Contract No 608224

Deliverable D3.2
Smart Grid Security Guidance

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 Guidance
Editor	Paul Murdock
Contributors	Ivo Friedberg, Robert Griffin, Martin Hutle, Lucie Langer, Silvio La Porta, Paul Murdock, Robert Ward,
Description	This document presents a consolidated view on security architectures for Smart Grids.
Requested deadline	30-Sep-2015

Executive Summary

This white paper, the second deliverable for SPARKS WP3, gives guidance that organizations can use in defining, designing and implementing security-related technologies, processes and organizational capabilities for Smart Grid environments.

We first offer guidance related to establishing an effective Smart Grid security architecture and build on the assessment of the Smart Grid reference architectures provided in the first deliverable for WP3. This includes explanations and recommendations related to three areas of security for Smart Grids that are not covered thoroughly in the NISTIR 7628 and SGAM reference architectures which we recommend as the starting material for establishing a Smart Grid architecture. The first of these areas concerns the use of microgrids in Smart Grid architectures, drawing particularly on work in this area by the U.S. Sandia National Laboratories and also combining information from a range of other sources. The second area is the use of security analytics as a core capability for detecting, analysing and responding to cyber-attacks. The third area concerns device authentication, in particular the use of PUF (Physically Unclonable Function) technology as a basis for unique identification of devices such as smart meters.

We next discuss several key issues in moving from architecture to the design of Smart Grid solutions, starting with a discussion of design methodologies. We then discuss the critical issue of integrating legacy and new technologies in a Smart Grid design. Additionally, we provide guidance related to Human Machine Interface (HMI) design, an area that we show to be important to the security and avoidance of human error in control systems in general and Smart Grids in particular.

The next topic we discuss is the use of modeling and simulation to validate architecture, design and implementation decisions. We review approaches and technologies for modeling and simulation of security and privacy in Smart Grid solutions, drawing on insights from the EU-funded CockpitCI project. We then discuss other areas of simulation that may be needed as a result of a Smart Grid design, such as performance modeling to understand the impact of the large-scale data collection in Smart Grid environments. We also show the importance of viewing modeling and simulation as an on-going, iterative activity rather than a one-time aspect of initial design and implementation.

Finally, we turn to guidance related to implementation, looking first at the “build versus buy” issue for the Smart Grid. We draw on significant research that has been done in this area, particularly by the Software Engineering Institute (SEI) at Carnegie Mellon University (U.S.), including the “Evolutionary Process for Integrating COTS-Based Systems” (EPIC) process defined by the SEI. We next discuss the critical importance of including design of processes, not just technology decisions, in architecture, design and implementation. We then review lessons that we believe can be learned from existing implementations, referencing both individual case studies and also the conclusions in this area provided in the ENISA 2012 report “Appropriate security measures for Smart Grids: Guidelines to assess the sophistication of security measures implementation”.

Table of Contents

Table of Figures

SPARKS Security Scrutiny Committee Assessment

This deliverable has been examined by the SPARKS Security Sensitivity Committee (SSC), in accordance with the process outlined in Deliverable D2.1 on SPARKS Security Management. According to the SPARKS Description of Work, this deliverable has a dissemination level of PU (Public). The SPARKS SSC understands there are no sensitive pieces of information contained within this deliverable that changes the level of risk relative to cyber-attacks.

Preface

In the first deliverable for SPARKS WP3, we focused on the assessment of Smart Grid reference architectures. In this second deliverable, intended for individuals and teams directly involved in Smart Grid implementations, we identify particular areas in which we believe guidance, best practices, new technologies or new insights on security process are needed in order to help Smart Grid organizations create secure environments. The goal of this deliverable is not to provide an exhaustive compendium of security-related guidance for the Smart Grid. Rather, we have focused on areas where we believe there are gaps in the guidance that is already available or that are of such importance that they deserve particular emphasis, as in the case of the discussion of the "build versus buy" decision in section 5 of this document.

Some of these gaps, particularly related to microgrids, security analytics and device authentication, were identified in the first deliverable. Other gaps, such as the integration of new and legacy technology, are well-recognized issues among Smart Grid practitioners. We have also discussed areas that until now have received relatively little discussion, particularly the area of Human Machine Interface (HMI) design as it relates specifically to the Smart Grid.

There are undoubtedly other areas in which security-related guidance is needed. But we believe this document provides the practical and pragmatic guidance needed by all of us working to create a more effective and secure Smart Grid.

1 Introduction

The previous deliverable for SPARKS Work Package 3, D3.1 Assessment of Smart Grid Reference Architectures, discusses a range of issues that are important in establishing an effective security architecture for a Smart Grid environment. These include the role of architecture within a secure development life cycle, as well as the importance of technologies such as security analytics and device identification. This document builds on D3.1 to discuss the process of establishing a security architecture for Smart Grid environments. It also introduces aspects that are not yet well-developed in industry standard references such as NISTIR 7628 [1]. It then discusses the process of applying the resulting guidelines to the design and implementation a Smart Grid security solution.

In systems as complex as the Smart Grid, it is valuable to establish an architecture that provides a longer-term and more durable understanding, its components and their interrelationship before commencing on a detailed design and implementation,. A good example of this is the California ISO "Smart Grid Roadmap and Architecture" first published in December 2010 [2] which describes a ten-year plan for implementing a Smart Grid at California ISO and maps that plan to an architectural model that describes the essential components of the system and the interaction between them. This includes defining the roadmap for instrumenting security within their Smart Grid solution as shown in Figure 1 from the California ISO Roadmap [3].

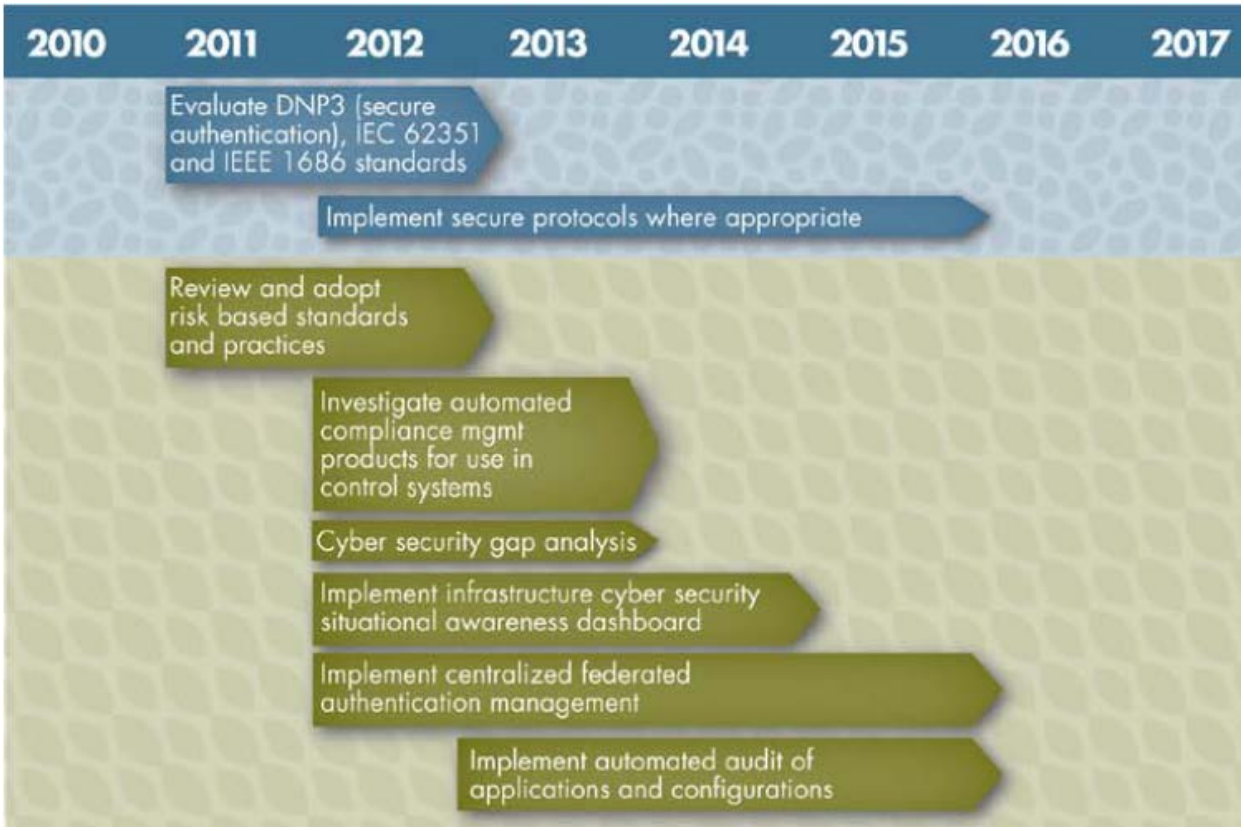

Figure 1 – California ISO Smart Grid Security Roadmap

In this roadmap, the implementation of various aspects of security, including authentication, situational awareness and audit processes, is preceded by evaluation of existing standards and strategies, identification of gaps and the development of architectural strategies that enable changes to existing systems while building and deploying enhancements to or replacements for existing capabilities. The constraint of adapting or replacing legacy systems is one that confronts most

organizations responsible for implementing Smart Grid solutions. Establishing the architecture for the solution can help significantly in managing that transition, both for the solution as a whole and in particular for the security-related aspects of that solution.

The California ISO architecture focuses on monitoring and analytics into a specific component. Such a component could be incorporated into the Energy Management System component in the NISTIR 7628 architecture. However, separating out the architectural level encourages consideration of a broad range of monitoring and analytics capabilities during the design process. For example, monitoring and analytics have been used to identify not only attacks within IT infrastructure but also fraudulent use of electric power, as discussed in the KEMA report on preventing energy theft [4].

The importance of monitoring and analytics has been touched on in D3.1 and is discussed in more detail in section 2.3.2 of this document. Although included in the California ISO architecture and roadmap, monitoring and analytics do not receive a great deal of attention in any of the reference architectures discussed in D3.1. The emergence of targeted attacks, however, has increased the importance of monitoring and analytics as a tool for the rapid detection of attacks that have succeeded in penetrating the defensive capabilities of a Smart Grid implementation. For example, monitoring can be used to detect attempted exploits targeting the communications infrastructure of a Smart Grid implementation. Enhancements of SCADA systems in power transmission networks by Energy Management Systems (EMS) provide system-wide monitoring capabilities that can detect anomalies resulting from a cyber-attack rather than to a component failure or malfunction.

D3.1 identified several gaps or limitations in each of the three Smart Grid reference architectures that an organization should be aware of as it applies the resources to their needs (NISTIR 7628, SGAM, MSRA). Some of these limitations in one architecture, such as the absence of microgrid architectural considerations in NISTIR 7628 and SGAM [5], are often addressed in another of the resources such as the Sandia “Microgrid Security Reference Architecture” (MSRA) [6]. However, there are several limitations that exist across all three architectures:

- Defining the role of monitoring and analytics in the security architecture
- Addressing the integration of legacy and new components
- Improving resistance to social engineering attacks

There are also emerging considerations related to recent advances in IT, particularly in terms of the integration of enterprise virtualization and cloud computing architectures with Smart Grid that, although not discussed above, are relevant to the development of a specific Smart Grid security architecture.

2 Establishing an Effective Smart Grid Security Architecture

2.1 Methodology

Architecture methodologies grow out of experience and generally derive from a deep understanding of context, concerns, reasoning, impacts, tools and technologies. Such understanding is often implicit and many architects build sound systems without conscious reference to any methodology. In these cases success derives from the architect’s experience of patterns, strategies and previous outcomes in a familiar domain. As pointed out by Tang et al. [7], the lack of explicit elaboration of methodologies

has been identified as an issue with some researchers making a case for improved methodology support.

The Smart Grid brings several disciplines together and the respective practitioners each bring a set of implicit and explicit methodologies to the table. The Smart Grid can also be seen as accelerating development of new disciplines - for example, big data management and analytics. Additionally, the emergent nature of the both the Smart Grid domain and of the security threats within that domain combine to make the methodological issues of Smart Grid security architecture very challenging

As discussed in the previous sections, Smart Grid reference architectures provide an indispensable resource for developing a Smart Grid security architecture applicable to the specific requirements, constraints and opportunities. NISTIR 7628, SGAM and the "Microgrid Security Reference Architecture" (MSRA) are particularly valuable in developing the specific architecture of a given Smart Grid environment. Both the roles of each of these reference architectures and their limitations are discussed in detail in the relevant sections of D3.1 which also focuses on how to apply the respective architectures. There are also a number of other valuable resources which explore the role of microgrids as a component of an architectural approach within the Smart Grid, such as the Considine paper [8].

2.2 Microgrids

Power and utility companies are facing a wide range of risks and challenges. These include risks to the physical resiliency of the grid infrastructure, challenges to the design and topology of that infrastructure and pressures on the underlying business models; see DOE [9] and Barrager [10]. Within this context, microgrids are seen as a significant part of both the challenge and the solution Degner [11].

2.2.1 Definitions

A microgrid is defined as a system which combines generation, storage and demand locally within a bounded, controlled network. Generation types typically include renewable energy sources as well as traditional backup generation such as fuel-powered generators or combined heat and power systems (CHP).

Various types of microgrids can be differentiated. One differentiation described by Considine et al. [12] highlights 5 types of microgrids:

1. **Industrial microgrids** are built to fulfil special requirements for high power and availability.
2. **Isolated microgrids** arise from the need for power in remote locations where the expense to expand power distribution does not pay off.
3. **Development microgrids** evolved in undeveloped countries where no distribution grid is available or accessible for a part of the population.
4. **Military microgrids** are developed to adjust to external factors in an insecure environment in order to ensure power supply.
5. **Motivational microgrids** are developed in well-supplied areas to integrate renewable energy sources or to improve the use of previous site-based energy initiatives.

Another classification is described in the "Maryland Resiliency Through Microgrids Task Force Report" [13]. This report focuses on industrial microgrids and motivational microgrids and describes the difference between campus style microgrids and public purpose microgrids. While a campus style microgrid serves a single customer on a single property, a public purpose microgrid (either operated

by existing power and utility companies or by third parties) serves multiple customers over property borders. Campus style microgrids raise fewer legal and technical issues while public purpose microgrids offer a more useful feature set when it comes to effective integration of renewable energy sources and resilient grid operation.

2.2.2 Resilience

One major motivation for microgrid-based grid architectures is their increased resilience. For instance, experience with severe storm damage to distribution infrastructure has shown the ability of microgrids to ensure local power supply well ahead of the main grid [14]. More strategic values can also be identified.

Microgrids cause segregation in the grid architecture. Isolation of faults and grid instabilities is therefore inherently supported by the architecture, as discussed in the Sandia "Microgrid Cyber Security Reference Architecture". Microgrids therefore play a valuable role in the isolation of Smart Grid capabilities in the event of cyber-attacks by minimizing the impact of cascades from one segment of a Smart Grid to another.

They can also provide important benefits in terms of the iterative adoption of new capabilities, including security capabilities, by reducing the risk of adverse impact across the entire grid solution in the case of installation or upgrade issues. Microgrids are also recognized as a key to increased energy efficiency without necessarily requiring investment in new transmission and distribution infrastructure [15]. Furthermore, microgrids can be designed to meet specific technical requirements of customers. This is of special interest for critical infrastructures that require significantly higher reliability levels than provided by the central grid.

2.2.3 Architectural Perspective

Microgrids can appear in various shapes and sizes. In their simplest form they consist of a generator to supply power, an end-user load, interconnecting cables and a transfer switch to separate or reconnect the microgrid from and to the central grid. The average microgrid is often more complex in order to meet customer demands. This diversity calls for best practices and standards for the execution of a microgrid project. IEEE 1547 [16] is a standard for interconnection of distributed resources and Electric Power Systems (EPS) that defines requirements on performance, operation, testing, safety and maintenance. IEEE 2030 [17] defines interoperability of Smart Grids and presents an interoperability reference model (SGIRM) that includes a knowledge base for developing microgrids.

The microgrid architecture consists of three different component types.

- Infrastructure components include, among others, transformers and automatic relays. These need to be configured according to the requirements of the surrounding central grid's distribution system in order to ensure safe operation.
- The types of generation components need to be decided. Microgrids can leverage a wide range of generation technologies.
- The third type of component – monitoring and control components – is the most critical for security considerations. Monitoring and control components help integrate the distributed devices of the microgrid and as such enable the microgrid to deliver the benefits described above. ICT infrastructure should already be considered during architectural decisions. Cyber security standards like the NERC CIP [18] requirements provide a good guideline during this process.

Standardized and well established communication protocols should also be used. Most communication protocols in the industrial control system domain (for example, DNP, Modbus and so on) do not involve any cyber security considerations. IEC 61850 [19] is a core Smart Grid standard that originally had the same limitations but has since advanced. The IEC 62351 series [20] provides cyber security considerations for these communication protocols with a special focus on IEC 61850. Extensions to standards that specify non-functional features are often left out of scope. That is why recent standardization efforts like IEC 61850-90-5 – an extension to IEC 61850 for synchro-phasor communication – includes security considerations in the core standard.

2.2.4 Operational Modes

What are the control tasks in each mode?

A microgrid can typically be operated in one of two modes. In the standard mode, the microgrid is connected to the main grid. In islanded mode, the microgrid is disconnected from the main grid and load is met by local generation or from local storage. Non-critical load can be intelligently shed in order that high priority assets remain energized. Depending on the microgrid architecture, islanded mode may be maintained only for a limited amount of time. The reason is that the power production from renewable energy sources often depends on the environment - for example, the weather or time of day. Environmental independent bulk generation sites are not accessible from the isolated microgrid to compensate for the loss of power generation caused by non-optimal environmental conditions. To bridge these shortcomings, microgrid architectures need to encompass power storage units. As mentioned above, a microgrid's capability to operate islanded can increase the resilience of the overall power network. In each operational mode, different control strategies are needed for the microgrid.

This has further implications for security and resilience that are not yet methodically laid out in existing security guidelines for Smart Grids such as NISTIR 7628 or SGAM . Sandia's "Microgrid Cyber Security Reference Architecture" (MSRA) is one document that tries to bridge the gap between existing guidelines for Smart Grids and the microgrid domain.

How is resilience affected by operational modes?

For architecture decisions, the differences in control between connected and islanded mode are of crucial importance. Two general grid architectures based on microgrids can be differentiated. In the first, microgrids are inactive for most of the operation. Control commands are received directly from the main control centre with local control entities acting as relays to the specific Intelligent Electronic Devices (IEDs). The microgrid is activated only if a power loss from the main grid is detected. In this case, when the microgrid becomes islanded, local control entities take over and the microgrid supplies the local loads. Once power supply from the main grid is established again, the microgrid hands back control and shuts down again.

The second architecture is termed a federation of microgrids. Here multiple microgrids are operated simultaneously thereby building a market. A central regulation authority controls the stability of the overall network. Optimization happens through financial incentives. Microgrids with unused storage capacity will buy energy when the price is low and sell stored energy when the price is high. As such they can act as buffer for renewable energy sources. As discussed in Barrager et al, this leads to the effective integration of small scale generation and storage devices [21].

What are the security implications?

A core architectural decision has to be taken between these two architectural approaches. This decision may have a big impact on further decisions on a specific microgrid architecture as well as on a resilient design. Concrete guidelines on how to approach these architectures are still unavailable to date. Sandia's "Microgrid Cyber Security Reference Architecture" does not address federated

microgrids and the resulting markets. Instead it focuses on independent microgrids to enhance resilience in fault situations on the main grid [22].

Power and utility companies are facing a wide range of new and emerging risks. One example concerns cyber-attacks. The increased use of ICT infrastructure in grid architectures opens up a new attack surface. As discussed in the Sandia "Microgrid Security Reference Architecture" referenced above, microgrids can play a valuable role in isolation of Smart Grid capabilities in the event of cyber-attacks, thus minimizing the cascade of impact from one segment of a Smart Grid to another. They can also provide important benefits in terms of the iterative adoption of new capabilities, including security capabilities, by reducing the risk of adverse impact across the whole of a grid solution in the case of installation or upgrade issues. Architectural models such as a federation of microgrids, as opposed to integration of microgrids in a heterogeneous grid/microgrid architecture, represent significant opportunities and decisions that are not yet explored in the methodologies behind NISTIR 7628 and SGAM.

2.3 Incorporating Analytics

2.3.1 Introduction to Security Information Analytics for Smart Grid

Most Smart Grid enterprises already monitor and analyse at least some of the sources of information discussed above for signs of unusual behaviour of people, applications, infrastructure, and communication. But often this analysis is focused on explicit indicators such as previously identified malware signatures or blacklisted IP addresses or domains. Sophisticated attackers can circumvent such static monitoring approaches by modifying malware signatures, by using virtual machines in the public cloud to obscure IP addresses lines, or by registering a new Internet domain as a command-and control or drop site.

Attackers typically operate by collecting information on the security systems and software installed on the target network. This allows them to test their malicious code and also to verify they will evade detection by the target network systems before launching an attack. It is much harder, however, for attackers to circumvent monitoring and analysis systems that are watching for unusual patterns and behaviors. Sooner or later, hostile malware or users must do something unusual that breaks with system norms, and that is when these kinds of analytic systems, often called "Intelligence-Driven Security", will detect them [23].

For example, when it comes to detecting malware, endpoint threat detection solutions do not look for "known bad" files; instead they look for suspicious behaviors. By comparing what is actually running in memory with what should be running based on the files residing on the local disk, malware detection tools are better able to identify discrepancies and obtain a direct, more reliable view of whether illicit code is present.

2.3.2 An Analytics Architecture for Smart Grid

Security analytics systems establish what "good" behavior looks like within an IT or control system environment by monitoring and learning a variety of machine and human activities, from what ports on servers are typically used for outside communications to employees' individual log-in locations and habits. Analytics solutions often rely on logs and configuration information as data sources. They can achieve far greater reach by also incorporating other sources. Figure 2 below shows an example of data integration and information exchange for operational and security analytics for a substation [24]. It includes the broad range of input sources described in Popovic's 2013 discussion of Smart Grid data analytics [25]. These input sources include digital protective relays (DPR), digital fault recorders

(DFR), digital disturbance recorders (DDR), sequence event recorders (SER), remote terminal units (RTU) and phase measurement units (PMU), as well as other sources.

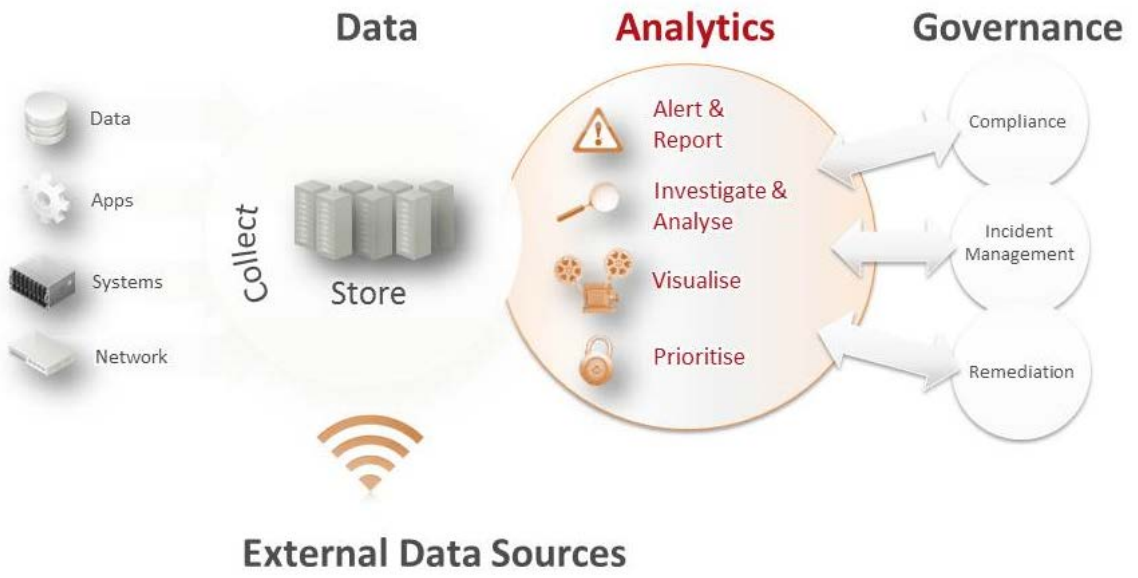

Figure 2 – Deriving Patterns of Normal Behavior for Substations

Similarly, capabilities such as network packet-capture are important in establishing normal behavior in the IT infrastructure. Full network packet-capture implies recording, parsing, normalizing, analyzing, and reassembling all data traffic at every layer of the network stack. As network traffic is captured, it is examined and tagged to facilitate subsequent threat analysis and investigation. Capturing and tagging network data enables security analysts to reconstruct users' sessions and activities to understand not just basic details such as what time or to which IP address specific data packets were transmitted, but exactly what information was sent in and out and the resulting damage. These techniques help organizations learn what is typical within an IT environment so that future deviations from normal can be identified and investigated as they arise.

With patterns of normal behavior in hand, activities outside the norm can be detected, analyzed and appropriately acted upon. For example, if an anomaly is flagged as a potential security issue, it can be passed to an analyst for further investigation. If the analyst determines that the event is a false positive, the analytics tools can learn from that experience so that they are less likely to flag future recurrences of that event as a potential security violation.

2.3.3 Capture, Stream and Batch Analytics

Analysis systems capture and process massive amounts of rapidly changing data from multiple sources. These may process terabytes of data in real time and are typically organized into various levels in order to enable different types of detection. For example, data can be captured and analysed for potential security issues as they traverse the network. This *capture time analysis* identifies suspicious activities by looking for the tools, services, communications and techniques often used by attackers without depending on logs, events, or signatures from other security systems. Examples of this capture time analysis include the detection of non-browser software programs running HTTP, protocols over non-traditional ports and executables embedded in PDF files. Additionally, these sophisticated tools can detect subtle signs of attack by correlating events that seem innocuous in

isolation but that are problematic when strung together. Analytical techniques combine internal inputs from various sources using metadata. These advanced detection mechanisms also act as trip-wires that can provide early warning of potential infiltration. Processing of these information flows happens as they occur, so that suspicious activities are spotted in time for security teams to stop attacks in progress.

This is comparable to the real-time operational response that is a fundamental capability in Smart Grid systems. Papers such as the California ISO Smart Grid Roadmap and Architecture describe the application of synchro-phasor technology in real-time fault isolation and remediation: “Phasor units measure voltage and electric current physical characteristics. This data can be used to assess and maintain system stability following a destabilizing event within and outside the ISO footprint, which includes alerting system operators to take action within seconds of a system event. This capability reduces the likelihood of an event causing widespread grid instability” [26]. Such capture time analysis is shown in Figure 4 of the Popovic paper [27], illustrating the extraction of phase current features to determine if a fault has occurred.

This kind of capture analysis and response is important in terms of real-time faults caused by cyber-attacks rather than natural disasters or equipment failure. The Aurora attack, in this case referring to the demonstration by Department of Homeland Security conducted at the Idaho National Laboratory (INL) in 2007, showed the creation of an out-of-phase condition that could damage alternating current (AC) equipment [28]. This attack forced the repeated opening and closing a circuit breaker or breakers to rapidly disconnect and reconnect an out-of-phase generator to the grid. Many circuits of utilities consist of various load profiles from resistive to inductive loads and these load profiles facilitate the kind of real-time failure demonstrated in Aurora. Analytics that detect the anomalous behavior in circuit breakers can enable automated responses that prevent equipment damage or worse.

Analysis systems can also perform *batch analysis* on large volumes of historical security data. In the case of security analytics, such data are needed not only to fulfil most companies’ data retention and audit requirements but they are also invaluable in uncovering adversarial tactics that may have taken many months to execute and may even be ongoing. For instance, batch analysis of security data archives can help uncover previously overlooked cyber-attacks in which illicit data was transmitted sporadically in small, stealthy streams over weeks or months. These types of “low and slow” attack techniques are hard to spot when they are occurring because they are designed to seem innocuous by taking cover under existing processes and communication streams. These techniques usually become evident only when executed in a particular pattern over a specific window of time. Detailed, automated analyses of security data archives can discover attackers in the midst of establishing a foothold. They can reveal information losses organizations may not even realize they sustained.

An example of batch analysis concerns the identification of compromised hosts through the use of large volumes of historical information in order to establish a pattern of normal behavior for hosts in an enterprise. This information is then reviewed to identify hosts that diverge from the pattern. For example, HTTPS packet data may be used as input. The security analytics tool looks for anomalous HTTP access, DNS lookups, accessed domains, traffic, users, IP addresses, beaconing activities, event timestamps and other network information. Using this information, the tool can create a ranked list of likely malicious IP addresses that require further investigation. Furthermore, the tool can create reports containing additional information regarding the IP addresses that can help in forensics and threat detection. The tool can then also search connections to IP addresses belonging to the same malicious IP subnet to identify other machines that require further investigation.

Batch analysis can also use rapid transitions in DNS addresses to identify potentially compromised hosts. In this case, DNS packet data is used as the input. The security analytics tool looks for

anomalous subdomains, users, IP addresses, ISP domains and other network information. Using this information, the tool can create a ranked list of likely fast-fluxing domains that are strong candidates for further investigation. The tool can also create reports containing historical visibility about each domain (for example, 30-day history) and additional information regarding the domain that can help in forensics and threat detection.

In summary, batch analyses can uncover attacker techniques and indicators of compromise that security teams can use in the future to detect similar attacks. More generally, batch analysis enables organizations to detect operational and security anomalies and reconstruct incidents with certainty and detail so they can investigate their losses and remediate problems faster and more effectively.

2.3.4 Taking Action

Advanced analytics tools examine the behavior of machines, networks and processes to determine whether they are subject to operational problems or have been compromised by malware. However, such tools do more than detect incidents; they can also assess risk and prioritize alerts.

Visibility and analytics enable effective action for recovery from incidents, remediation of vulnerabilities and mitigation of risk. For example, a cyber-attack launched via a compromised communication network against the circuit breakers in a substation may result in damage to transformers in the station. Because the disabled substation could result in loss of power for millions of customers, this is assessed as a high priority issue. Typically a response team springs into action and endeavours to restore power as quickly as possible.

Once the immediate problem has been fixed and power restored, remediation activity can help to determine how the attack occurred and whether there is a vulnerability that can be addressed to reduce the risk of similar attacks in the future. At the same time, a risk management team may investigate the failure scenario to determine whether there are mitigation strategies that would reduce the likelihood and impact of transformer failure.

Even in the best instrumented and most secure operational model, incidents have to be expected. The incident response system needs not only to prioritize the open incidents but also to eliminate false positives. New incidents should be automatically checked against a global repository of previously investigated items before being added to the pending queue. The incident response system should continually learn from these previous incidents, updated threat information, changes to operational configurations and other data sources in order to simplify the analyst's job as much as possible.

An incident response system should provide a rich set of contexts about prospective problems. For instance, for an incident related to a suspicious file that may represent malware (for example, a driver, a process or a dynamic linked library), the system should correlate suspicious behaviors about the file, capture what is known about the file (file size, file attributes, MD5 file hash and so on) through static and heuristic analysis and thus, provide context on the file owner or user and so on. Security analysts can then use this information to investigate if the file is malicious and should be blacklisted. If an item is deemed malicious, all occurrences of the problem across the entire IT environment can be instantly identified. Once a remedy is determined, the security operations team can perform any necessary forensics investigations and clean up the affected endpoints.

Incident response systems should also ingest information from external sources to enrich the organization's internal data sources for purposes of incident investigation and response. For example, the security analytics platform and management dashboard should aggregate the best and most relevant intelligence and context from inside and outside the organization to accelerate the analysts' decision making.

Remediation after malware infection is a complicated task. If a compromised machine is vital for system availability, it may not be possible to use previously saved machine images. The incident response team needs to check all the machine environments in order to remove all potential access points that attackers could utilize. Cyber criminals tend to use different entrenchment techniques in a victims' network. (The term entrenchment describes a technique that allows attackers to maintain unauthorized access into an enterprise network despite attempted remediation efforts by the victim). The victims' machine can be compromised in a variety of ways; for example the attackers might install web shells, add malicious or modified dynamic link libraries (DLLs) to running web servers, utilize remote desktop backdoors, hide malware that will commence malicious activity after a period of time and so on.

Determining whether there were vulnerabilities that contributed to the incident's occurrence or impact is also important. These vulnerabilities may have been technological, such as software vulnerabilities that provided access for an attacker or that caused unexpected behavior in operation of a component. There may also have been process issues that prevented an issue from being recognized until it had reached a critical level or that resulted in a failure condition. Alternatively, there may be organizational, educational or other issues related to the structure and people of the organization, such as individual vulnerability to social engineering attacks, that contribute to malware infections.

2.3.5 Mitigating Risk

Security information analytics for Smart Grid includes effective risk management disciplines, employing a broad range of factors to make probabilistic decisions about risk and take prioritized actions, including alerting the response teams. But an incident may also provide the opportunity to take actions to mitigate the risk associated with that incident.

Process integration is an important aspect of improving the impact and contributions of the employee community. It eliminates many routine steps, such as copying-and-pasting incident information, that go along with manually joining disparate security operations workflows. Integration also reduces opportunities for error, because activities for complex processes such as incident response can be programmed to follow a deterministic sequence of actions based on best practices. Finally, process integration can facilitate cooperation among different parts of the business—among audit, information security and compliance, for example—and help organizations create a unified view of conditions and risks throughout the organization.

This collaboration across the enterprise is essential in creating a culture of engagement that enables effective operations. Such a culture may have a dramatic impact on security as well by encouraging a personal commitment to security by every employee. While social engineering attacks continue to remain a significant threat, the awareness of individual responsibility for security can be a powerful force in helping each employee recognize and avoid responding to such phishing, pharming and vishing attacks.

2.4 Defining the Architectural Approach to Device Identification

Smart meters are anticipated to be relatively low cost and ubiquitous and will provide real time data analytics. However, the inherently embedded nature of these devices, coupled with a strong incentive for tampering by the customer, opens up a range of security issues. As discussed in the SPARKS deliverable D4.2, in order to resist unauthorized modification of these devices, a PUF device can be used to provide a low-cost layer of security within the existing PKI structure [29].

A PUF, or physically unclonable function, may be thought of as a unique physical object that provides an interface with the features of a mathematical function. The PUF has a physical structure that has been uniquely created in such a way that the function that it implements cannot be reproduced. Creating the physical structure of a PUF relies on random processes that take place during device manufacture. Given that the physical structure of a PUF instance cannot be exactly reproduced using the same manufacturing process, or in any other way, the PUF is effectively unclonable. Creating the physical structure of a PUF usually relies on random processes in order to obtain random physical properties defining the identity of the PUF. The randomness can be introduced either explicitly or using intrinsic randomness. Examples of explicitly introduced randomness are optical PUFs [30] and coating PUFs [31].

There are two main approaches to authentication based on PUFs. The first is to use established authentication protocols based on cryptographic algorithms where the required secret/private keys are provided by a PUF. The second approach is to use a PUF directly with a PUF-specific authentication protocol. D4.2 discusses in detail these and other issues in terms of using PUFs for smart meter authentication.

While there are still significant issues to be addressed, a Smart Grid architectural model should at least consider how to support the future introduction of smart meters based on PUFs such as the use of PKI infrastructure for device identification that will support the transparent replacement of existing smart meters with meters whose identification credentials are based on PUF technology.

3 Establishing an Effective Smart Grid Security Design

3.1 Design Approaches

When designing secure Smart Grids, there is no one-size-fits-all solution. Many existing implementations and Smart Grid pilot projects are tailored to the particular needs of Smart Grid stakeholders such as local Distributed System Operators (DSOs). However, certain best practices should be adhered to. For example, an emphasis should be placed on seamless interoperability between components from different vendors, in order to ensure Smart Grid components function correctly as part of an overall complex system.

At this point, Smart Grid reference architectures can play an important role. Consistent reference architectures help to unify the design process of secure Smart Grids and to define the minimum requirements for Smart Grid components. They can be used as a blueprint for developing a practical Smart Grid implementation. By instantiating parts of the reference architecture in a concrete implementation, a secure and interoperable Smart Grid solution can be developed in a consistent and efficient way. By considering security-by-design issues, it is possible to significantly reduce the attack surface and thus the risk from cyber-attacks targeted at critical control elements. At the same time, user acceptance can be enhanced by taking end-user requirements into account and following a privacy-by-design approach. Therefore we encourage the definition of Smart Grid reference architectures as a means of efficient Smart Grid security design.

While Smart Grid reference architectures will vary across different countries, a set of common properties can be defined at least as far as European grids are concerned. Existing methods and tools such as the SGAM Toolbox can be leveraged to define a secure Smart Grid reference architecture by populating the individual interoperability layers.

During the design phase, special focus has to be given to the supporting ICT system. Three different domains need to be considered during the design phase.

3.1.1 Network Layout

First, a secure network layout needs to be designed. In order to know the network requirements, security enclaves need to be designed. A security enclave is a set of logically and physically connected devices that fulfil a set of functions. Communications in and out of the enclave are possible only over a limited number of well-defined access points. A common approach is a 3-enclave design as used in industrial control systems. The three enclaves are the business network, a supervisory demilitarized zone and the control system. The problem with a limited number of enclaves is that they cannot sufficiently prevent lateral movement of attacks within the enclave. In order to achieve a higher level of security additional, finer grained enclaves may be defined. For example, it is common for business functionality, which is traditionally located in the office LAN, to require data from the control systems. This makes it difficult to design a single access point for traffic between enclaves.

In contrast, Knapp argues in his book “Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems” for a more detailed enclave design process [32]. This process starts by defining functional groups. A functional group is defined by all “assets (physical devices), systems (software and applications), users, protocols and other items” that are involved in the completion of a specific function. It is important to identify assets, protocols and applications separately. Every protocol supported by an asset that is not involved in the function under evaluation should be deactivated and the same holds true for unnecessary systems and users. The set of functional groups can easily grow enormous and a strict and secure separation in the form of security enclaves between all functional groups is probably not useful. Too many assets may be part of more than one functional group and as such need to support multiple protocols or provide access for various users from different groups. Therefore, functional groups need to be combined to establish sensible enclaves. Still, the previous assessment of functional groups helps as a guideline to disable unused access or not used protocols within an enclave. Furthermore, it is now possible to identify a limited set of required access points between enclaves.

Once the enclaves are decided upon, they need to be secured. Here the most restrictive security possible without limiting functionality should be applied. Perimeter defence systems such as firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be put into place at the various access points. These should restrict and analyse the traffic in and out of the security enclave. Furthermore, host-based security systems such as anti-virus, malware detection and host based IDS systems may also be installed within the enclave in order to limit lateral movement within it. The behaviour within an enclave can be monitored using anomaly detection tools and these can help identify insider threats as well as anomalous behaviour of components that are potentially infected with malware.

3.1.2 Protocols

In the design phase of the ICT network, the decision on the right protocols for different communication paths is critical. We have already argued that protocols need to be considered during the assessment of functional groups. There the main goal was to remove unused protocols in order to minimize the attack surface. Another decision concerns the choice of the right protocol for a specific communications link. Communication links between field devices are typically subject to low bandwidth. At the same time, commands at this level often have strict time requirements - for example if the command instructs a circuit breaker to trip. In order to avoid conflict between low bandwidth and strict time constraints, the communication protocol should not introduce additional overheads. The collection of measurement data by a concentrator on the other hand is not exposed to the same restrictions and can therefore make use of more complex protocols.

In order to fulfil the requirements of the low bandwidth link, low-level protocols such as Modbus or C37.118 are often used between field devices. The same protocols may also be applied within a substation network. There the communications between field devices and the controlling substations and also between different substations are transmitted. This may involve more complex protocols such as IEC61850 which are also used for substation communication with the control centre or for inter-control-centre communication. Choosing the right protocol is often effected by the communication medium and the type of the data sent (that is, is the functionality time critical or not).

In contrast to traditional industrial setups, the Smart Grid relies on device interoperability. With the increasing number of devices that are participating in the communication network, vendor independent standardized protocols are receiving more attention. But standards may come with their own risks. First, a given vendor specific implementation may not be completely compatible to the standard. Furthermore, standards often leave a certain degree of freedom for the implementation and hence the application of a standard protocol between devices from different vendors or between different implementations of a certain protocol may not always be straightforward. Standards focus on the technical challenge for the protocol regarding functional requirements of the supported features and commands. Non-functional features – especially security – are often left out of the standards and hence need to be actively considered in the design process of a Smart Grid. The IEC 62351 series is an example of a standard extension for cyber security in IEC 61850 and similar protocols. It is not automatically implemented when a device supports IEC 61850 and as such is often omitted. More recent Smart Grid protocol standards take a different approach. For example, the IEC 61850-90-5 extension includes data integrity features. Yan (2013) gives a good overview on communication infrastructures in Smart Grids with a special focus on the recent standardization efforts [33].

3.1.3 Component Security

With the increased connectivity enforced through the Smart Grid we also have to revaluate security at the device level. Many devices that are today air-gapped or hard-wired to a specific controller can obtain access through ICT networks. Therefore, each device needs to be evaluated based on the criticality of its functionality. One example concerns the increasing connectivity of protective relays. These devices are traditionally hard-wired to the transmission lines to detect fault situations such as over-voltage and to automatically isolate the fault. The ability to configure such devices remotely opens up a range of new attack vectors. To respect this trend and reflect the increased risk in the design process, this assessment needs to be fed back into the functional groups. A functional group (and with it the encompassing security enclave) can be seen as critical if it contains at least one critical asset. This has further implications on the security mechanisms in place at the respective enclave. It can further affect the enclave design. It might be useful to split an enclave into critical and non-critical parts in order to enforce proper security on the critical paths.

3.2 Key Issues in the Integration of Legacy and New Components

The transformation from our current power grid to a future Smart Grid containing new ICT components, thus enabling a greater degree of monitoring and control, will happen incrementally. Most components of the electrical grid have a lifecycle of 20 years or more, which means that our power supply will be provided by a combination of legacy systems and new components for the next decades. Both from a financial perspective and a risk management perspective, it is important to leverage legacy capabilities, using an evolutionary approach to building out a Smart Grid environment rather than creating one from scratch. As part of this iterative, dynamic process, new insights and strategies are incorporated as they emerge.

However, the nature and behavior of legacy components is very different from those of new ones. An example concerns the implementation of voltage control [34]. In legacy distribution grids, voltage control is enforced through controllers that remotely operate a limited number of actuators, such as tap-changer transformers and switched capacitor banks. The controllers' decisions are based on a few voltage measurements, typically taken at some of the end buses of the distribution lines which are often insufficient to provide a complete picture [35]. Legacy voltage control schemes with reduced observability and controllability require wider safety margins and operational constraints to prevent voltage collapse and this may lead to a less efficient use of the distribution grid. In Smart Grids, voltage control is supported by dedicated controllers and actuators, such as on-load tap changer transformers. These ICT-enabled components implement additional control loops that improve voltage controllability and observability, thus making grid operation more efficient but also much more complex [36].

A crucial distinctive feature of legacy components compared to smart components is that legacy grid components have mostly been operated in an isolated fashion without a connection to external communication networks. Also, these systems have been based on custom proprietary hardware and software, thereby providing a reasonable level of "security by obscurity". Consequently, they tend to provide limited or no cyber-security capabilities at all. Legacy control systems often run on old operating systems versions with archaic software which is not updated to support new operating systems or libraries because this would potentially expose them to unpatched vulnerabilities [37].

The relationship of legacy and new components has important implications not only in terms of the roll-out of a solution over time, but also in terms of understanding and responding to threats. In particular, understanding the integration of legacy and new components can affect decisions such as where to install sensors within the legacy environment that would in order to enable a greater degree of accuracy in identifying anomalies that could be attacks [38]. Given the large cost of securing legacy devices, the question of where to deploy modern equipment with enhanced cyber-security features is highly relevant. Knowing the answer enables the cost-efficient deployment of limited protection resources to increase the system's security [39]. The fact that the future power grid incorporates both legacy and novel components must therefore be considered also for Smart Grid risk assessment; efficient approaches that are able to deal with a complex combination of both are desirable but yet to be defined.

In this context, both the risk from legacy systems and the risk to legacy systems by introducing new sub-systems should be considered. In some cases, the different technologies may not interact, for example, because they use different protocols. When they do interact, there may be unclear security outcomes because of poorly documented legacy systems and such risks may be challenging to evaluate. Therefore, the first step towards addressing this challenge is developing a clear picture of the existing legacy systems, sub-systems and components in the electrical grid. The security risks associated with adding new sub-systems to the grid should then be examined while these are at a conceptual level. Such an analysis at design-time can help to identify topological vulnerabilities, and ensure that secure architectural decisions are made.

Alongside these forms of analysis, concrete threat and vulnerability assessment can be undertaken, for example, via penetration testing in order to understand the implementation-based risks that are related to legacy systems. However, it is widely understood that legacy industrial control systems can be fragile when subject to active vulnerability scanning. This can result in the need for manual procedures, thus increasing the complexity of Smart Grid risk assessment. Similarly, the limited possibilities to perform active security tests may require expensive testing facilities that represent copies of the operational infrastructure, or limited passive tests being realized that are based on eavesdropping communication, as discussed for example in Hecht et al. [40].

With regard to the efficient integration of legacy systems in Smart Grids, to the best of our knowledge there are no ready-made technological approaches available. It is, however, important to establish a

durable but flexible architecture that allows the gradual replacement of legacy capabilities. Smart Grid reference architectures can facilitate the planning of migration activities from legacy systems to future Smart Grid architectures and are therefore considered to be of great help regarding the challenge of integrating legacy components.

3.3 Human Machine Interface Issues, including operational risk related to human error

3.3.1 Introduction

Smart Grid technology is synonymous with the automation of the power infrastructure and brings with it the attendant advantages of improved energy efficiency, outage management, mobile workforce management and overall customer satisfaction among others. However, as with all automation projects, it is not possible to remove the human aspect completely out of the loop. The fact that automation is greatly increased in all Smart Grid implementations implies that it becomes even more important to understand how the interactions between the automated Smart Grid and the human component function together.

Even with the advent of automation, the utility control centre still plays a significant role. Control centre personnel are responsible for monitoring the grid, reacting to fault alarms, revision planning, management of customer requests, responding to requests for information and so on. Clearly, how these personnel interact with the automated technologies is important from the aspects of promoting efficiency, reliability and safety.

Therefore it is pertinent to consider how aspects of human psychology and behavior affect and are affected by automation technologies. Poor human-machine interface (HMI) designs have been implicated in creating or exacerbating operating errors thereby leading to deleterious situations as well as contributing to accidents and fatalities. World-wide, the associated financial costs run into billions of dollars *per annum*. This section describes HMI concerns from a wider perspective than that of the Smart Grid. However all large-scale industrial processing plants, power utilities and so forth share common issues when it comes to designing or evaluating a proper HMI

3.3.2 Background

It is not hard to find high profile examples in the literature illustrating how quickly and disastrously matters can go wrong when the interface between man and machine impedes a full understanding of the situation at hand, especially in the aeronautics, chemical and nuclear industries. The following two examples are representative.

3.3.2.1 Example 1 – Flight AF447

In general the avionics industry of today is regarded as being exemplary in its ability to design high-quality HMI implementations in the cockpit. However, the case below illustrates how even mature and well understood HMI principles may fall short when aircraft pilots are confronted with an unexpected and highly stressful situation.

On 1st June 2009 the Airbus 330-203 flight AF447 *en route* between Rio de Janeiro and Paris crashed into the Atlantic Ocean resulting in the deaths of 228 passengers and crew. The immediate cause of the crash was put down to the plane's Pitot tubes, which help to determine airspeed, freezing up in tropical storm conditions. In turn this caused the auto-pilot to disengage and hand over control to the pilots who were suddenly and unexpectedly confronted with flying the plane in difficult conditions. The final report on the crash was published three years after the accident and highlighted several issues relating to shortcomings in the human-machine interface [41]:

1. Because of the lack of any feedback mechanism from the stick controller on one side to that on the other, the PNF (pilot not flying) was oblivious to the fact that the PF tried to master the situation by continuously and erroneously attempting to bring the aircraft nose up, a fact which directly contributed to the plane's stalling.
2. Critical flight information, specifically the all-important angle of attack parameter, was not displayed directly to the pilots. Indeed the pilots probably remained unaware throughout the entire incident that the plane had stalled.
3. Multiple starts and stops of the aural stall warnings did not aid the flight crew in understanding their predicament.
4. There had been no pilot training for coping with unreliable airspeed indications at high altitude. The training for dealing with abnormal events such as this did not enable the crew to appreciate the "startle effect" generated by stall warnings, nor the reflex actions on the controls that may be induced.

In short, therefore, the HMI failed to display the necessary flight information and did not allow one pilot to know how the other was attempting to control the plane. The alarm mechanism did not contribute to the pilots' understanding of what had happened. The training procedures for dealing with such an emergency situation proved to be inadequate.

3.3.2.2 Example 2 – The Explosion at the Texaco Milford Haven Refinery

This example is a case of what can happen when a inadequately designed alarm mechanism fails to inform the plant operators of the true nature of a chemical processing plant and indeed hindered them from understanding what was happening.

On 24th July 1994 an explosion followed by a number of fires occurred at the Texaco refinery, Milford Haven, Great Britain. The official report into this accident drew attention to the following [42]:

1. The control room displays did not help the operators to understand what was happening.
2. There were too many alarms and they were poorly prioritized. In the last 11 minutes before the explosion, the operators had to acknowledge and act upon 275 alarm notifications.

3.3.3 Human-Machine Interface Design

Fortunately, and despite these two examples, HMI design is now a reasonably well-understood art and following best practices can go a long way to help mitigate such problems.

HMI design comprises several areas. The first and most obvious area is the design of the graphical interface itself. The overriding purpose of the HMI is to show relevant and necessary information while minimizing the potential of confusion. The key here is situation awareness and this is described briefly below.

Alert management is also an important concern. The purpose of an alarm is to draw attention to an abnormal condition requiring action and hence proper alert management also promotes situation awareness.

The ergonomic design of the control room is also a significant consideration. Lighting, thermal comfort, noise, vibration are all factors that can induce operator stress and fatigue which in turn can lead to unprovoked mistakes.

3.3.4 Overview of the Literature on HMI Design

Substantial literature on HMI design exists in the form of standards, guidelines and handbooks. The most useful documents in the field of HMI include the following:

- Standards:
  - ISO11064-5 – Ergonomic design of control centres — Part 5: Displays and controls [43]
  - ISA101 – Human-Machine Interfaces [44]
- Guidelines:
  - EEMUA 201 – Process plant control desks utilizing human-computer interfaces: a guide to design, operational and human-computer interface issues [45]
  - NUREG-0700 – Human-System Interface Design Review Guidelines [46]
  - ASM Consortium: 2013 Effective Console Operator HMI Design: Second Edition [47]
- Handbooks:
  - The High Performance HMI Handbook [48]
  - Human Factors in the Design and Evaluation of Central Control Room Operations [49]

These documents generally make similar points concerning graphical user-interface design. They differ in the level of detail they cover and in their specificity. The standards documents tend to be more concise and prescriptive. In their nature, they tend to concentrate on the minimum acceptable rather than the optimum. The ASM guidelines and HMI handbook contain helpful examples and explain the reasoning behind their recommendations. The NUREG document is somewhat impenetrable.

Other readily available documents (Gruhn [50], Hollified [51], Opto22 [52], ABB [53]) describe the principles of good user-interface design and generally emphasize the same points while also being quite readable. Acuite gives a useful summary of these standards and guidelines along with their respective strengths and weaknesses. [54]

3.3.4.1 Situation Awareness

A good HMI is one that promotes situation awareness. Gruhn describes situation awareness as being cognizant of what is currently happening, understanding what the provided information indicates now and what that information implies will happen in the future. He gives three levels of situation awareness:

1. Perception of provided data. That is, being aware of the status, attributes and dynamics of elements in the environment.
2. Comprehension of the current situation. This is based on a synthesis of the level 1 elements and a comparison of that information against the required objectives. Novices may not have the knowledge base to draw on and may be at a disadvantage when trying to develop Level 2 situation awareness.
3. Projection of future status. Prediction of the future status can only be achieved by having a good understanding of Level 2 situation awareness, along with a highly developed mental model of the system.

Factors that undermine situation awareness include attention tunneling (fixating on one set of information to the exclusion of others), data overload, complexity creep, incorrect mental models and out-of-the-loop syndrome.

3.3.4.2 Graphic Design Principles

Good graphic design clearly goes a long way to help build a good HMI implementation. The HMI standards and guidelines outlined above generally advocate the same principles including the following:

1. Use a functional depiction of the process rather than a schematic diagram.

   P&ID (piping and instrumentation drawings) are commonplace throughout the process industry and are a hangover from the early days of computer-automated process systems. They often depict a schematic diagram of a plant or power generator and this may not particularly help the operator understand the state of the system as a whole. Typically too much of the screen is taken up by a schematic depiction of the equipment, often in 3-D form. Data are displayed in a raw, numeric form which also does not aid the operator in understanding the overall state of the system: whether it is functioning properly (level 2 situation awareness) and whether any parameters are approaching hazardous levels (level 3 situation awareness).

2. Consistency in the design and layout

   Display layouts need to be consistent and appropriate to process behaviors. The presentation of information should follow explicit, consistent visual coding, navigation and layout schemes.

3. Robustness

   Where interface action is taken by the operator, the system should be designed so it can cope with incorrect key strokes or mouse clicks and so the operator can return to the original position if need be. Any significant change will require confirmation or duplication of the data.

4. Color should be used conservatively and consistently.

   Color is an important cue in human visual processing and can be used to draw attention to graphical elements. In order that the potential benefits not be lost, color should generally be used sparingly. However, it should be noted that color is not processed well in peripheral vision and so should be combined with other visual clues such as movement or blinking. Color may also induce eye-strain leading to operator fatigue. Finally, 8% of men and 1% of women have some form of color blindness. These factors should be taken into consideration when making use of color in graphical elements.

5. Use low-contrast layouts and grey backgrounds.

   A light grey background helps to reduce glare from room lighting. This also helps reduce visual “interference” and operator fatigue.

6. Depict important parameters and trends using analogue techniques

   Humans can process analogue symbols more quickly and more reliably than they can read raw, numeric values. Hence graphical elements such as bar charts are to be preferred over densely packed textual data.

7. Distinguish clearly between normal and abnormal values.

   This leads on from the previous point. Use of analogue graphical elements can help an operator easily see whether a given parameter has, say, exceeded or is approaching some threshold.

8. Provide context-sensitive navigation.

A hierarchy of display content including the ability to "drill down" (for example, using right-click menus) allows the operator to obtain additional information.

9. Use of symbols and process connections, choice of fonts and font sizes, layout and navigation are also important considerations.

10. Graphical techniques such as 3D objects, shading and animation should in general be avoided. As always, there are exceptions to all rules and such techniques may be used sparingly – for example, to draw the operator's attention to values that need to stand out.

3.3.5 Alarm Management

The proper management of alarms is a significant element of the overall HMI implementation. The Health and Safety Executive (HSE) run by the UK government makes the following statements concerning alarm management: [55]

1. Alarms should direct the operator's attention towards plant conditions requiring timely assessment or action.
2. Alarms should alert, inform and guide required operator action;
3. Every alarm should be useful and relevant to the operator, and have a defined response;
4. Alarm levels should be set such that the operators have sufficient time to carry out their defined response before the plant condition escalates;
5. The alarm system should accommodate human capabilities and limitations

3.3.5.1 Overview of the Literature on Alarm Management

- Standards:
  - IEC 62682 – Management of alarms systems for the process industries [56]
  - ANSI/ISA-18.2 – Management of alarms systems for the process industries [57]
- Guidelines:
  - EEMUA 191 – Alarm systems – A Guide to design, management and procurement [58]
  - ASM Consortium Guidelines – Effective Alarm Management Practices [59]
  - *Better alarm handling,* **HSE** *information sheet, Chemicals Sheet No 6, 2000* [60]
  - HSE Human Factors Briefing Note No. 9, Alarm Handling [61]
- Handbooks:
  - The Alarm Management Handbook – A Comprehensive Guide [62]

As with the literature on HMI design, the standards tend to be prescriptive and terse while the other documents are less prescriptive but contain more explanatory examples. The ANSI/ISA-18.2 standard was published in 2009 and is applicable to the US. A good overview of ISA-18.2 may be found in Stauffer et al. [63] and PAS [64]. The ISA-182.2 standard was influential in the production of the IEC 62682 standard which was published in 2014. A brief summary of the differences in these two standards is provided by Stauffer [65]. Other documents of note are "ABB – Nuisance alarm management" [66] and Smith et al. [67].

4 Using Modeling and Simulation to Validate the Design

4.1 Applying Modeling and Simulation in Smart Grid Design

Building on industry standards provides a strong foundation for an effective and stable Smart Grid security architecture. It is also useful to validate the architecture and design in order to identify and correct issues before beginning implementation.

One approach to validation is modeling. For example, modeling of attack scenarios relative to a particular architecture in terms of risk assessment for false data injection attacks provides insights regarding the resistance of the architecture to such attacks. Such modeling can be valuable in identifying segments within a given grid that result in highest impact in the case of the attack and therefore should be given highest priority in terms both of defensive security capabilities and of monitoring capabilities that can rapidly detect and respond to attacks.

Modeling of attacks against physical components provides insights into effective mechanisms in preventing or reducing the impact of such attacks. These insights can have a significant impact on the security architecture such as regarding key management (in particular the storage of key material) and using PUFs for device authentication and key storage. As discussed in section 2.4 of this document, the use of PUFs may be viewed as an architectural issue to the extent that it changes how and where a public key infrastructure is used for device identification.

Simulation can also provide different insights into a security architecture, particularly in terms of such issues as resiliency and performance. For example, simulation of specific attack scenarios against a Smart Grid security architecture and design can reveal unexpected interactions. In the case of an attack, tampering with measurement signals, for example, may not only mask attack manipulation of devices from operators but also affect how the control systems for the affected devices respond, thereby resulting in cascading impact across multiple components not directly manipulated by the attacker. The instrumentation of monitoring and analysis designed to improve the detection and response to attacks may have negative impacts on the performance of the system. Simulation of the monitoring and analysis can uncover these impacts and enable architectural and design choices that mitigate that impact. The simulation of microgrids in the SPIDERS project is an example of the use of simulation to validate a Smart Grid architecture [68].

4.2 Modeling and simulation for security and privacy validation

The CockpitCI project, funded under the European Union Framework 7 program, provides helpful insights regarding modeling and simulation approaches and tools and their application to Smart Grid architectural validation [69]. The final deliverable for the project, “Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructure”, discusses the range of approaches that are available for modeling and simulation of the resistance and resilience of cyberphysical systems to cyber-attack. The document identifies four major approaches to modeling and simulation:

1. Models and simulations focused on attacks, attackers and vulnerabilities. These include such approaches as attack trees, Petri nets and game theoretic models. These approaches can use probabilistic (stochastic) modeling to express attacker and system behavior or can take alternative approaches such as discrete event or agent-based simulation.
2. Models and simulations focused on enterprise network design and industrial control system network design. This includes such approaches as network state change models or the use of Petri Nets to model network attack scenarios.

3. Power system models and simulation. This includes power flow simulation, modeling of fault detection and use of the SIR (susceptible, infected, recovered) model to study the potential for cascading impacts.
4. Composite models. This approach brings together at least two of the previous modeling and simulation techniques in order to investigate complex interactions, such as attacks that leverage vulnerabilities in the enterprise network to establish remote access infections that can then propagate into the control system.

As the CockpitCI document concludes, no single modeling or simulation technique is sufficient to validate a given Smart Grid architecture and/or design. Rather, all four of these approaches, in terms both of methodologies and of tools, should be considered in determining a strategy for validation a particular architecture and design. The SPARKS project, particularly in Task 4.4, is working on extending the state of the art in this area, particularly in terms of co-simulation of multiple aspects of a Smart Grid and on physical operation and cyber-attacks in order to present a more comprehensive and effective investigation of the impact of various attacks. Even with such advances, however, the use of other simulation and modeling techniques should also be considered when establishing the program for validating a given architecture and design.

4.3 Modeling and simulation for performance validation

In addition to modeling and simulation focused on the resistance and resilience of Smart Grid systems to cyber-attacks, it is also valuable to use these techniques to understand other aspects of the system. As discussed in Skopik et al., the resilience of Smart Grid environments is an important focus of modeling and simulation, particularly in terms of understanding the success of new control mechanisms and algorithms to support graceful degradation in the face of excessive demand, component failure, and other conditions [70]. Modeling and simulation are also important in understanding risk related to privacy, an area that requires significant research [71].

Architectural decisions related to security, such as the use of security analytics for detection, analysis and response to cyber-attacks, or the use of automated response capabilities that perform dynamic reconfigurations to minimize the impact of cyber-attacks, can have significant implications in areas such as grid performance. Modeling and simulation of these aspects of the architecture should also be considered. Considerable work has been done on the modeling and simulation of performance aspects of Smart Grid systems. For example, the U.S. government established the “Advanced Modeling Grid Research Program” in May 2012 to develop new approaches and tools for the modeling of dynamic events related to Smart Grid performance and resilience [72]. There are also a number of academic papers in this area, such as Natsheh et al., on the performance and resilience impact of integration wind and solar energy resources into a Smart Grid [73].

The composite modeling techniques described in CockpitCI are particularly important in terms of understanding the interrelationship between architectural decisions such as the use of security analytics and the performance of a Smart Grid system. For example, high rates of data sampling within an Automated Meter Infrastructure (AMI) are useful in creating an energy usage model that can help in detecting energy theft and fraud [74]. But massive data collection could result in CPU and network bottlenecks that impact the ability of control systems to detect and respond to changes in demand. This interrelationship of security and performance can be investigated through simulation and modeling. Another example relates to events such as the 2003 blackout in northeaster United States, in which a massive increase in energy demand resulted in a widespread power outage. [75] Cyber-attacks that manipulate the AMI infrastructure could result in artificial spikes in demand that could similarly result in a power outage. Modeling and simulation of Smart Grid security design, not just of control system

design, can help to quantify and characterize the impact of cyber-attacks such as these and should therefore be considered as part of the strategy for validating Smart Grid architecture and design.

4.4 Modeling and simulation as on-going activity

As discussed both in this deliverable and in many other resources, cyber-attacks must be viewed as a constantly evolving, dynamic landscape. Modeling and simulation, therefore, also have to be viewed as continuing activities that are applied within an iterative process, such as that described in [76], which considers new attack strategies, new attacker goals and new vulnerabilities as input to the models and simulations. As mentioned there, secure development lifecycle models require "a dramatic change in the way of thinking". The same is true in terms of the approach to modeling and simulation for the purposes of understanding the resistance and resilience of a Smart Grid to cyber-attack. Modeling and simulation have to be understood as a continuous process, rather than purely as a design-time activity.

This on-going nature of modeling and simulation is also important because of the immaturity of these techniques as applied to Smart Grid. We have already touched on the relatively limited research on the use of modeling and simulation in terms of the impact of data disclosure attacks on privacy. As noted in Skopik et al: "modeling disclosure attacks gathering private information from the plant and control algorithms are also relevant. Methodologies to address privacy while ensuring adequate levels of control and estimation performance are required to handle disclosure attacks" [77]. Modeling the susceptibility of Smart Grid systems to data theft, corruption or loss will become increasingly important as pending legislation in the European Union regarding protection of consumer privacy, ownership of data and disclosure of data breaches is approved and enforced.

5 Implementation Considerations for Smart Grid Security

5.1 Commercial-Off-The-Shelf and Custom Capabilities

In section 3.2 of this paper, we discussed the architectural and design issues regarding the integration of legacy and new components in a Smart Grid environment, showing the importance of establishing a durable but flexible architecture that allows that replacement of legacy capabilities. From both the perspectives of financial and risk management, it is important to leverage legacy capabilities, using an evolutionary approach to building out a Smart Grid environment rather than a "Big Bang" approach that attempts to create a new Smart Grid environment from scratch. There may of course be new projects, such as the local implementation of a microgrid, that uses a generation strategy based on renewables, for example, or that will provide a laboratory environment for examining the resilience, security and cost issues of particularly Smart Grid technologies and designs. But in most cases, establishing a Smart Grid environment should be viewed as an iterative, dynamic process that incorporates new insights and strategies as they emerge in this rapidly evolving arena.

That being the case, one of the most important decisions to be made in instantiating a given Smart Grid design is the balance between using commercial-off-the-shelf (COTS) capabilities and using custom-developed capabilities, including processes as well as technologies. Organizations must always consider the "build versus buy" decision when determining a detailed design and implementation process. But as Anvaari et al. argue in their paper presented at the January 2012 ISGT conference, "The large-scale system-of-systems nature of Smart Grid, the evolving nature of the Smart Grid and the changing expectations of Smart Grid stakeholders make these decisions especially important for Smart Grid environments [78].

Most of the research into this issue suggests favoring COTS capabilities, particularly those that leverage standards in order to maximize the opportunities for interoperability across vendor implementations. However, there may be issues even in the use of technology that conforms to well-established standards, as is discussed in Osborn regarding the deployment of Phase Measurement Units (PMUs) in distribution systems [79]. In those cases in which custom development is necessary because of unique requirements or lack of COTS capabilities supporting those requirements, the discussion of a Secure Development Life Cycle earlier in this deliverable should be considered.

To the extent that COTS capabilities can be leveraged, it is also valuable to employ the recommendations from by Morisio et al. regarding a combined COTS and custom development approach [80]. This leverages ideas from rapid software development techniques, particularly in terms of managing evolving requirements. This approach has been developed further by the Software Engineering Institute at Carnegie Mellon in the methodology called "Evolutionary Process for Integrating COTS-Based Systems" (EPIC) that is applicable to Smart Grid environments [81].

5.2 Integrated approach to processes and technology

As in the EPIC methodology, an important consideration in establishing an effective Smart Grid implementation is the integration of process and technology. This is clearly evident in the SGAM methodology which addresses not just technological issues but also critical processes such as risk management. The importance of considering both processes and technology is also called out in the ENISA report on security measures for Smart Grid, again with a particular focus on risk management processes [82]. As James Ketchledge says in "Successful Smart Grid Implementation": "Organizations are required to overhaul their internal business processes to take advantage of new enabling technology, process improvement opportunities, and business strategies afforded by the Smart Grid" [83].

There are several areas in which an integrated approach to processes and technology is particularly important for Smart Grid implementations:

- Changes in technology that require changes in business processes. There are some areas in which this relationship is obvious such as in changing from pre-Smart Grid support processes requiring physical reading of meters to Smart Grid processes providing oversight on the reliability and performance of the Automated Infrastructure. But other areas are not so obvious, such as in the importance of establishing incident management processes and organizational structure that can leverage the large volume of data from the Smart Grid environment to detect, analyze and respond to attacks.

- Changes in technology that benefit from changes in business processes. Information sharing both within the organization and across the organization can substantially increase the ability of the Smart Grid organization to anticipate and take action against cyber-attacks. Although instituting such a process is not required by the Smart Grid, the benefit of having such information sharing is enabled by the increased data available in the Smart Grid and the opportunities for automation of incident management processes provided by the Smart Grid.

- Changes in technology that support new business processes. As discussed in section 2.3 of this document, the much greater volume of information provided by an automated meter infrastructure (AMI) enables new processes for fraud detection and identification through data analysis techniques that were not feasible prior to the Smart Grid. Similarly, the Smart Grid provides opportunities for business process automation in energy flow management, integration of dynamic energy sources such as wind, fault isolation and many other areas.

Ketchledge provides valuable guidance about the Smart Grid processes including formulating two approaches to undertaking the business process transformation that a Smart Grid implementation entails. While he does not discuss in detail the full range of technological drivers for this transformation, he does provide useful insight in the range of process implications that should be considered. Most importantly, he clearly demonstrates that a Smart Grid implementation is not just a question of technology, but also of the intersection of technology, process and organizational issues and opportunities.

5.3 Lessons from current implementations

A significant number of Smart Grid implementations have published case studies, reports and other information regarding their experiences. We began this document by referring to the California ISO report that describes their 10-year plan for their Smart Grid environment. There are also a number of U.S. case studies collected at smartgrid.gov [84] and by the U.S. Energy Information Administration [85]. European case studies are available from KEMA Laboratories [86], the JRC Reference Reports series [87], joint JRC/US-DoE reports [88], studies by analyst firms such as McKinsey [89] and industry organizations such as GEODE [90].

These case studies provide valuable security-related insights into Smart Grid architectures, design and implementation strategies. However, it can be difficult to synthesize these insights into security guidance for a particular Smart Grid implementation. The ENISA 2012 report "Appropriate security measures for Smart Grids: Guidelines to assess the sophistication of security measures implementation" presents an list of key conclusions derived from a range of sources that are borne out by reports and other information from Smart Grid implementations. In particular, there are five key conclusions from the ENISA report that repeatedly surface in case studies of Smart Grid implementations [91]:

- "The **security of the Smart Grid** should be taken into account at an early stage in order to allow set security requirements at planning or development stage at the latest;
- An adequate **risk assessment process** is necessary in order to select the adequate security controls for the Smart Grid organization while designing the overall architecture and the component specification;
- One of the most important objectives of the security infrastructure protecting the Smart Grid is the **prevention/detection as well as the response against cyber events and/or cyber incidents** before there is significant power system impact;
- **Physical security aspects** should address the protection of Smart Grid devices located in the organization's premises as well as outside of the organization's own grounds or premises (for example Smart Grid devices physically located in areas that are the responsibility of other utility providers);
- The necessity of an adequate **identification and authentication process** was acknowledged as one of the most relevant security control aspects in the view of the access to the Smart Grid."

All nineteen of the recommendations in the ENISA report are valuable. However, these five recommendations are particularly important because they are not necessarily familiar to organizations responsible for Smart Grid architecture, design and implementation. Ensuring that they, as well as the other ENISA recommendations, are given serious consideration can help organizations to protect themselves against the cyber-attacks that their Smart Grid implementations will inevitably face.

6 Conclusion

This document has focused on providing security-related guidance for Smart Grid across four aspects of Smart Grid solution development:

- Establishing an effective architecture for a particular Smart Grid environment. In this area, the guidance provided by the NISTIR 7628 and SGAM reference architectures is supplemented by discussions of key issues less thoroughly addressed by those resources, specifically microgrids, security analytics and device authentication.

- Establishing an effective design for a particular Smart Grid. Here, we focus on the critical issues of integrating legacy and new components, and of Human Machine Interface (HMI) design.

- Employing modeling and simulation effectively to validate a Smart Grid architecture, design and implementation. We focus particularly on security-related modeling and simulation, but also look at other areas of modeling and simulation that may be valuable because of security capabilities used in the environment, such as large-scale data analytics.

- Establishing an effective implementation. Here, we focus on the important issues of "Build vs. buy" and of the integration of processes and technology. We also review lessons both from Smart Grid case studies and from ENISA research.

In this document, we have provided guidance for those aspects of Smart Grid security that we believe have not otherwise been explored adequately in other resources. Our primary audience for this guidance is the individuals directly involved in Smart Grid implementations. However, some broader implications may already be apparent to the reader regarding gaps and opportunities in standardization. We intend this area to be the focus of the next deliverable of this work package.

7 References

This section lists the citations in this document.

1. NISTIR 7628, Revision 1. “Guidelines for Smart Grid Cybersecurity, Volumes 1 – 3”. 2014. http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
2. California ISO. (2010) Smart Grid Roadmap and Architecture. Retrieved from http://www.caiso.com/green/greensmartgrid.html
3. Cal ISO, p. 14.
4. KEMA. Combatting Energy Theft in Smart Grid Systems. 2014. http://smartgridsherpa.com/wp-content/uploads/2013/02/Energy-Theft-D1V4.pdf
5. 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
6. Sandia National Laboratories. “Microgrid Security Reference Architecture”. 2012. http://prod.sandia.gov/techlib/access-control.cgi/2013/135472.pdf Also available as Veitch, Cynthia K., Henry, Jordan M., Richardson, Bryan T., & Hart, Derek H. (2013). Microgrid cyber security reference architecture. United States. . doi:10.2172/1090210
7. Antony Tang, Jun Han, Rajesh Vasa, "Software Architecture Design Reasoning: A Case for Improved Methodology Support", IEEE Software, vol.26, no. 2, pp. 43-49, March/April 2009, doi:10.1109/MS.2009.46
8. Considine, T., Cox, W., Cazalet E., (2012). Understanding Microgrids as the Essential Architecture of Smart Energy. In Grid-Interop Forum. Irving, TX, Dec 3-7 2012. Gridwise Architecture Council. http://www.gridwiseac.org/pdfs/forum_papers12/considine_paper_gi12.pdf
9. DOE. Comparing the Impacts of Northeast Hurricanes on Energy Infrastructure. Washington, DC: Office of Electricity Delivery and Energy Reliability, DOE, April 2013. http://energy.gov/sites/prod/files/2013/04/f0/Northeast Storm Comparison_FINAL_041513c.pdf.
10. Barrager, S. E. Cazalet, 2014. Transactive Energy: A Sustainable Business and Regulatory Model for Electricity, Baker Street Publishing, E-book
11. Degner, T., Soultanis, N., Engler, A. and Muro, A. G. d. (2013) Intelligent Local Controllers, in Microgrids: Architectures and Control (ed N. Hatziargyriou), John Wiley and Sons Ltd, Chichester, United Kingdom. doi: 10.1002/9781118720677.ch03
12. Considine et al. 2012.
13. “Maryland Resiliency Through Microgrids Task Force Report”, 2014 http://cdm266901.cdmhost.com/cdm/ref/collection/p266901coll7/id/4862
14. Siemens. 2015. Microgrid Start Up: A Guide to Navigating the Financial, Regulatory, and Technical Challenges of Microgrid Implementation. http://w3.usa.siemens.com/smartgrid/us/en/microgrid/Documents/Ebook.pdf
15. Siemens . 2015.
16. IEEE 1547 Series of Standards http://grouper.ieee.org/groups/scc21/1547/1547_index.html
17. IEEE 2030 Series of Standards http://grouper.ieee.org/groups/scc21/2030/2030_index.html
18. NERC CIP Standards http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
19. IEC Core Smart Grid Standards http://www.iec.ch/smartgrid/standards/

20. IEC Core Smart Grid Standards http://www.iec.ch/smartgrid/standards/
21. Barrager. 2014.
22. Sandia. 2012.
23. RSA, the Security Division of EMC. (2013) Big Data Fuels Intelligence-Driven Security. Retrieved from http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf
24. Diagram adapted courtesy of RSA, the Security Division of EMC. (2013) Big Data Fuels Intelligence-Driven Security. Retrieved from http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf
25. Popovic, Tom et al. (2013). Smart Grid data analytics for digital protective relay event recordings. Retrieved from https://www.academia.edu/7691468/Smart_grid_data_analytics_for_digital_protective_relay_event_recordings
26. Cal ISO. 2010.
27. Popovic. 2011.
28. Swearingen, Michael et al. What you need to know (and don't) about the AURORA vulnerability. Retrieved from http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/
29. SPARKS D4.2. "PUF enhanced smart meter hardware architecture and an authentication/key management deployment architecture." 2015.
30. Ravikanth Pappu. Physical One-Way Functions. PhD thesis, Massachusetts Institute of Technology, 2001.
31. Pim Tuyls, Geert jan Schrijen, Boris Skoric, Jan Van Geloven, Nynke Verhaegh, and Rob Wolters. Read-proof hardware from protective coatings. In In Cryptographic Hardware and Embedded Systems—CHES 2006.
32. Knapp argues in his book "Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems" Knapp, E. (2011). *Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*. Elsevier.
33. Yan (2013) Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, *15*(1), 5–20. doi:10.1109/SURV.2012.021312.00034
34. Skopik, Florian et al. Smart Grid Security: Innovative Solutions for a Modernized Grid. 2015. Elsevier. http://www.amazon.com/Smart-Grid-Security-Innovative-Modernized/dp/0128021225/ref=sr_1_1?ie=UTF8&qid=1440160373&sr=8-1&keywords=skopik+smart+grid
35. Teixeira, A., Dán, G., Sandberg, H., Berthier, R. Bobba, R., & Valdes, A. (2014). Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures. In Proceedings of the American Control Conference.
36. Skopik. 2015. Chapter 6.
37. Skopik. 2015. Chapter 9.
38. Skopik. 2015. Chapter 7
39. Skopik. 2015. Chapter 6.
40. Hecht et al., (2014). Thomas Hecht, Lucie Langer, Paul Smith (09/2014): Cybersecurity Risk Assessment in Smart Grids. Fifth Symposium on Communications for Energy Systems (ComForEn), September 29-30 2014, p. 39-46, Schriftenreihe Nr. 77, OVE.
41. Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile. (2012). 'Final Report On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris.' http://www.bea.aero/en/enquetes/flight.af.447/rapport.final.en.php

42. Health and Safety Executive. 1997. 'The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994: A report of the investigation by the Health and Safety Executive into the explosion and fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 July 1994', ISBN 0 7176 1413 1.
43. International Standards Organization ISO 11064-5:2008. 'Ergonomic design of control centres — Part 5: Displays and controls.' https://www.iso.org/obp/ui/#iso:std:iso:11064:-5:ed-1:v1:en
44. International Society of Automation ISA 101. Human-Machine Interfaces https://www.isa.org/isa101
45. Engineering Equipment and Materials Users' Association. 2010. EEMUA Publication 201 'Process plant control desks utilising human-computer interfaces: a guide to design, operational and human-computer interface issues.' Second Edition.
46. United States Nuclear Regulatory Commission. 2002. Human-System Interface Design Review Guidelines (NUREG-0700, Revision 2).
47. ASM Consortium. 2013. 'Effective Console Operator HMI Design: Second Edition'. ISBN 978-1492875635.
48. Hollifield, Oliver, Nimmo and Habibi. 'The High Performance HMI Handbook: A Comprehensive Guide to Designing, Maintaining and Implementing Effective HMIs for Industrial Plant Operations'. ISBN 978-0977896912.
49. Stanton, Salmon, Jenkins and Walker. 'Human Factors in the Design and Evaluation of Central Control Room Operations'. ISBN 978-1439809914.
50. Gruhn. 66th Annual Instrumentation Symposium for the Process Industries. 2011. 'Human Machine Interface (HMI) Design: The Good, The Bad, and The Ugly (and what makes them so)' http://www.kirp.chtf.stuba.sk/moodle/pluginfile.php/61474/mod_resource/content/2/hmi_rules.pdf
51. Hollifield and Perez. PAS 2012. 'High Performance Graphics to Maximize Operator Effectiveness, Version 2.0' https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/white-papers/pas-high-performance-graphics-to-maximize-operator-effectiveness/
52. Opto 22. 2013. 'Building an HMI that Works: New Best Practices for Operator Interface Design'. http://www.opto22.com/documents/2061_High_Performance_HMI_white_paper.pdf
53. ABB. 2013. 'Best Practice Guidelines. Operator workplace and process graphics'. https://library.e.abb.com/public/c2583a86b2762b79c1257c440052de84/3BSE068129_A_en_800xA_best_practice_guidelines_-_Operator_workplace_and_process_graphics.pdf
54. Acuité. 2011. 'Human Machine Interface Standards: A critical review and help for users'. https://www.acuite.com/sites/default/files/HMI%20Standards%20Review_Aug2012.pdf
55. Health and Safety Executive. 2000. Better alarm handling, HSE information sheet, Chemicals Sheet No. 6.
56. International Electrotechnical Commission. IEC62682:2014. 'Management of alarm systems for the process industries'.
57. ANSI/ISA ISA18.00.02-2009 "Management of Alarm Systems for the Process Industries".
58. Engineering Equipment and Materials Users' Association. EEMUA Publication 191. 'Alarm systems, a guide to design, management and procurement'. Third Edition.
59. ASM Consortium. 2009. 'Effective Alarm Management Practices'. ISBN 978-1442184251.
60. Bransby and Jenkison. 1997. 'The Management of Alarm Systems.' http://www.hse.gov.uk/research/crr_pdf/1998/crr98166.pdf
61. Health and Safety Executive. 2005. 'HSE Human Factors Briefing Note No. 9 Alarm Handling'. http://www.hse.gov.uk/humanfactors/topics/09alarms.pdf
62. Hollifield and Habibi. 2010. 'The Alarm Management Handbook'.
63. Stauffer, Sands and Dunn. 2010. 'Alarm Management and ISA-18 – A Journey, not a Destination'. http://exida.com/images/uploads/Alarm_Management_and_ISA_18_2-_A_journey_not_a_destination.pdf

64. Hollifield. 2010. 'Understanding and Applying the ANSI/ISA 18.2 Alarm Management Standard'. http://www.pas.com/Downloads-(1)/AMORt/SP18.aspx
65. Stauffer. 2014. 'Alarm Management Goes Global with the Release of IEC 62682!' http://www.exida.com/Blog/alarm-management-goes-global-with-the-release-of-iec-62682
66. ABB. 2012. 'Nuisance alarm management'. https://library.e.abb.com/public/79988bb270b5637d48257b1e005595e3/Nuisance%20alarm%20management(PRS079a)LowRes.pdf
67. Smith, Howard and Foord. 2003. 'Alarms Management – Priority, Floods, Tears or Gain?' http://wildeanalysis.co.uk/system/downloads/369/original/Alarms_Paper_Smith_Howard_Foord.pdf
68. Stamp, J. Experiences and Lessons Learned From SPIDERS Microgrids Rollout and Demonstrations. http://www.ieee-pes.org/presentations/gm2014/PESGM2014P-002516.pdf
69. CockpitCI Project. Cybersecurity on Scada. 2011. http://www.cockpitci.eu/wp-content/uploads/2015/04/CockpitCI-D5.4-CockpitCI-System-Factory-Trials-Report.pdf
70. Skopik, p. 295.
71. Skopik, p. 296.
72. United States Department of Energy. "Advanced Modeling Grid Research Program" . 2012 http://energy.gov/oe/services/technology-development/advanced-modeling-grid-research-program
73. Natsheh, E.M. et al. Modeling and control for Smart Grid integration of solar / wind energy conversion system. 2011 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6162643&url=http%3A//ieeexplore.ieee.org/xpls/abs_all.jsp%3Farnumber%3D6162643
74. KEMA. Combatting Energy Theft in Smart Grid Systems. 2014. http://smartgridsherpa.com/wp-content/uploads/2013/02/Energy-Theft-D1V4.pdf
75. Wikipedia. . List of major power outages. N.d. https://en.wikipedia.org/wiki/List_of_major_power_outages
76. Skopik, p. 229.
77. Skopik, p. 179.
78. Anvaari. Smart Grid software applications as an ultra-large-scale system: Challenges for evolution http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6175687. Also available at www.idi.ntnu.no/grupper/su/publ/smartgrid/ISGT2012.pdf.
79. Osborn, Mark. .IEC 68150 Interoperability Challenges. 2013. https://www.qualitylogic.com/community/index.php/iec-61850-interoperability-challenges/
80. Morisio. Investigating and Improving a COTS-Based Software. 2000. http://www.cs.umd.edu/projects/SoftEng/ESEG/papers/83.83.pdf
81. http://www.sei.cmu.edu/acquisition/tools/methods/epicprod.cfm. See also www.cs.umd.edu/projects/SoftEng/ESEG/papers/83.83.pdf.
82. ENISA. "Appropriate security measures for Smart Grids: Guidelines to assess the sophistication of security measures implementation". 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at_download/fullReport
83. Ketchledge, James. Successful Smart Grid Implementation. 2015. P 138.
84. Smartgrid.gov. N.D. https://www.smartgrid.gov/recovery_act/featured_case_studies.html
85. U.S. Energy Information Administration. Smart Grid Legislative and Regulatory Policies and Case Studies. 2011. www.**eia**.gov/analysis/**studies**/electricity/pdf/**smartggrid**.pdf
86. KEMA. N.d. http://smartgridsherpa.com/case-studies
87. JRC Reference Reports. Smart Grid Projects in Europe: Lessons Learned and current developments. 2011. http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe_lessons_learned_and_current_developments.pdf

88. JRC DOE. Assessing Smart Grid Benefits and Impacts. 2012. https://ec.europa.eu/jrc/sites/default/files/eu-us_smart_grid_assessment_-_final_report_-online_version.pdf
89. MCKinsey. Can the Smart Grid live up to Expectations? 2010. http://www.mckinsey.com/client_service/electric_power_and_natural_gas/latest_thinking/mckinsey_on_smart_grid
90. GEODE. Bringing Intelligence to the Grid. 2013. http:/www.geode-eu.org/uploads/REPORT%2520CASE%2520STUDIES.pdf
91. ENISA. "Appropriate security measures for Smart Grids: Guidelines to assess the sophistication of security measures implementation". 2012.

The Smart Grid Interoperability Panel â€“ Cyber Security Working Group. August 2010. NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. The Smart Grid Interoperability Panelâ€“Cyber Security Working Group. August 2010. U. S. Department of Commerce Gary Locke, Secretary.Â This National Institute of Standards and Technology Interagency Report (NISTIR) discusses ITLâ€™s research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. National Institute of Standards and Technology Interagency Report 7628, vol. 1. The invention of â€œsmart gridâ€ promises to improve the efficiency and reliability of the power system. As smart grid is turning out to be one of the most promising technologies, its security concerns are becoming more crucial. The grid is susceptible to different types of attacks. This paper will focus on these threats and risks especially relating to cyber security. Cyber security is a vital topic, since the smart grid uses high level of computation like the IT. We will also see cryptography and key management techniques that are required to overcome these attacks. Privacy of consumers is anot