 <a href="http://d2cigre.org">http://d2cigre.org</a>	CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS
	<b>STUDY COMMITTEE D2</b> INFORMATION SYSTEMS AND TELECOMMUNICATION <b>2013 Colloquium</b> <b>November 13-15, 2013</b> <b>Mysore – KARNATAKA - INDIA</b>

## D2-02\_12

### Comprehensive Cybersecurity strategy for Smartgrid equipment manufacturers

by

**M.A. Alvarez\*, T. Arzuaga**

**CG Automation BU**

#### SUMMARY

The benefits in the evolution of traditional electrical grid into the Smart Grid, are more evident every day. However, this evolution is also offering more rewards to potential attackers as well as a wider range of potential attack vectors due to the increase in the use of communications and the integration of operational systems in the internet. This has led to an increased awareness of the need for implementation of Cybersecurity measures in the Smart Grid.

Cybersecurity field has not been part of the body of knowledge of electrical grid designers, though. So, even if equipment manufacturers are beginning to deal with the inclusion of CyberSecurity features to their developments, they are not always following the best approach but trying to find and follow recommendations and best practices guides. However, there are no fixed rules that ensure the security of equipment yet.

The main aim of this paper is to use a pragmatic approach to create a reference guide for a first approach of equipment manufacturers to the world of cybersecurity. To achieve this, it is necessary to analyze very different aspects ranging from the work of public agencies such as NERC CIP or penetration testing techniques (such as those made by Digital Bond in S4), to international standards (IEC62351...), key management procedures. All of this should also be combined with the study of known Cybersecurity attacks such as Stuxnet.

This paper takes into account that the implementation of Cybersecurity is a quite different task compared with the ones usually tackled by manufacturers. On one hand, it must be considered that it is not a concrete and definite task, but a set of decision making and measurement implementation rules relatively unconnected to one another. However, they help in the prevention of a whole range of risks for equipment.

On the other hand, and, unlike what happens with other features, the implementation of security measures does not 100% guarantee the security of equipment, so the task does never end, and in addition to the prevention methods, detection methods should also be implemented to offer quick detection of new vulnerabilities. The combination of prevention and detection will sometimes fail, so a good Cybersecurity system must also consider mitigation and recovery techniques.

---

\* Parque Tecnológico de Zamudio, Edificio 210 48170 Zamudio, Spain  
 Fax: + 34 94 403 7440 e-mail: ma.alvarez@ziv.es


This paper proposes as a practical approach the decomposition of the system in use cases as concise and clear as possible. The different steps proposed for use cases are as follows:

- Initial analysis based on abstract concepts such as confidentiality, integrity and availability (CIA model).
- Analysis of risks and vulnerabilities, focusing primarily on scaled potential attacks.
- Selection of generic methodologies for prevention, detection and response.
- Selection of the security features both hardware (chip key storage, cryptographic coprocessors, biometric protection ...) and software (security libraries, logs and event managers ...).

Tracking a top-down methodology for writing use cases, favors Cybersecurity non based on "magic formulas", but on common sense.

## **KEYWORDS**

Smart Grid, Cyber Security, risk analysis, CIA model, McCumber cube, SGAM, SGIS

 <a href="http://d2cigre.org">http://d2cigre.org</a>	CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS
	<b>STUDY COMMITTEE D2</b> INFORMATION SYSTEMS AND TELECOMMUNICATION <b>2013 Colloquium</b> <b>November 13-15, 2013</b> <b>Mysore – KARNATAKA - INDIA</b>

## 1. INTRODUCTION

The benefits in the evolution of traditional electrical grid into the Smart Grid, are more evident every day. However, this evolution is also offering more rewards to potential attackers as well as a wider range of potential attack vectors due to the increase in the use of communications and the integration of operational systems in the internet. This has led to an increased awareness of the need for implementation of Cybersecurity measures in the Smart Grid.

## 2. GAP OF KNOWLEDGE

Although the word Cybersecurity is something that has appeared in the media in the last year, it is not part of the traditional Body Of Knowledge of the engineers working in the energy sector. Some companies are beginning to hire Cybersecurity experts or subcontract services from companies involved in the security sector.

Whether this is the right approach or not is out of the scope of this paper. However, the situation is quite similar to the moment in which communications arrived to the energy sector. At that moment, a gap appeared between the energy experts who did not know anything about communications and the communications experts who were new to the sector.

What has been learned from these last years, is that this gap is not good for the business, and that some degree of understanding of both energy and communications is ideal to build efficient teams and obtain best results.

The situation with Cybersecurity is more or less the same, so whether security experts are hired or not, at least a minimum understanding of the Cybersecurity fundamentals is required inside any company in the energy sector. This way, they will know when and how to follow recommendations and best practices guides.

## 3. WHAT IS CYBERSECURITY?

But... what is Cybersecurity? The answer to this question is not simple as there is not a global agreement of the scope of the term. In fact [1] states that “The understanding of Cybersecurity and other key terms varies considerably from country to country. This influences the different approaches to Cybersecurity strategy among countries. The lack of common understandings and approaches between countries may hamper international cooperation, the need of which is acknowledged by all countries”.

One of the most interesting definitions of Cybersecurity is the one offered by Menny Barzilay in [2]. He bases his definition of Cybersecurity in the definition of a cyberrisk. In his opinion, “cyberrisk is not one specific risk. It is a group of risks, which differ in technology, attack vectors, means, etc. We address these risks as a group largely due to two similar characteristics: A) they all have a potential great impact B) they were all once considered improbable.”.

In his approach, “something has changed recently. The threat landscape evolved to the point that risks that were once considered unlikely began occurring with regularity... This trend can be attributed to higher maturity of attack tools and methods, increased exposure, increased motivation of attackers, and better detection tools enabling more visibility. With that said, we must accept that some of this shift is a result of our increased awareness to this new, highly focused group of risks”.

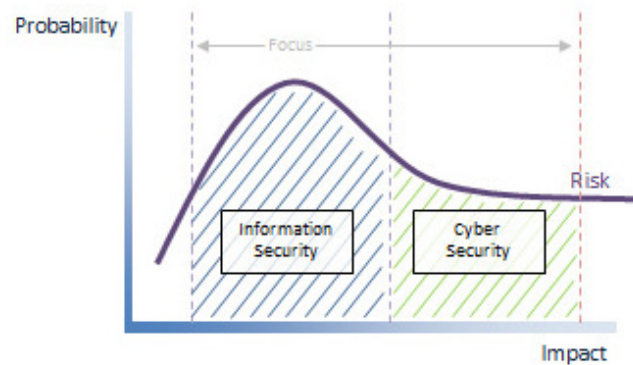


Figure 1: Scope of Cyber Security

So, Cybersecurity can be seen as an extension of information security with the need of dealing with high impact and not so “less probable as before” risks.

So, one of the most important things to take into account when dealing with Cybersecurity is that we are not talking about certainties, but probabilities, so risk analysis and risk management methods are in the core of all Cybersecurity procedures. And the fact of dealing with risks and probabilities also implies that Cybersecurity does not only deal with technical solutions, but also with costs. So Cybersecurity should be put in place from the first steps of the design process in the products produced by the manufacture companies. There a good balance between risk prevention and cost effectiveness should be taken into account.

#### 4. STANDARDS FOR CYBERSECURITY

Probabilities and uncertainties are not something easy to deal with in a design process. That is why it is quite common that the first thought is: “which standard / protocol should we implement to guarantee the Cybersecurity of a product?”.

The sad answer is that there is no standard / protocol that warrant this. However there is a global tendency to build up a framework that covers all Cybersecurity gaps. In fact, the Smart Grid Information Security group form SGCG has performed a work of analysing the state of art in this field and find the gaps [3], so that they can be covered in following steps.

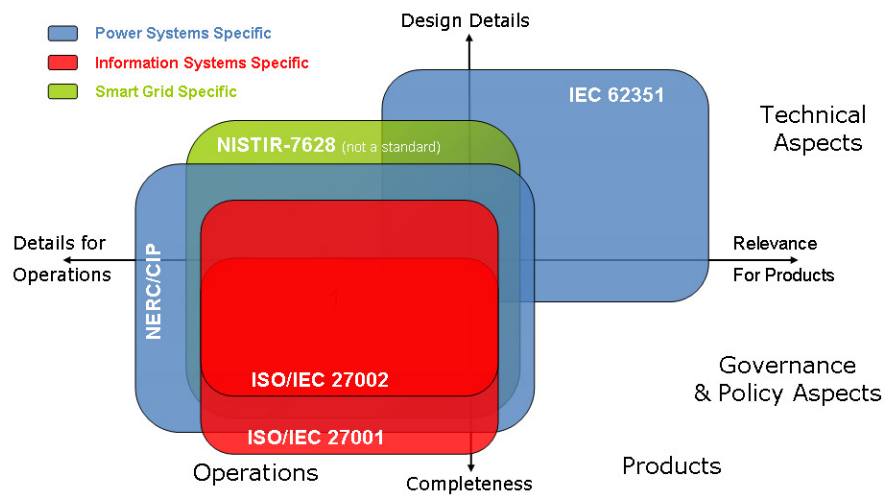


Figure 2: Cybersecurity standard framework

## 5. CIA MODEL AND THE MCCUMBER CUBE

So, there is no easy way. Standards do not cover 100% of the scope, and in addition we are dealing with probabilities and risks. In this situation the best arms for a manufacturing engineer are two; knowledge and common sense.

Regarding the knowledge aspect, there are two very simple and useful tools; the CIA model and the McCumber Cube [4].

CIA model states that all risks should be classified by their impact in three different aspects; confidentiality, integrity and availability.

The McCumber cube considers the CIA model just as one phase of the method being the second the “information states” (transmission, storage and processing) and the third the “safeguards” (human factors, policy and practices, and technology).

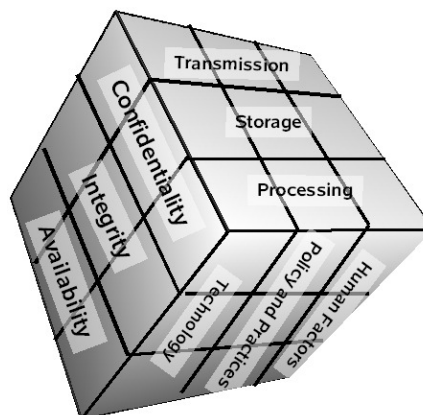


Figure 3: McCumber cube

This helps to determine what should be protected, in which moment, and with which methods.

## 6. SMART GRID ARCHITECTURE MODEL (SGAM)

Another important question is who is responsible for the Cybersecurity. The answer is clear; all stakeholders in the system are responsible of their part, and overlaps between the different responsibilities exist.

For the case of the Smart Grid, the SGCG is trying to standardize a reference architecture called Smart Grid Architecture Model (SGAM). This model defines a three axis (domain, zone and interoperability layers) architecture and helps in the clarification of the scope of each of the stakeholders.

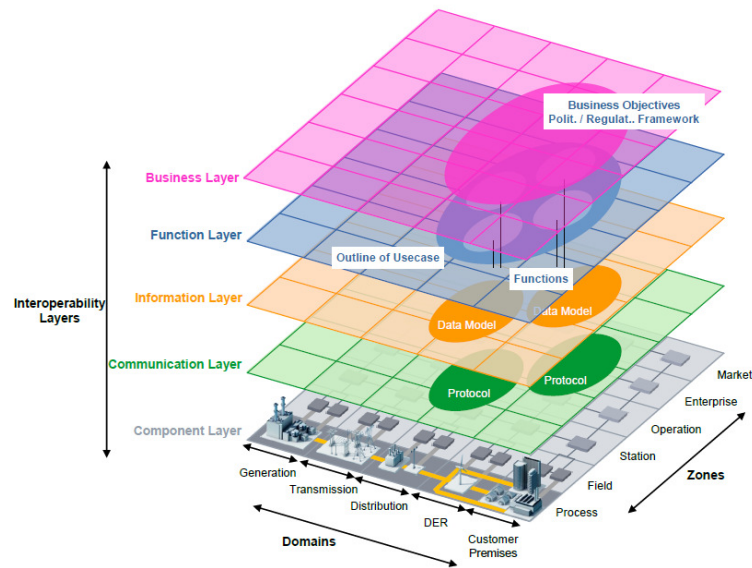


Figure 4: Smart Grid Architecture Model

## 7. USE CASES

Previously we have stated that there is not just a single cyber risk. In the same way there is not just one single cyber security. So it is important not to mix different problems, because not all of them will be caused by the same attacker, shares the same effects or should be solved with the same methods.

The first (and possibly the most important) step is to build up different use cases that split the whole problem into more affordable issues. The opposite usually guides into maximalist approaches in which not the most effective measures are taken, and additionally with greater than desired impact in the performance of the system and its costs.

Generating the right use cases is not an easy task. Some platforms are trying to standardize the use cases for different aspects of the Smart Grid. Some of them, such as the European Smartmetering Interest Group (ESMIG) are even trying to coordinate their efforts with the SGCG developments.

In any case, it is quite important that at least each use case identifies:

- Information assets
- Owners
- Actors

Other things that should be taken into account are:

- Operation and management: Quite often, only the operation processes are taken into account (e.g. iec60870-5-104 communications). However, a break in the security of

management processes (e.g. web parameterization) could be as harmful in terms of denial of service, for example, as a breach in the operation processes.

- Defence in depth: Security layers can and must overlap. There is no sense in deciding not to protect the Ethernet access of a data management concentrator considering that all the communications are performed via a secure router (for example). Someone can enter into the facility, disconnect the router and access directly to the concentrator.
- Security through obscurity: Although there is somekind of “securityfeeling” that comes from the fact of using obscure or not public known technologies or devices, this is something that cannot be guaranteed in the future, so do not consider it.

## 8. SGIS TOOLCHAIN

The SGCG is trying to standardize the process of building security based on the creation of use cases in a four steps process:

- Identify use cases
- Map use cases on SGAM
- Link the result with the SGIS toolbox
- Identify standards (and gaps).

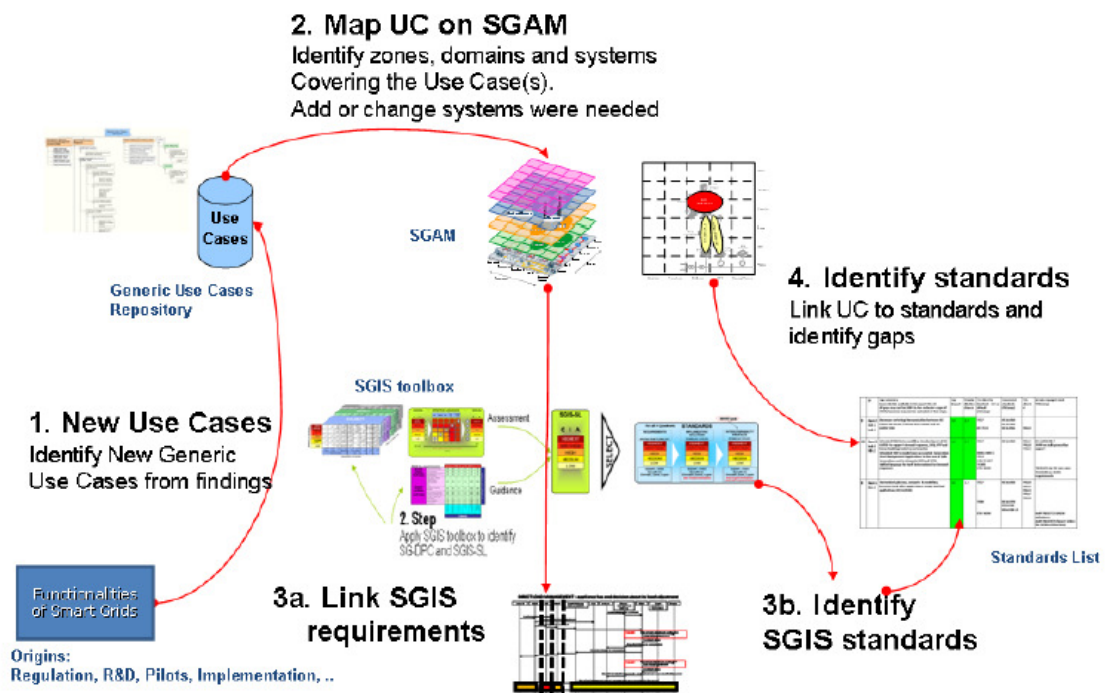


Figure 5: Security process of SGCG

The SGIS toolbox, first enforces the user to think in terms of the CIA model, so that a use case is analysed separately in terms of confidentiality, integrity and availability. This is a very interesting process as well as useful in terms of better contextualizing the risks.



e.g. The first approach to the security of measures sent by an RTU to a SCADA system is usually to use all kind of modern encryption. Nevertheless, thinking in terms of the CIA model, there is no much discussion in considering the importance of integrity. However it seems that the availability could be compromised to some extent without harming the grid. Regarding confidentiality, the thing is not so clear, but probably there could be no problem in some attacker violating the confidentiality of the transmission. In this case, the answer could be just to add a signature to the measurement, requiring less CPU use and impacting less on the performance of the communications.

e.g. Sending a disconnection or reconnection order to a Smart Meter, requires also a great deal of integrity, but it is possible that also confidentiality must be taken into account to guarantee the privacy of the user. In addition, in some countries the time to perform a reconnection order is legally established. In this case, availability is also a concern, and the security problem does not end on compression, but requires also redundancy (whether cyber redundancy, or the existence of a group of workers that can perform the reconnection manually).

The second step of the SGIS toolbox is to map each part of the use case (C-I-A) to a security level that clarifies the impact of a security breach. Their proposal is to use a 5 level chart that classifies the impact in terms of power capacity compromised.

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Figure 6: SGIS security levels

This factor helps to rationalize the Cybersecurity issues and when analysed during design processes, also leads to devices that are more secure by design.

e.g. Imagine the security breach offered by the JTAG pins left in the PCB of a Smart Meter. Someone could (hypothetically) use them to gather information about the key used to encrypt the data sent to the HES. This could be used to perform fraud in the billing of a household. The impact is low (almost negligible). However, if the same key is used in all meters of a model, the criticality increases exponentially as well as the interest of possible attackers interests to find it.

This example also gives another clue for manufacturers in their designs; uniqueness. Everything that transform one device of a whole into a unique device helps in reducing the impact and the risks.



The final element of the SGIS toolbox, the likelihood, is perhaps the most subjective one and the one that in our opinion is somehow distorting the model. From the definition previously used of cyber risk, we are dealing with some risks that were previously considered improbable. However we are being told that the attackers can come from a wide spectrum from hobbyist to cyberterrorists. So the tendency is to consider always that the likelihood is very high.

As the SGIS toolbox combines impact levels and likelihood, no matter the impact level is low, the combination tends to be high and the security measures proposed always guide to implement the highest levels of the standards...

It is difficult to know if this is the correct approach or not, because cyberterrorism is a fact. However this same approach could lead to wear Kevlar in the streets or prepare all buildings against attacks of nuclear weapons.

## 9. INFORMATION SECURITY PROCESS

In this point, the information security comes with help in the form of the Information Security Process.

The methods offered by the security standards and the SGIS toolbox usually deal with the prevention. However, detection and response are as important as the prevention.

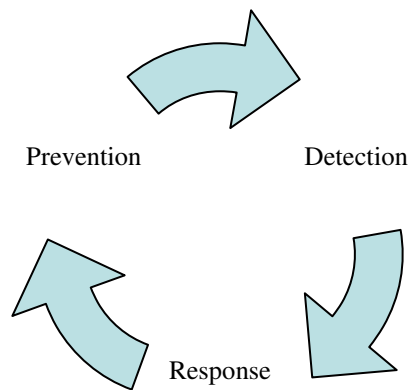


Figure 7: Information security process

Attacks require some degree of preparation, so Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) could be quite helpful with dealing with the breakages and reducing their likelihood. Sometimes these are implemented as standalone devices, but from a manufacturer perspective it is interesting to consider how internal logs and events can offer information regarding abnormal activity. The Smart Grid represents a lot of devices to be attacked, but also a whole security network to prevent and detect attacks.

Regarding the response aspect, it will depend on the type of attack, of course. However, it could be a good design practice to isolate the vital and non-vital parts of a device so that a response to an attack could make the device enter into an ultra-secure mode in which the non-vital features are deactivated. E.g. A 61850 protection relay could maintain the protection functions restricting the sending of gose information or disabling the configuration features.

## **10. THE BOTTOM UP APPROACH : PENETRATION TESTING**

Although this paper has followed a top down approach, for manufacturers it is quite interesting to consider also the bottom up approach as this, at least will prevent the most simple security breakage and prevent attacks from script kiddies or even more experienced hackers. Penetration testing is an art that is acquired with years of experience. However, hacking techniques and penetration testing tools are available nowadays and offer an entry point for this.

Elaborated attacks could be difficult to reproduce or prevent, but at least some simple guides should be always followed during design:

- Implement access control based on roles, prevent the use of usernames in brute force lists, and restrict password selection so that no weak passwords are selected.
- Do not leave unnecessary entry points whether they are not used TCP ports or footprints for JTAG connectors.
- Check the lists of vulnerabilities of the operating system used, implement the patches.
- Use trusted security modules in high critical assets or use unique passwords in the rest.
- Try to use non-standard platforms (reduction of availability of general malware).
- Limit the use of readwrite filesystems.
- When dealing with 3<sup>rd</sup> party software, implement just the required features (limits the number of possible vulnerabilities).
- ...

## **11. AWARENESS**

Last but not least, it is very important to raise the awareness regarding the cyber risks at all levels in the organization. In a world of IP interconnection, it is not enough to have the best Cybersecurity experts designing a secure product, if there is someone that plugs a USB pen drive with unknown origin. Something like this was in the root of the Stuxnet incident that is probably the most important cyberattack ever produced in the electrical network until this moment.

## **12. CONCLUSIONS**

Implementing Cybersecurity in the Smart Grid is not an easy task, it is not even a onetime task, there are different stakeholders involved, and we are not dealing with certainties but with probabilities.

The only way to face the problem is using a knowledge that was not previously present in the energy sector and using methodologies that help in dealing with cyber risks in a rational way. This knowledge and methodologies must impregnate the Body Of Knowledge of the engineers in the energy sector. If this does not happen, devices and systems in the sector will be required to incorporate over dimensioned security methods that will negatively impact in the performance and costs of the systems and could even endanger the evolution of the Smart Grid.

However, some efforts to incorporate information security to the Smart Grid is being performed in the last years by people such as the Smart Grid Information Security group. The work is far from being finished, but some clues of the required methodologies are already offered. Using these methodologies and combining them with common sense, Cybersecurity will be in the near future part of the design process.

## **BIBLIOGRAPHY**

- [1] “National Cyber Security Strategies”, ENISA, May 2012
- [2] “A simple definition of Cybersecurity”, Menny Barzilay, May 2013  
(<http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296>)
- [3] “Smart Grid Information Security”,  
CEN-CENELEC-ETSI Smart Grid Coordination Group, November 2012
- [4] “Assessing and Managing Security Risk in IT Systems: A Structured Methodology”  
Auerbach Publications, John McCumber , June 15, 2004.