_103199/103118/01.01.01_60/tr_103118v010101p.pdf

71. https://www.oasis-open.org/committees/kmip

72. CEN/CENELEC/ETSI Smart Grid Coordination Group. Smart Grid Information Security. 2014. (see #3 above)

73. NISTIR 7628, Revision 1. "Guidelines for Smart Grid Cybersecurity, Volumes 1 – 3". 2014. (see #6 above)

74. Sandia National Laboratories. Microgrid Security Reference Architecture. 2012. (see #22 above)

75. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=49742

76. ISO TR 18532; Guidance on the application of statistical methods to quality and to industrial standardization. 2009. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51651

77. Stimmel, Carol. Big Data Analytics Strategies for the Smart Grid. 2014. Auerbach

78. EMC Education Services. Data Science and Big Data Analytics. 2015. https://education.emc.com/guest/campaign/data_science.aspx

79. EEMUA. Publication 201 Process plant control desks utilising human-computer interfaces: a guide to design, operational and human-computer interface issues. 2010. http://www.eemua.org/Products/Publications/Print/EEMUA-Publication-201.aspx

80. Stimmel, Carol. Big Data Analytics Strategies for the Smart Grid. P. 188 (see #77 above)

81. Schmiit, Laurent. "New ICT Architectures for Smart Cities". 2014. Retrieved from http://africasmartgridforum2014.org/fr/expert/sessionb3/laurent-schmitt-new-ict-architectures-forsmartiescities-en.pdf

82. http://www.en13606.org/the-ceniso-en13606-standard

83. https://www.oasis-open.org/committees/cti

84. IEC. IEC 61968 Common Interface Standard. 2003 Retrieved from http://www.iec.ch/smartgrid/standards/

85. SGIP. "Multispeak™ Version 3.0 and MultiSpeak Security Version 1 Approved as Entries to SGIP Catalog of Standards." 2014. Retrieved from http://www.sgip.org/SGIP/files/ccLibraryFiles/Filename/000000000637/SGIP_June2014_Newsletter.pdf

86. Kabadayi, Sanem et all. Virtual Sensors; Abstracting Data from Physical Sensors. 2006.. http://mpc.ece.utexas.edu/Papers/TR-UTEDGE-2006-001.pdf

87. http://www.opengeospatial.org/standards/sensorml

88. Ilic,Marija. Smart Grid in a Room. 2014. Retrieved from http://www.nist.gov/smartgrid/upload/Ilic_NIST-TEChallenge-091015.pdf

89. http://www.ogcnetwork.net/

90. https://project-sparks.eu/events/2nd-sparks-stakeholder-workshop/

91. NIST Special Publication 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. 2014. (see #1 above)

92. CEN/CENELEC/ETSI Smart Grid Coordination Group. Smart Grid Information Security. 2014. (see #3 above)

93. ENISA. Smart Grid Security: Smart Grid related standards, guidelines and regulatory documents. 2013. (see #2 above)

94. ISO/IEC. A List of Cybersecurity for Smart Grid Standards and Guidelines. 2013 (see #15 above)

95. Electric Power Research Institute (EPRI). “National Electric Sector Cybersecurity Organization Resource (NESCOR)”. 2015. (see #25 above)

96. Ilic,Marija. Smart Grid in a Room. 2014. (see #88 above)

97. ENISA Security Related Working Group: Standards and Initiatives 2013. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability/ics-security-related-working-groups-standards-and-initiatives

98. ENISA. ENISA Smart Grid Certification in Europe: Challenges and Recommendations. 2014. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification/smart-grid-security-certification-in-europe/at_download/fullReport

99. ISO/IEC 61850-10: Conformance Testing. 2012. Retrieved from http://www.iec.ch/smartgrid/standards/