RISK MANAGEMENT
IBERDROLA'S CASE

IBERDROLA
DISTRIBUCIÓN ELÉCTRICA

RISK MANAGEMENT – IBERDROLA’S CASE

TODAY’S ENVIRONMENT

Smart grids entail introducing millions of new intelligent components to energy infrastructures that communicate and control energy distribution and transmission in much more advanced and optimal ways than in the past.

Such new components, however, introduce new risks and vulnerabilities that have to be faced in carefully thought-out and innovative ways.

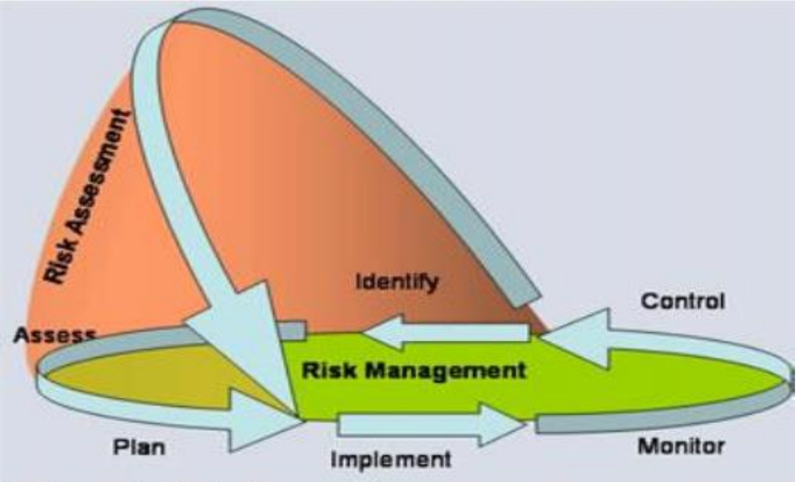
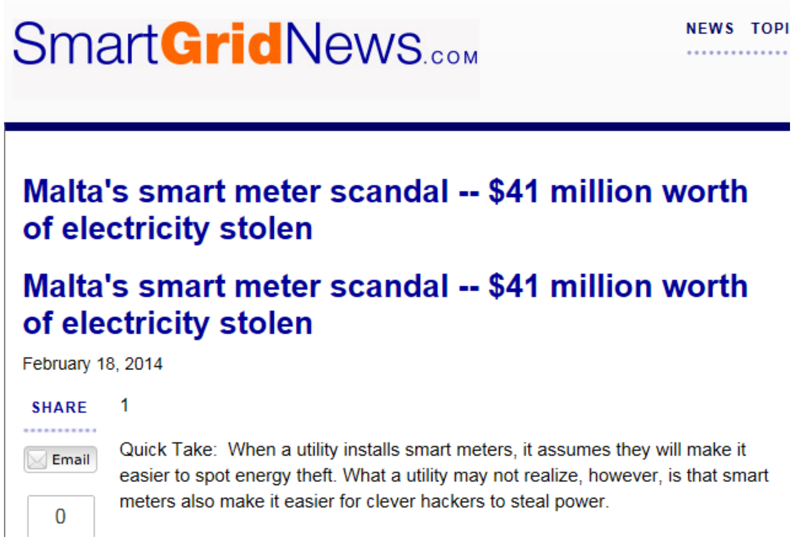


Fig 2 [Source: ENISA/Octave]

RISK MANAGEMENT – IBERDROLA'S CASE

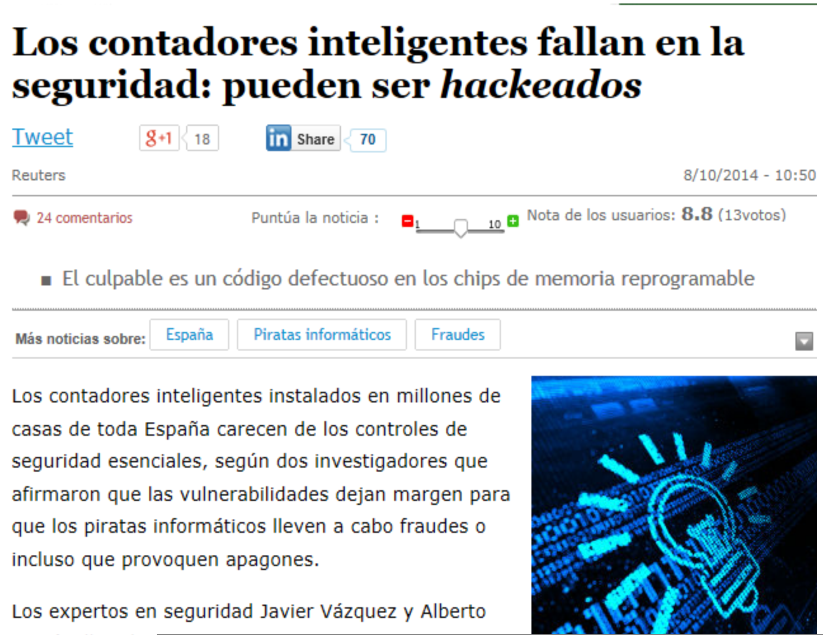


Malta's smart meter scandal -- $41 million worth of electricity stolen

Malta's smart meter scandal -- $41 million worth of electricity stolen

February 18, 2014

Quick Take: When a utility installs smart meters, it assumes they will make it easier to spot energy theft. What a utility may not realize, however, is that smart meters also make it easier for clever hackers to steal power.



Los contadores inteligentes fallan en la seguridad: pueden ser *hackeados*

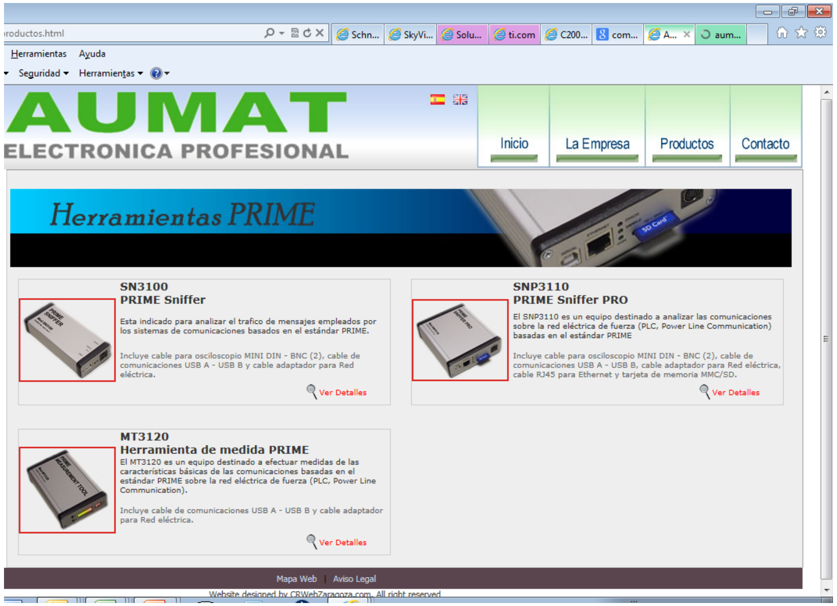
Reuters 8/10/2014 - 10:50

Nota de los usuarios: 8.8 (13votos)

- El culpable es un código defectuoso en los chips de memoria reprogramable

Los contadores inteligentes instalados en millones de casas de toda España carecen de los controles de seguridad esenciales, según dos investigadores que afirmaron que las vulnerabilidades dejan margen para que los piratas informáticos lleven a cabo fraudes o incluso que provoquen apagones.

Los expertos en seguridad Javier Vázquez y Alberto García Illera har
llamados contac
alcanzar los obj
garantías básica
piratas informát



SN3100
PRIME Sniffer

Esta indicado para analizar el trafico de mensajes empleados por los sistemas de comunicaciones basados en el estándar PRIME.

Incluye cable para osciloscopio MINI DIN - BNC (2), cable de comunicaciones USB A - USB B y cable adaptador para Red eléctrica.

SNP3110
PRIME Sniffer PRO

El SNP3110 es un equipo destinado a analizar las comunicaciones sobre la red eléctrica de fuerza (PLC, Power Line Communication) basadas en el estándar PRIME

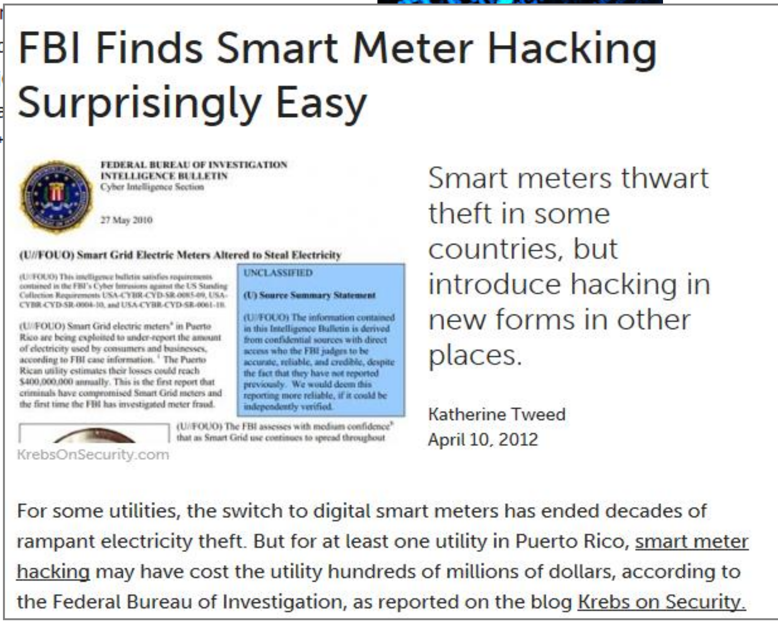
Incluye cable para osciloscopio MINI DIN - BNC (2), cable de comunicaciones USB A - USB B, cable adaptador para Red eléctrica, cable RJ45 para Ethernet y tarjeta de memoria MMC/SD.

MT3120
Herramienta de medida PRIME

El MT3120 es un equipo destinado a efectuar medidas de las características básicas de las comunicaciones basadas en el estándar PRIME sobre la red eléctrica de fuerza (PLC, Power Line Communication).

Incluye cable de comunicaciones USB A - USB B y cable adaptador para Red eléctrica.

Website designed by CRWebZaragoza.com. All right reserved



FBI Finds Smart Meter Hacking Surprisingly Easy

FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

27 May 2010

(U//FOUO) Smart Grid Electric Meters Altered to Steal Electricity

(U//FOUO) This intelligence bulletin satisfies requirements contained in the FBI's Cyber Intrusions against the US Standing Collection Requirements USA-CYBR-CYD-SR-0085-09, USA-CYBR-CYD-SR-0004-10, and USA-CYBR-CYD-SR-0061-10.

(U//FOUO) Smart Grid electric meters[a] in Puerto Rico are being exploited to under-report the amount of electricity used by consumers and businesses, according to FBI case information.[1] The Puerto Rican utility estimates their losses could reach $400,000,000 annually. This is the first report that criminals have compromised Smart Grid meters and the first time the FBI has investigated meter fraud.

UNCLASSIFIED

(U) Source Summary Statement

(U//FOUO) The information contained in this Intelligence Bulletin is derived from confidential sources with direct access who the FBI judges to be accurate, reliable, and credible, despite the fact that they have not reported previously. We would deem this reporting more reliable, if it could be independently verified.

(U//FOUO) The FBI assesses with medium confidence[b] that as Smart Grid use continues to spread throughout

Smart meters thwart theft in some countries, but introduce hacking in new forms in other places.

Katherine Tweed
April 10, 2012

For some utilities, the switch to digital smart meters has ended decades of rampant electricity theft. But for at least one utility in Puerto Rico, smart meter hacking may have cost the utility hundreds of millions of dollars, according to the Federal Bureau of Investigation, as reported on the blog Krebs on Security.

RISK MANAGEMENT – IBERDROLA’S CASE

- Cybersecurity is a real problem and utilities need to face it.
- Senior Management commitment is needed.

*“**Addressing cybersecurity is critical** to enhancing the security and reliability of the nation’s electric grid” – U.S. Department of Energy*

*“Lack of NIS can **compromise vital services** depending on the integrity of network and information systems” – NIS Directive*

RISK MANAGEMENT INITIATIVES IN EUROPE

European Union is fostering Network and Information Security (NIS) through different initiatives that try to respond to the NIS Directive.

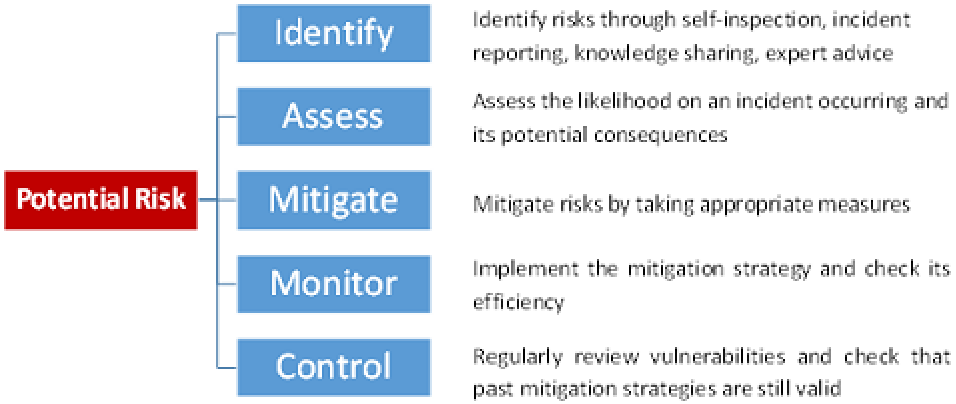
One of those initiatives is the DG CONNECT NIS Platform, a public-private initiative to identify good cybersecurity practices across the value chain and create favorable market conditions for the development and adoption of secure ICT solutions.

Other initiatives, more specific for the electric sector are:

- Smart Grids Stakeholder Forum
- ENISA (ISC/SCADA and Security measures for Smart Grids)
- DG ENER DPIA
- Etc.

RISK MANAGEMENT DEFINITION

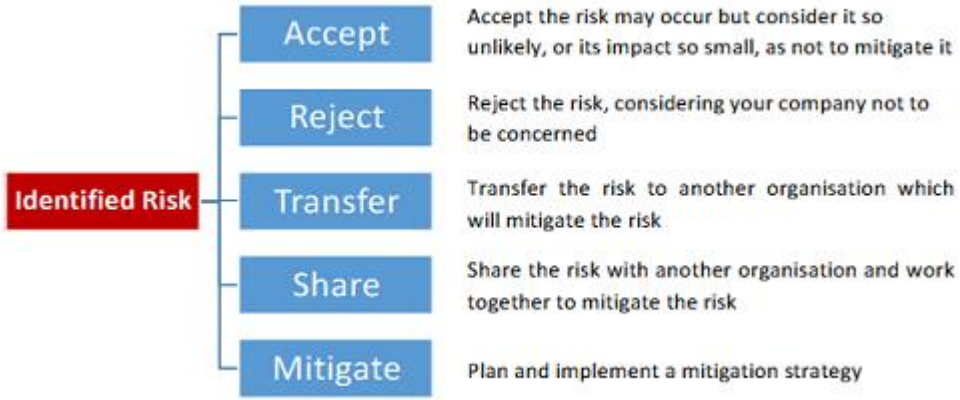
Risk management is the process of identifying , assessing and responding to risk.



Potential Risk

Identify	Identify risks through self-inspection, incident reporting, knowledge sharing, expert advice
Assess	Assess the likelihood on an incident occurring and its potential consequences
Mitigate	Mitigate risks by taking appropriate measures
Monitor	Implement the mitigation strategy and check its efficiency
Control	Regularly review vulnerabilities and check that past mitigation strategies are still valid

With this information, organizations must determine its level of risk tolerance



Identified Risk

Accept	Accept the risk may occur but consider it so unlikely, or its impact so small, as not to mitigate it
Reject	Reject the risk, considering your company not to be concerned
Transfer	Transfer the risk to another organisation which will mitigate the risk
Share	Share the risk with another organisation and work together to mitigate the risk
Mitigate	Plan and implement a mitigation strategy

RISK MANAGEMENT – IBERDROLA'S CASE

IBERDROLA's RISK MANAGEMENT

Iberdrola has a multi-layer approach where corporate security define the global policies and each business, based on their knowledge and experience, apply the specific measures.

Each business area (Generation, Networks, IT, etc.) is responsible for their own risk assessment and define its risk tolerance.

These multi-layer approach make a clear difference between IT and OT due to the different nature of the assets operated and the nature of each business.

IBERDROLA NETWORKS RISK MANAGEMENT

Iberdrola Networks in Spain includes all the Distribution Networks and Telecommunications for the areas covered, as of today:

- + 4MM smart meters installed for a total of 11MM meter
- + 20.000 Data Concentrators installed and communicating with HES for a total of 80.000 Data Concentrators
- + 5.000 Supervision and Automation RTUs

* Legal requirement to install all the smart meters by 2018.

To secure all these infrastructure, risk management planning is a key aspect to address potential risks and vulnerabilities.

RISK MANAGEMENT – IBERDROLA’S CASE

IBERDROLA NETWORKS RISK MANAGEMENT

Iberdrola Networks, with the support of its senior management, has performed different risk assessments in the past years, in order to Identify the risks, assess its impact and plan the solutions to mitigate those risks, in a compatible solution with the installation legal requirement:

- 2011-2012 risk assessment with S21Sec and EPRI
- 2013 risk assessment with INDRA (project specific)
- 2013-2014 risk assessment with EPRI

After the Identify and Assess phases have been completed, the Implement, Monitor and Control phases are in progress.

RISK MANAGEMENT – IBERDROLA'S CASE

IBERDROLA NETWORKS RISK MANAGEMENT (1)

A first risk analysis phase was performed in 2011-2012, covering the different areas and technologies applied:

- Smart Metering infrastructure (including Meter, Data Concentrator and HES) and its communications
- Automation RTUs communications
- SCADA

Three primary objectives in cybersecurity where taken into account:

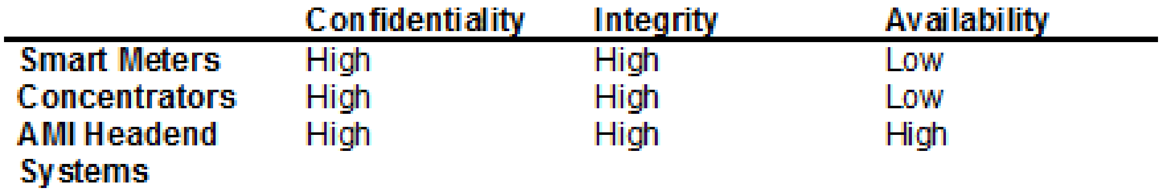
- Confidentiality
- Integrity
- Availability

And three additional security objectives (Authentication, Auditability and Non-repudiation)

For that first analysis of risks and possible solutions, Iberdrola had the help of **S21sec and EPRI**.

IBERDROLA NETWORKS RISK MANAGEMENT (1)

The three security objectives where analyzed for the devices/systems of the metering solution



	Confidentiality	Integrity	Availability
Smart Meters	High	High	Low
Concentrators	High	High	Low
AMI Headend Systems	High	High	High

Security requirements were matched to potential risks in the devices/systems like Access Control, Awareness and Training, Audit and Accountability…

Smart Grid Cyber Security Requirements from NISTIR 7628, *Guidelines for Smart Grid Cyber Security*	Use and Potential Risk Factors
Access Control (SG.AC)	
SG.AC-6: Separation of Duties	Applicable: meter, concentrator, headend. Potential risk: Without separation of duties, a malicious or non-malicious cyber security event could impact multiple devices in the AMI system.
SG.AC-7: Least Privilege	Applicable: concentrator, headend. (Recommended by S21sec for the concentrator.) Potential risk: Ensures that a user does not have "superuser" privileges to all devices and to minimize the likelihood of successful privilege escalation attacks. As discussed with Iberdrola, field technicians typically want this type of access. To address the potential risk, Iberdrola is proposing that sensitive data (such as cryptographic keys) be provided to field technicians through a separate network.

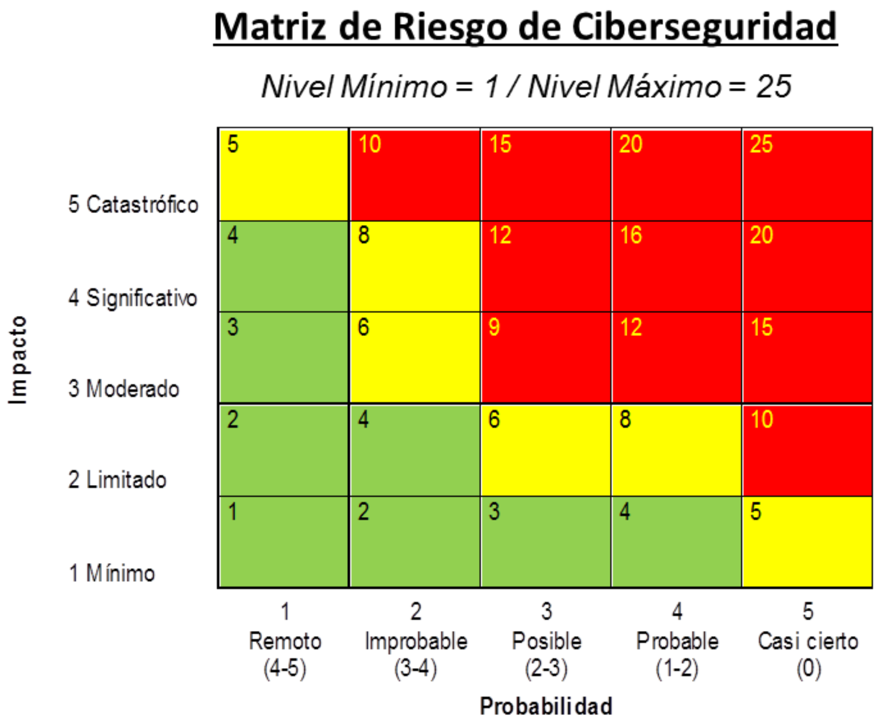
RISK MANAGEMENT – IBERDROLA'S CASE

IBERDROLA DISTRIBUCIÓN ELÉCTRICA

IBERDROLA NETWORKS RISK MANAGEMENT (1)

The level of risk and priorities are defines based on the impact and likelihood of the risks.

An action plan was defined according to the priorities defined.



Matriz de Riesgo de Ciberseguridad

Nivel Mínimo = 1 / Nivel Máximo = 25

Impacto	1 Remoto (4-5)	2 Improbable (3-4)	3 Posible (2-3)	4 Probable (1-2)	5 Casi cierto (0)
5 Catastrófico	🟨 5	🟥 10	🟥 15	🟥 20	🟥 25
4 Significativo	🟩 4	🟨 8	🟥 12	🟥 16	🟥 20
3 Moderado	🟩 3	🟨 6	🟥 9	🟥 12	🟥 15
2 Limitado	🟩 2	🟩 4	🟨 6	🟨 8	🟥 10
1 Mínimo	🟩 1	🟩 2	🟩 3	🟩 4	🟨 5

Probabilidad

Impacto en términos:

- Financieros
- Reputacionales
- Operacionales
- De cumplimiento

Probabilidad:
Estimada a partir del resultado de los cuestionarios

IBERDROLA NETWORKS RISK MANAGEMENT (1)

Based on a matrix evaluation methodology, the possible solutions where evaluated in order to be prioritized, as resources are limited and have to be used efficiently.

		Esfuerzo Económico		
		Bajo	Medio	Alto
Facilidad de implantación	Difícil	Medio	Alto	Alto
	Medio	Bajo	Medio	Alto
	Fácil	Bajo	Bajo	Medio

		COSTE		
		Alto	Medio	Bajo
BENEFICIO	Alto	Medio	Alto	Alto
	Medio	Bajo	Medio	Alto
	Bajo	Bajo	Bajo	Medio

ID	Solución	Excluye a	Benef.	Facil.	Esfuer.	Coste	Comentarios
13	Aplicar medidas de protección al sistema de autenticación web.		🟩	🟨	🟨	🟨	
14	Utilización de mecanismos de autenticación externos.		🟨	🟨	🟨	🟨	
15	Aplicar timeouts en sesiones.		🟨	🟩	🟩	▨	

IBERDROLA NETWORKS RISK MANAGEMENT (2)

In 2013, with the risks identified with EPRI and S21Sec, Iberdrola prioritized the possible mitigations, and as a result of the Implementation phase of Risk Management, a thorough project with INDRA was launched to address cybersecurity in the different areas of Iberdrola's smart grids architecture.

Based on the priorities identified in 2011-2012, this project has different phases in time in order to achieve partial objectives in a short period of time.

The first priority is to secure the already installed RTU's, meters and concentrators, so the solution can be used for the new ones.

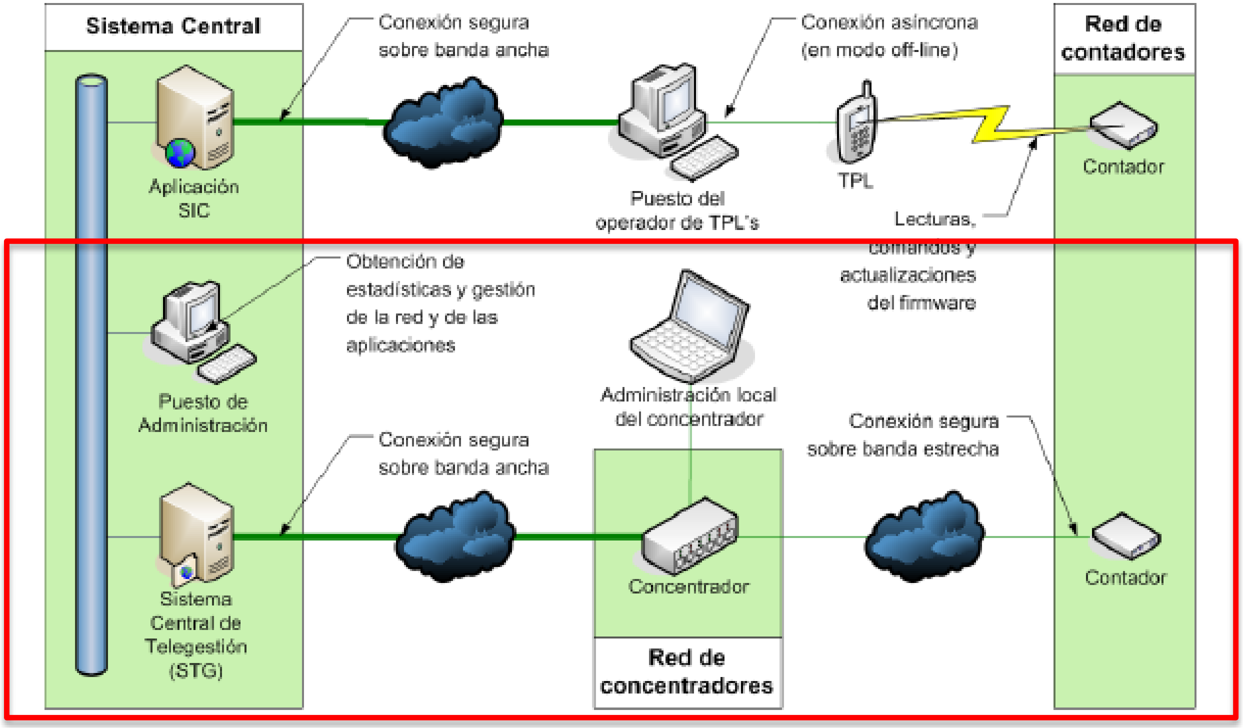
During the project, a second risk assessment was performed within a working group including the main CN and DC manufacturers in order to set up the more suitable security solution for the already installed devices (short term) and the latest and state-of-the-art solution for the new ones (mid term).

RISK MANAGEMENT – IBERDROLA'S CASE

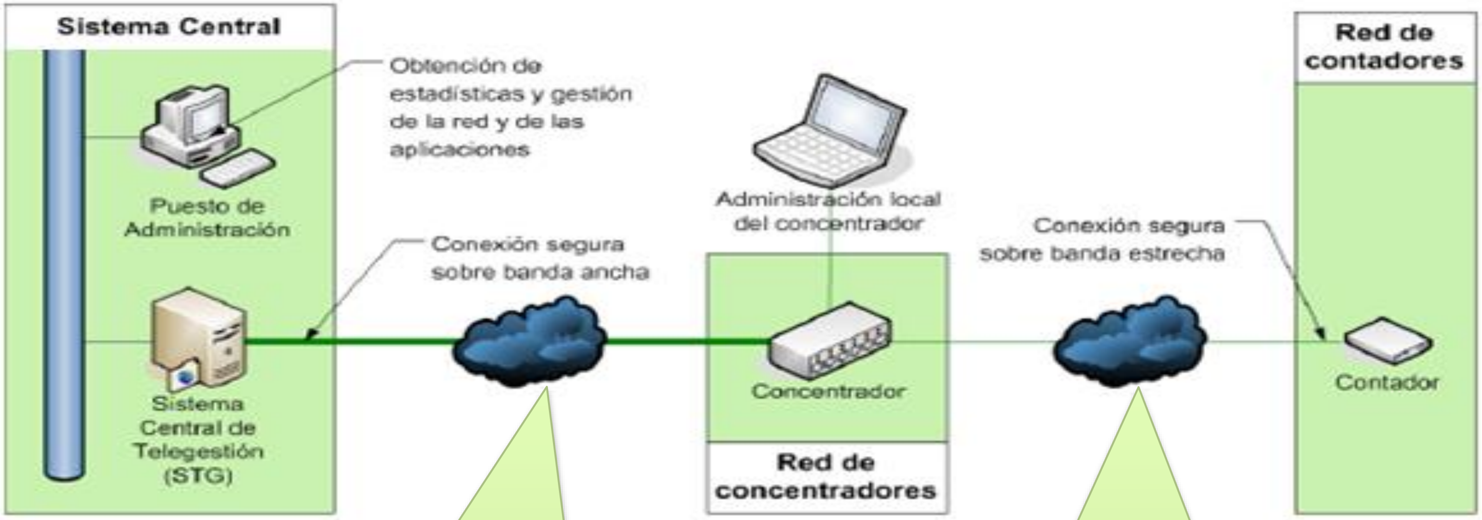
IBERDROLA NETWORKS RISK MANAGEMENT (2)

The different areas faced in the project in first stage are:

- Last mile – Meters, DCs and its communications
- TCP/IP protocols communications – RTUs, DC and HES


Sistema Central
Conexión segura sobre banda ancha
Conexión asíncrona (en modo off-line)
Red de contadores
Aplicación SIC
Puesto del operador de TPL's
TPL
Contador
Lecturas, comandos y actualizaciones del firmware
Obtención de estadísticas y gestión de la red y de las aplicaciones
Puesto de Administración
Administración local del concentrador
Conexión segura sobre banda ancha
Conexión segura sobre banda estrecha
Concentrador
Contador
Sistema Central de Telegestión (STG)
Red de concentradores

IBERDROLA NETWORKS RISK MANAGEMENT (2)


Sistema Central
Obtención de estadísticas y gestión de la red y de las aplicaciones
Puesto de Administración
Conexión segura sobre banda ancha
Sistema Central de Telegestión (STG)
Administración local del concentrador
Concentrador
Red de concentradores
Conexión segura sobre banda estrecha
Red de contadores
Contador

TCP/IP Protocols

- IP Protocol securization with certificates
- Local and remote access control
- System authentication

Last Mile – Metering comms:

- DLMS/COSEM over PRIME
- Authentication and Encryption of all messages.
- Unique keys per meter

IBERDROLA NETWORKS RISK MANAGEMENT (3)

In 2013 a third risk assessment is carried out with EPRI, in order to have a second point of view on the smart metering architecture, its specific implementation and the testing procedures defined for the project.

Besides, a SCADA security requirement review was performed in order to identify possible weaknesses.

Two different documents with gaps and activities to perform where issued as a result of this last analysis:

- Iberdrola ami assessment 05-13-14
- SP SCADA doc comments 05-13-14

RISK MANAGEMENT – IBERDROLA'S CASE

IBERDROLA NETWORKS RISK MANAGEMENT - CONCLUSIONS

Iberdrola is fully aware of the cybersecurity risks arisen with the arrival of the smart grids.

Senior management is strongly committed with the cybersecurity objectives, supporting the different initiatives carried out so far.

To secure its infrastructure, risk management planning is a key aspect for Iberdrola to address potential risks and vulnerabilities.

RISK MANAGEMENT – IBERDROLA'S CASE

IBERDROLA NETWORKS RISK MANAGEMENT - CONCLUSIONS

Iberdrola has an implementation plan to progressively introduce and increase the level of cybersecurity in all its networks during the following years.

This plan is in place since 2013 and covers both legacy already installed devices and new devices with security by design.

The approach followed by Iberdrola, deploying meters without security and upgrading them when the protocols are mature enough, allowed the company to comply with the demanding legal requirements for meter installation.

As part of this planned strategy, periodic risk assessment should be carried out in order to assess the level of compliance and update the potential risks in place.