ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Agosto

2014

Rapporto tecnico N.51

Terms of Reference for the trials

Antonio Diu

Consiglio Nazionale delle Ricerche
CERIS Istituto di Ricerche sull'Impresa e Lo Sviluppo

RAPPORTO TECNICO CNR-CERIS

Anno 9, N° 51; Agosto 2014

Direttore Responsabile

Secondo Rolfo

Direzione e Redazione

CNR-Ceris
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
www.ceris.cnr.it

Sede di Roma

Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano

Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione

Enrico Viarisio
e.viarisio@ceris.cnr.it

ESSENCE

***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment*

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

The Essence project is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.

Networked computers reside at the heart of critical infrastructures, these are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, and expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber security of control and communication systems is now very strong worldwide. To that aim, several frameworks have been developed or are under development at present, both in the form of guidelines and proper standards, but it is difficult to evaluate costs and benefits of their adoption, although experimentation so far has shown that they may be huge.

In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts;
2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;
4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

Partners of the project are:

CNR-Ceris *(Coordinator) (Italy);* Università del Piemonte Orientale Amedeo Avogadro *(Italy);*
Deloitte Advisory S.L. *(Spain);* Antonio Diu Masferrer Nueva Empresa SLNE *(Spain);*
Enel Ingegneria e Ricerca S.p.A. *(Italy);* Abb S.p.A. – Power systhems division *(Italy);*
IEN - Institute of power engineering *(Poland);* PSE – Operator SA *(Poland).*

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs
The Commission is not responsible for any use that may be made of the information contained therein, the sole responsibility lies with the authors.

Terms of Reference for the trials

Antonio Diu[1]

ADConsulting
Cooperativa, 17, 08302 - Mataró -
Tel. +34.607.798.444
Tel. +34.93.798.4444
Mail: antonidiu@gmail.com

ABSTRACT: The aim of the report "Terms of Reference for the trials" is to carefully present the impact of malicious incidents, or natural ones, on the main layers of an electric system. The single components of the service, physical, communication and cyber layer have been described and a procedure for the estimation of the possible damage of an incident has been reported. Attacks might affect large portions of the European power system, make restoration difficult and cause huge societal impact. In fact, due to the interconnection of the networks, a blackout in one or more countries could derive from an attack directed to neighbouring countries facilities, Thus there is a need for establishing the economic and organisational impact of the implementation of emerging cyber security frameworks in Europe. Cyber security needs first of all to define tests to verify the impact of standard procedure or countermeasures designed to limit the consequences of incidents on each layer. The report presents the test in order to verify: the security criteria and calculate the operative costs; apply the emergency or attach scenario; apply standards and countermeasures and evaluate the standards and countermeasures. The objective of this project is to identify costs and benefits for industrial stakeholders and for the society on an objective basis, and outline organisational processes wherever beneficial. To do so, a general procedure has been designed and applied on two particular cases of cyber-attacks: a SCADA based Control System operated by a TSO; a control room of a thermal Power Plant, operated by a generation utility. Along the text of this report, the aspects related to the physical system are included only to have a global view of potential attacks and the standards and countermeasures that will potentially reduce the vulnerability of the systems or speed up the restoration.

KEYWORDS: cyber security, malicious attack, power control center, hardware breakdown, security standards, power threats, scenarios definition, evaluation criteria

JEL CODE: L94, H43, L51

[1] This report is the output of the activity "Terms of reference of the trials", which was coordinated by Antonio Diu, and was based on the work of Marco Biancardi, Hanna Burczy, Luca Guidi, Gabriele Nani, Daniela Pestonesi, Elena Ragazzi and Alberto Stefanini.

SUMMARY

1. RATIONALE

Nowadays Large Complex Critical Infrastructures (LCCI) are operated and monitored thorough complex IT Systems and electric systems are not an exception.

Extraordinary natural phenomena or human made malicious attacks can be directed against the physical elements of the system or to the IT systems that control system operations.

IT systems allow the operators to receive real time information from the field and rely on a number of processes and applications that assist them to take decisions.

IT systems permit the operator to execute the decisions taken in order to change the generation and voltage profiles or introduce changes in the system topology which will modify the system flows. In exceptional occasions can also reduce the system demand.

Malicious attacks may target IT systems to disturb the control of the system or to impact to the physical system in order to produce local, regional or national blackouts.

The IT systems under possible threats are:

a. The computer systems placed in Control Rooms at control National, Regional and Local Systems to limit the operators automatic or manual control capacity.
b. The power plants control rooms that may modify the generation profile or even impact in the security of some of the power plant elements.
c. Substations, that in most cases are unattended, the IT local and remote supervisory control and data acquisitions (SCADA's) or the Intelligent Electronic Devices (IED) placed in substations with the mission to control and protect their active elements.
d. The intensive use of communications, public and private, to link all those elements are at the same time possible targets for malicious activity.

The Control IT Systems are sensitive to extraordinary meteorological incidents that may impact on their availability or performance, but are also attractive for malicious attacks due to the impunity for the attacker who acts away from the Control Centres in case of hijack.

The impact of these threats is twofold:

a. Reduce the control capacity of system operators by limiting their information, with consequences in the decision making processes, or reducing its capacity to implement those decisions. This situation will carry an immediate loss of control over the system which in the medium term, if not corrected, may impact on the electric energy users.
b. The malicious use of the IT systems may directly impact on the physical layer and modify topology, generation or any other system parameter. This may influence into the system performance and

produce loss of some of the services given to system clients. The consequences are potentially the worst for the system including their main elements as generators or substations.

The cyber security has been presented always as one of the main concern in the electric systems management.

Networked computers reside at the heart of critical infrastructures and systems on which people rely on, such as the power grid. Today, many such systems are vulnerable to cyber-attacks that can inhibit their operations, corrupt valuable data, expose private information or even directly impact into the physical system elements.

Attacks might affect large portions of the European power system, make restoration difficult and cause huge societal impact.

Thus there is a need for establishing the economic and organisational impact of the implementation of emerging cyber security frameworks in Europe. The objective of ESSENCE is to identify costs and benefits for industrial stakeholders and for the society on an objective basis, and outline organisational processes wherever beneficial.

In order to improve cyber security, Standards against cyber-attacks testing is a part of the ESSENCE project that will evaluate their effectiveness evaluated in order to come to an assessment of the economic impact for the firms applying them and for customers who benefit of increased security and continuity of supply.

To do so, a general procedure has been designed and applied on two particular cases of cyber-attacks:

1. A SCADA based Control System operated by a TSO

2. A Control room of a thermal Power Plant, operated by a generation utility.

Along the text of this document, the aspects related to the physical system are included only for the sake of completeness, to have a global view of potential attacks and the standards and countermeasures that will potentially reduce the vulnerability of the systems or speed up the restoration.

2. ELECTRIC SYSTEM STRUCTURE AND THREATS

Electric Systems are Very Large and Complex Critical Infrastructures and can be traced as formed in four layers:

a. **Service Layer,** constituted by all services provided by the system itself to all those clients, as final users of the electricity, and other infrastructures that has the electric system as part of the infrastructure.

b. **Physical Layer**, as the assembly of all physical elements of the electric systems, from power plants to a single breaker.

c. **Communication Layer**, as part of the communication infrastructure and used by the electric system as part of it and for critical purposes.

d. **Cyber Layer**, as the assembly of electronic and IT equipment that supports the Electric System for critical purposes.

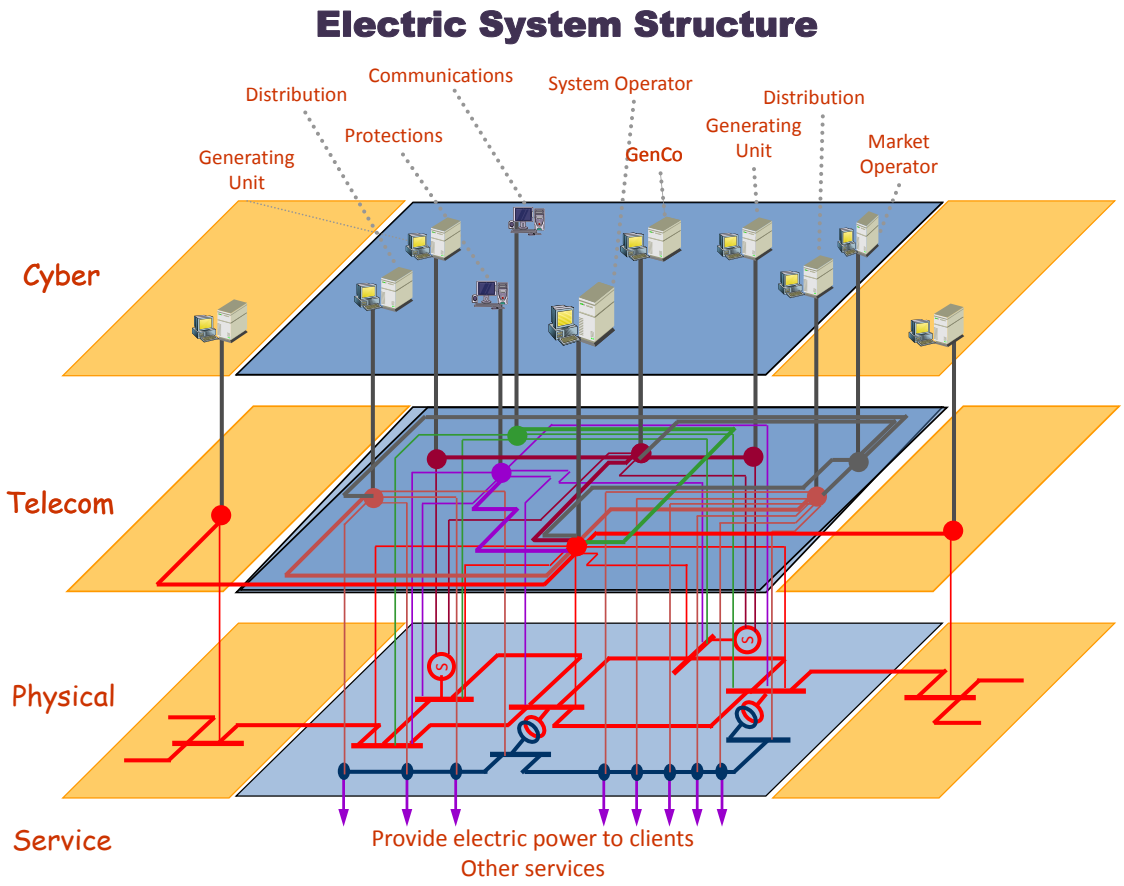
The four Layers have specific functionality and can be differently hurt by natural or malicious causes.

To protect itself for these incidents, different protections and countermeasures can be adopted:

a. **Part of the procedures** of infrastructure protection oriented to defend the system against natural ordinary causes, with a certain probability to take place, like overloads or short circuits. These procedures has been developed, tested and developed in recent years.

b. **Part of emergency procedures** oriented to limit the extension and deepness of any incident or to accelerate the system restoration. These procedures had the peculiarity to be specifically designed for each system and for each system condition.

c. **Part of new standards** oriented to deal with malicious actions against the whole system or parts of it. These Standards will be evaluated for different situation and in different systems.



2.1 Service Layer

The main and principal mission of an Electric System is to deliver the requested electric energy at any instant with the due continuity and wave quality, as Voltage, Frequency…

But the electricity infrastructure is also used as a service for other utilities. So the protection offered byu the Electric System Security is shared with other Critical infrastructures. In the cases when for any incident part of the electric physical infrastructure is damaged, some of these by-product services are also lost.

An example clarifies the concept: In all electric system lines there is, on top of the tower that support them, one (or in some cases two) guard cable, connected to ground and with the main mission to protect the line against lighting during storms. This guard cable contains inside fibre optics that have a high communication capacity. Part of this capacity is used for operations and protections of the electric system itself and the rest is made available to communication operators to be used as part of their infrastructure. In this case, if the line is damaged, the transmission capacity is lost for the electric system, causing or not the loss of electric supply for some of the system clients but also is lost the communication capacity provided to the communication operators.

In general the electric infrastructure is accessible to anyone due the fact that almost all its high voltage elements are spread throughout the territory, without any protection or inside areas unattended, located in isolated areas and with a light protection.

This physical system will be considered in the following points.

The Service is the most attractive layer for malicious attacks, due to the remarkable reactions of the electric system against malicious actions:

a. Impact on the general electricity users consists in the loss of capacity in using electric energy for a certain period of time. The impact is on the comfort of the citizens, any elements that use electricity as primary energy cannot be used (house appliances, elevators, heating…)
b. Impact on the industrial and commercial uses of electricity, making impossible to continue their activities.
c. Immediately impact on other infrastructures that in some cases will stop to supply their services to same clients: communications, transport, banking and so on
d. The damage produced over the comfort of the population and the economy of the area affected can be controlled during the malicious attacks. The damage of one or two lines could produce a blackout that can be restored by the electric company in minutes or hours. The damage of, as example, most of the high voltage transformers in the same area, may cause a damage that can last for days or weeks.
e. The damage produced directly against the clients is controllable and limited. In cases of blackout there will not be individuals directly hurt and only some side effects could take place due the fails in other infrastructures like Health (hospitals as example).

f. The effects of the incident are immediately reflected and made public. There is no way to hide the incident that impact the continuity of electric service in areas of the country.
g. The system, formed by thousands of kilometres of lines, is impossible to completely protect and this circumstance is a point in favour of the attackers, because they have plenty of time to prepare and easy escape.

The high number of clients makes more feasible to attack the service layer by impacting on the other layers so indirectly will cause damage to a maximum number of clients and services.

2.2 Physical Layer

Physical Layer is formed by all physical elements that form the electric network.

The electric network is composed by

a. Nodes represented by the different Busbars in Substations. Two aspects will be considered regarding substations.
    i. The substation itself as objective of malicious attacks or being damaged by any natural disaster.
    ii. Elements that uses the substation to be connected to the system. In this field two are more relevant than others: Power Plants and big consumers.
b. Arcs represented by lines and transformers.

In general all technologies and applications used in the network are applicable to the electric network.

2.2.1 *Substations*

Substations represent the nodes of the electric network and are the place where lines gets connected among them to form the network.

It contains not only all the connecting equipment but also transformers among different Voltage levels and all the IT systems needed to protect the lines and facilitate information and control actions capacity to the different Control Centres.

Substations are unattended and disperse in the territory. Normally are protected by a fence and electronic means. But we will consider that the:

a. The Fence only retards the malicious attack and is effective only if the time to violate the fence is bigger than the time to detect the attack plus time for security forces to react plus time that will take them to be present in the substation, and prevent or abort the attack.
b. The substation can be attacked from outside, without the need to enter in the substation: drop bombs or use of high calibre rifles to produce the damage.

The substation is full of sensitive elements, the damage of them may cause serious problems in the continuity of supply:

a. A Busbar or the node where different elements are connected. Its main characteristic is the Voltage level.
b. Bays of Lines. A bay is the union of equipment used to connect a single element to the Busbar. In general is formed by
    i. Breaker (or breakers) as the elements that will interrupt the electricity continuity between the element and the Busbar. Could be operated by hand or by electronic elements that will detect the presence of short circuits in the element and which mission is to isolate the faulted area of the element.
    ii. Isolators or elements dedicated to modify the topology of the system, when there is no electricity circulation through it.
    iii. Measurement equipment. It is used to measure the only two parameters relative to electric systems: voltage (in volt) and Flow (in Amperes). All other parameters will result by these two. This equipment includes Voltage transformers (TT) and Current Transformers (CT).
    iv. Electronic equipment, especially protections, dedicated to detect anomaly conditions and eliminate them by isolating the fault causes by opening the adequate breakers.
    v. Transformers to modify the voltage and connect two (or three) different voltage levels.
    vi. Transformer bays oriented to connect the transformer to the Busbars (in all voltage sides). Transformer bays are equipped by the same elements than a line bay with capacities and protections adequate to a transformer, but with the same objectives.
    vii. Communication elements, used to facilitate the information and control capacity to the Control Centre. Also some protections require secure communications (with the other side of the protected element) to correctly operate.
    viii. Protections are electronic elements that detect short circuits in the system and have the mission to isolate them as soon as possible (in general, in milliseconds, in order to not cause instability in the system that will carry large regions blackout.
    ix. IT systems to collect the information from the field and send it to the Control Centre. The same equipment will receive orders from the centre to operate, among others, the breakers.
    x. Auxiliary equipment, as elements without a main role but absolutely needed for the right substation operation like: AC and DC supply…

Most of this equipment is highly sensitive to malicious or natural effects.

A review of the potential damage and some of the effects will be analysed in the following points.

To start with will be said that there is not a fixed rule about which damage may cause any action. In the following points we will only assume the most probable damage and consequences of a successful malicious attack.

2.2.1.1 Global Substation

A substation is a facility covering a huge extension of land, filled with electric elements. Certainly any circumstance that may damage or destroy one substation will generate a considerable incident in the network. Substations do not have other spare substations to support their loss.

In most cases, the total destruction will carry a relatively extended blackout and its reparation will last for weeks.

Meanwhile, the system can recover part of their elements by direct connections, probably outside the substation, but all services connected to it will be loss: generations or big clients.

Consequences could be a more than probable blackout that will last for hours or days and later on some potential restrictions in the electric supply like total amount of energy limitations.

2.2.1.2 Busbar

Busbars are one of the elements excluded from the most of the Security Criteria elements included in the Grid Code. That means that the system is not designed to support the loss of any Busbar.

If a busbar is successfully damaged, that will carry the loss of any element connected to it (lines and transformers) most of these incidents will carry a blackout, depending on the network conditions and the number of elements connected to the Busbar.

Reparation of the Busbar itself could be easy and do not imply sophisticated elements or operations. In case that by any circumstance the Busbar could not be repaired immediately, lines or transformers could be given continuity by connecting them directly and modifying the setup of protections.

In general a potential blackout has in this case a medium duration.

2.2.1.3 Breakers and isolators

Each breaker will automatically leave out of service the elements that use it to connect to Busbar.

System is designed and prepared to survive to the loss of a single element, so there will not be any consequence to the system. Breaker can be substituted in hours or days, regarding the availability of spare parts.

2.2.1.4 Measurement equipment

Values obtained from the measurement elements are used for controlling the magnitudes and flows in the system in order to react if some of them is out of limits. Also and more important, they are used for system protections. Losing the measurements will carry the loss of the protections (this will be dealt further on).

In the particular case of Current transformers, if it remains connected with the low voltage circuit open, it may cause an explosion which may affect to adjacent elements.

2.2.1.5 Communications

Normally communications have alternative routes and the loss of one of them will not impact in the system security or capacity to be controlled.

Only the loss of some specific communications used by protections may cause problems to the network. This aspect is considered in the following points.

2.2.1.6 Protections

In case of a short circuit in any part of the system, if it is not isolated immediately, will carry stability problems that will end up in an extended blackout. To isolate the short circuit, a protection is set in the system designed to eliminate short circuits in a range of milliseconds and has the necessary selectivity in order to remove from the system only the elements directly affected by the short circuit.

Protections use measures from the field to take the decisions and breakers to execute them. Those elements in addition to the protection equipment forms the basics of the protection system.

Protection equipment can be located in a single room in the control area or in small bay housing where are located the protections for few elements.

If protections are leaved out of service, the elements protected will be leaved out of service too.

Restoration of damaged protections may take hours depending on the availability of spare parts.

2.2.2 *Generators*

Generators are elements that transform other primary energy sources (water, gas, oil, nuclear, wind…) to electric energy.

Generators are complex systems that integrate different subsystems which could be subject of extraordinary incidents or malicious activity:

2.2.2.1 Primary Energy source

The storage and the transportation of fuel to the power plant are subject of natural disasters or malicious attacks.

a. **Fuel Oil and Gas** powered plants have normally a combination of storage facilities in the power plant and direct supply from other bigger reserves of an independent company. Affecting the storage capacity or the outside direct supply may provoke the interruption of the power plant.
b. **Nuclear Power Plants** has normally fuel storage in the facilities for one or more years, located in the fuel pools inside the power plant facilities. It is very difficult to manipulate, but wrong manipulation or a malicious operation with them may cause a nuclear disaster. In any case nuclear power plants are provided with the highest levels of security. The consequences of a natural disaster or a successful attack will exceed by a large margin the electric system impact.

c. **Water Power Plants** primary energy is stored in dams and transported with under pressure tubes. Disasters to the barrier of the dam have an impact bigger that the loss of the power plant for weeks or months. Damages into the pressurized tubes will cause direct damage to population and will leave the power plant out of service for weeks.
d. **Wind and solar generation** have a natural continuous supply and there is not any opportunity to damage. Only in cases of extraordinary wind speed, exceeding the design security criteria may seriously damage the power plant, living it out of service for months.

For what has been said above, the primary energy storage must be considered as a vulnerability of the power plants, especially in the case of Nuclear Power Plants and in the water storage.

2.2.2.2 Turbines and generators

Turbines and generators are the rotating parts of the unit.

Turbine is the responsible to convert the primary energy in rotating mechanical energy. Turbines can be in general moved by water, steam or wind.

Generators are the ones that convert the mechanical rotating energy into electrical energy.

Both elements, including the axe that transmit the rotation from the turbine to the generator, are normally accessible and may cause serious impact to the system if affected during the incident, especially due to the long reparation time.

2.2.3 *Control and protection subsystem*

The physical elements in a substation can be operated automatically from the equipment itself but for a more secure operation, can be also operated from the substation control room. To facilitate, the operation can be done by a cabling from the elements to the control room or by placing a mini SCADA system and transmit the orders to elements using communication protocols. This more advanced methodology known as "Substation Automate" provide to local operator with enough information.

In case of a short circuit it is necessary to isolate the element (line, Busbar or transformer) that has suffered it as soon as possible. To do so, the protections system is permanently watching the main parameters (Voltage and Current) of the protected element and, in case of detection of a short-circuit, the element will be isolated. The time to measure and give the order to open the breaker is in the range of milliseconds. Longer times put on risk the system stability.

2.2.4 *Connection to the Grid*

Generators are normally connected to the network grid in substations appropriate to their own size. As clients of the substation its availability is subject of the substation availability.

2.3 Communication Layer

Most of the substations and power plants are today unattended. This circumstance has been feasible due to the availability of communication networks that allow control centres to have all the information needed to take decisions and to execute those decisions by operating directly the topology elements in the substations or controlling the power plants.

The topology in any network is defined by the status (open or close) of the different switches in the network. The topology will define the flows in the system. In case of communications, it will define the use of the different communication facilities in the system either in systems with communication channels switches or in cases of data packages' switch. In a Communications control centre the operator can redirect communications in cases of failures of some communications channels. In general those points where the topology can be changed are located in substations and power plants, where SCADA communications are already available.

There are different types of communications, in accordance with the property of the communication support and the use of them:

2.3.1 *Communication Ownership and Technologies*

Traditionally electric utilities had the capacity to build and use for operations their own communication system and used a mix of private and public communications.

There is more control in the private ones, for example the capacity to redirect or repair in case of unavailability of some channel.

Also from the security point of view, a public facility will be easier to penetrate than a privately controlled network, where security criteria can be established considering the use of the communication.

The explosion of Internet has given the possibility to establish point to point communications at low cost, and so it has become a real alternative. The security problem associated with the use of an open and public alternative is being minimized by using some securities at the top of the standard communication protocols (encryption…).

2.3.2 *Communication Technologies*

Communication channels may apply on a wide range of technologies, but it is possible to establish three main groups:

a. **Power Line Carrier or PLC**: Using the high voltage cables as a communication support. This communication is often used for the most transcendent communications use: the protections system, since it is almost impossible the access to a hacker from outside the substations.

b. **Optical Fibre** built inside or wrapped to the grounded cable or to the guard cable: this technology is used internally by the utility for SCADA and control communications or voice communications. But the high capacity given by this technology generates a spare capacity that in many cases is rented to communication operators for public use. The main difference of this mix of private-public communications is that the access to facilities, the maintenance schedule and priority and the operations control is under the utility responsibility.
c. All other communication technologies may be used as private or public communications.
d. Special mention should be given to **smart meters** communications. The communications between meters and concentrators normally use PLC technology through the same cables used to feed the final user. But the communications between concentrators and Meter Values Data-Base normally use different kind of facilities like GSM or radio links. The point is that for a country with 30 Million meters and considering an average of 30 meters for concentrator we are talking of close to 1 million nodes for a communication network. This will give to the communications all problems related to very large networks.

2.3.3 *Communication Protocols*

The Remote Terminal Units (RTU) are pre-programmed to communicate with the central station SCADA and other networked systems in protocols that are designed to deliver reports on the status of all the input and output devices in the field.

Protocols are similar to languages, which allow the RTU/SCADA units to communicate with each other. All network architectures are loosely based on ISO (International Standards Organization) standard seven layer OSI (Open Systems Interconnection).

The protocols used in the communications between the RTU´s and the Control Centre has been modifying its philosophy from a proprietary protocols designed by the SCADA supplier to standard protocols.

This last movement has produced two impacts into the communication system. On one hand it opens the RTU's market to all kind of suppliers but on the other hand anybody may have the protocol structure which makes easiest its violation by hackers.

a. **Proprietary protocols** like Allen Bradley DF1,DH and DH+, GE Fanuc Siemens Sinaut, Mitsubishi, Modbus RTU / ASCII, or Omron among others, have been the most used until the arrival of standard protocols.
b. **Standards protocols**: IEC 60870 part 6 is one of the IEC 60870 set of standards which define systems used by SCADA. The IEC Technical Committee 57 (Working Group 03) has developed part 6 to provide a communication profile for sending basic telecontrol messages between two systems which is compatible with ISO standards and ITU-T recommendations.

These standards include:

- IEC 60870-6-1 Application context and organization of standards
- IEC 60870-6-2 Use of basic standards (OSI layers 1–4)
- IEC 60870-6-501 TASE2.1 Service definitions
- IEC 60870-6-502 TASE.1 Protocol definitions
- IEC 60870-6-503 TASE.2 Services and protocol
- IEC 60870-6-504 TASE.1 User conventions
- IEC 60870-6-601 Functional profile for providing the connection-oriented transport service in an end system connected via permanent access to a packet switched data network
- IEC 60870-6-602 TASE transport profiles
- IEC 60870-6-701 Functional profile for providing the TASE.1 application service in end systems
- IEC 60870-6-702 Functional profile for providing the TASE.2 application service in end systems
- IEC 60870-6-802 TASE.2 Object models

2.4 Cyber Layer

The Cyber layer is formed by the IT system that provides operability to the system. The cyber layer is a hierarchical structure with different functionalities at each level:

a. **Substation Level**: In modern substations the local control is based on IT systems and became the first level in the hierarchy. In some cases the information and operation capacity from few substations are concentrated in one of them becoming an elementary first level of the Control Centre.

b. **Control Centres**: with a more sophisticated information coming from all substations which gives them a superior level of control capacity. Control Centres can be hierarchically located among them, with regional and central Control Centres.

In the following points a description of the functionality is included. Hardware and software will depend on the system supplier meanwhile the functions are similar in all cases.

2.4.1 *Substation Level*

The basic elements of the substation automation are the Intelligent Electronic Devices (IED) that incorporates one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers).

IED technology can help utilities improve reliability, gain operational efficiencies, and enable asset management programs including predictive maintenance, life extensions and improved planning.

The main functionalities provided by this system are:

a. Data collection from the RTU's located in the different bays (or bays grouping) and transmit them to the substation central SCADA
b. Monitor flows, voltages, breakers or isolators positions in the substation and alarms the topology changes or limits violation.
c. Register the information for future analysis. Historic log.
d. Local Supervisory control of breaker's and isolator.
e. Human Machine Interface (HMI)
f. Communication capacity with:
    - the local RTU's to collect information and perform supervisory control actions
    - with other substation, to transfer individualized information or transfer local control
    - with the main Control Centre to act as an RTU, with one or more control centres (regional, national…) using appropriate communication protocols to each centre.

Other potential functionality, available in some vendors:

a. Predictive maintenance through analysis of operating conditions
b. Sophisticated protection algorithms
c. Enables integration of protection systems
d. Provides remote data retrieval & setting capability
e. Common database
f. Web-enabled design
g. Automatic voltage control
h. Synchronism
i. Tap position monitoring
j. Load & bus transfer
k. Load curtailment
l. Capacitor control algorithm
m. Substation maintenance mode
n. Fault detection
o. Sequence of event recorder

[2] TASE: Telecontrol Application Service Elements (IEC communications protocol)

Especial mention must be done to standard protocol IEC 61850 that is a part of the International Electro technical Commission's (IEC) Technical Committee 57 (TC57) reference architecture for electric power systems. The abstract data models defined in IEC 61850 can be mapped to a number of protocols.

These protocols can run over TCP/IP networks or substation LANs using high speed switched ethernet to obtain the necessary response times below four milliseconds for protective relaying.

The use of this protocol in the IED's will allow the mix of different suppliers in the same structure in the substation.

The security of this level of automation, will be considered high if no communications to outside are available. But this circumstance is far away of the reality. In fact there are many communications going in and out of the substation and some of them sharing hardware from the substation like control centre communications, protections set up control, communication network topology control, Other substations information interchange or even switchboards for administrative communications and internal or external voice.

2.4.2 *Control Centre Level*

The Control Centre receives all information of their own Transmission or Distribution System and needed information from the neighbouring, via their Control Centres.

It needs to perform the required security studies in order to guarantee the operability of the system fulfilling the security criteria constrains and providing good quality to Distribution Systems.

The Control Centre will have the capacity to perform supervisory control actions over breakers (if possible also over isolators) and raise/lower actions in the transformer's taps in order to control Voltage in the high Voltage system.

2.4.2.1 Main SCADA functionality, including Supervisory Control

The basic functionalities of the SCADA system are

a. Data Acquisition, basically communication with the different RTU's or digital equipment in case of Substation Automation and stored in the Real Time Data Base.
b. Validate the information received and if detected an out of limits condition, originate the corresponding alarm to the operator.
c. Allow the operator to change status of breakers (and in some cases isolators) which increases the system security and in cases of emergency speeds up the restoration. In case of lines or transformers these breakers will modify the network topology and in case of shunts or capacitors will modify the system conditions, specially the voltage profile.
d. Allow the operator to modify the ratios of transformers in order to avoid recirculation of reactive power and adjust the voltage to the network requirements and possibilities.

e. Fill and maintain the logs with all alarms and incidences in the system for future analysis.

The Load Frequency Control is one of the main tasks in the SCADA, it consists in detecting deviations from the scheduled interchanges with other systems and correct them using the reserves (secondary and later tertiary) in an close loop from the Control Centre.

The main functions to be performed are:

a. Enter all programs (exporting or importing) with other systems interconnected.
b. Calculation of the Area Control Error (ACE) or instantaneous difference between the scheduled and real interchanges plus the schedules and real frequency, multiplied by a factor that represents the relative size of the system in comparison with other partners in the synchronous area.
c. Activate or deactivate power plants to be directly controlled by the Load Frequency Control system.
d. Send orders to the power plants activated in order to reduce the ACE to zero.
e. Register all incidences, deviations and the energy deviation from the scheduled hourly programs.

2.4.2.2 EMS functionality

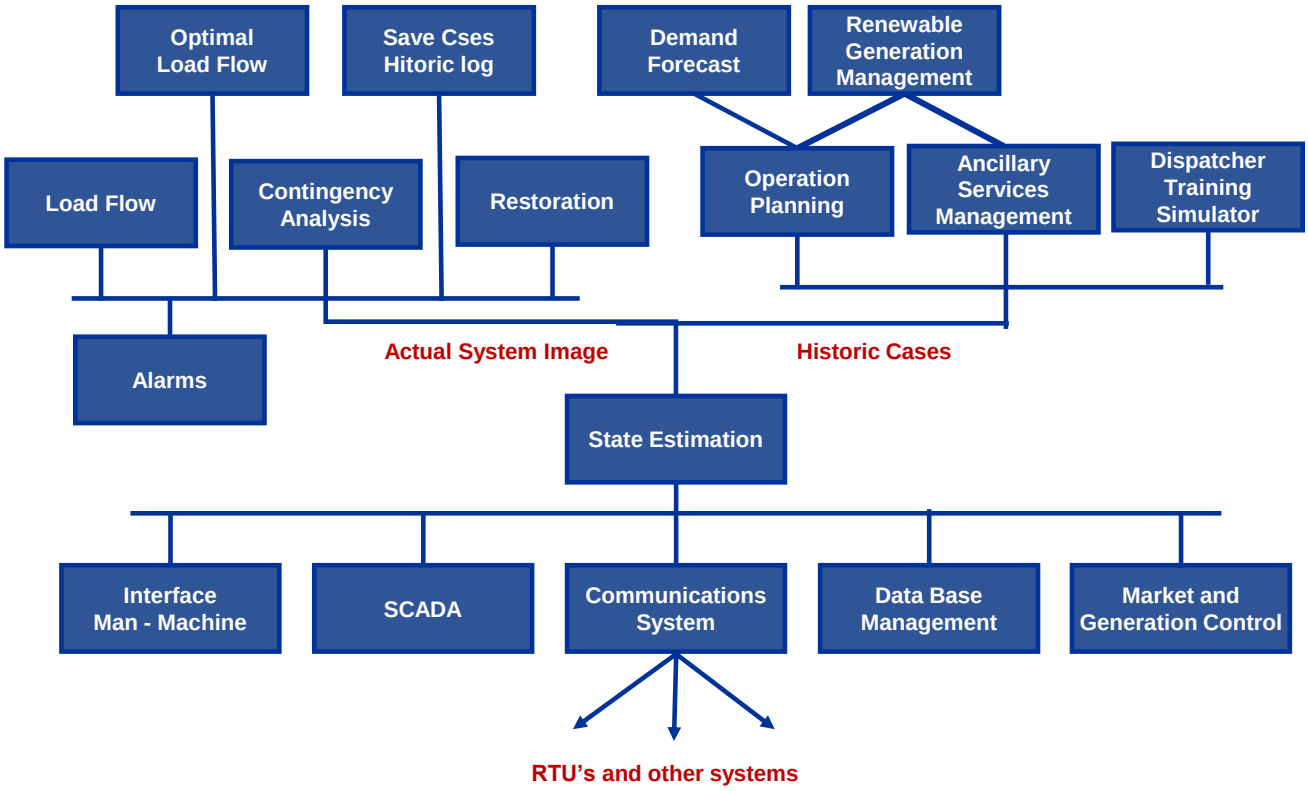
The Energy Management System (EMS) is oriented to perform activities oriented to guarantee the system security and the fulfilment of the security criteria established in the Grid Code or other internal or external codes and rules.

The basic function is the **State Estimator**, which determines the most probable network situation at the time of run. Values received from substations have unavoidable errors, depending on the equipment class or caused by unavailability or damage in measurement equipment.

The State estimator will recalculate the missing values, detect erroneous data and replace them by the most probable one.

The output of the State Estimator is a picture of the system that follows the electric laws (kirchhoff, Ohm…) and can be used as starting point of the remaining security process, among others:

a. Contingency Analysis
b. Operator power flow
c. Optimal Power Flow
d. Save cases for Operation planning or post-mortem studies



2.4.2.3 Advanced functionalities: Renewable Control Centre.

The emergence of renewable energies, also called intermittent energy, and the embedded energy in Distribution Systems makes the Transmission System Operation more complex and unpredictable.

To assist operators in the system control, new facilities and functionalities are needed in the Control Centres. In this case one of the most relevant are the Renewable Energies Control Centre oriented to control in real time their generation and deviations from the programs and in consequence the requirements of more tertiary reserves and in case of security violations, give orders to "generation rejection", reducing to acceptable limits the power generated in Real Time.

3. TEST PROCEDURES.

Some tests are designed to assess the impact of any standard procedure or of a set of countermeasures designed to limit the consequences of malicious human interventions or extreme natural conditions .

The tests will run under different parts of the system: Physical and Cyber.

The procedure designed is the same in both cases but it needs to be customized and adapted to the different circumstances and technological procedures, but the system to calculate the impact of the incidents, and costs of the measures or of the standards adopted is the same.

In general, the simulation of the physical system is more based on numerical calculations over a physical mathematical model of the network while the cyber simulation will be based on more logical models and analysis.

The test procedure has been designed as a general purpose but needs to be customized for the different types of incidents. In the following points the general process will be described and customized for physical and for cyber incidents.

3.1 Base procedure

The procedure is divides in six steps:

a. Define the initial scenario and generates the corresponding base case model and parameters.
b. Verify that the model fulfils the security criteria established and calculates the operative costs to be taken as a base cost.
c. Apply the attack or extreme conditions scenario and calculate the incident costs (including costs incurred by clients due the lack of service)
d. Apply standards and countermeasures. Calculate the investments and operative costs.
e. Apply the attack or extreme conditions scenario and calculate the incident costs (including costs incurred by clients due to the lack of service)
f. Evaluation of the Standards and Countermeasures.

3.1.1 *Initial scenario and Base Case Model*

As starting point the initial scenario is described and particularly:

a. Date of the base case. If some countermeasures are supposed to be in service and some standards in place, there is a need of time to prepare them, so the system will be considered in an immediate future. Of course for the project purposes, any time frame could be considered even the past.
b. Conditions of the system as a base start.
    - Load level, generation profile, topology…
    - Communication topology, system back up availability…

3.1.2 *Verify the security criteria and calculate operative costs*

Normally the regulation provides some security criteria that must be followed by each system. It is responsibility of the operator to guarantee to the regulator that those criteria are fulfilled.

There are sometimes other security criteria established among the TSO or other agents, due to the fact that the global security is guaranteed by the security of all members. There could be some rules, not included in the regulation, but established in the association treaties (ENTSOE and others).

The criteria vary accordingly to the analysed subsystem:

i. For impact in the physical layer due to attacks generated in the cyber or physical layers, the security criteria is based on the tripping probability of some elements presents in the system: lines, generators, transformers…

ii. In the impact into cyber systems could be software, hardware or organizational aspects like the existence of protections or fire walls against hackers, complex operator identification systems (iris or fingerprint scanners…), system back up's, communication redundancies…

Once the security criteria are fulfilled, it is possible to calculate the basic operative costs. In one case, it could be generation cost while in the other it could be personnel or communication costs.

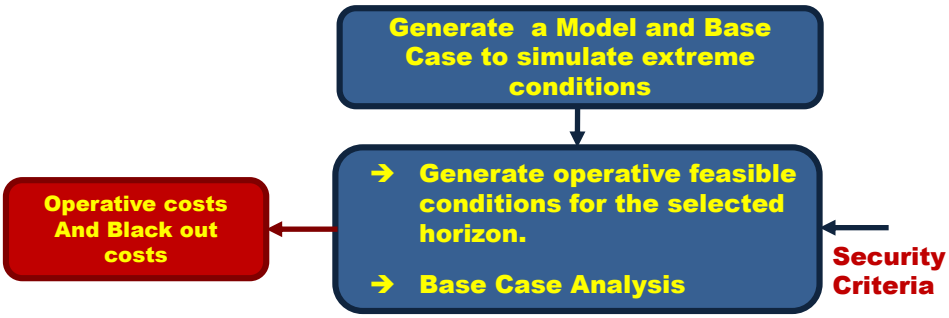
This cost (€/hour) will be considered as permanent in the system during the time of the study.

3.1.3 *Apply the emergency or attack scenario to the Base Case*

At the beginning of the scenario described above, the consequences of the malicious attacks (or of other extraordinary conditions) will be applied.

As a result of this scenario some services may be lost: final electricity users and/or control capacity.

With the simulation it is possible to obtain the impact of the extraordinary conditions into the system and the potential costs of the situation generated.



3.1.4 *Apply Standards and countermeasures to the Base Case*

Some of the countermeasures are infrastructure enhancements that require investments. They will be in place all the time or in the case they were programmed to be committed in the future, the financial cost to anticipate some investments has to be considered.

Some actions, resulting from standards application or countermeasures, could consist in a more intensive use of available generating infrastructures in order to have more reserves available or a more convenient

generation distribution in the territory. In this case the situation will probably increase the permanent operative cost. As a consequence, the new operative cost has to be considered.

Others countermeasures are emergency procedures to be applied in case of emergency, activating some resources which are not used in normal conditions. This situation will increase the operative costs, but only in the case of incident and not as a permanent cost.

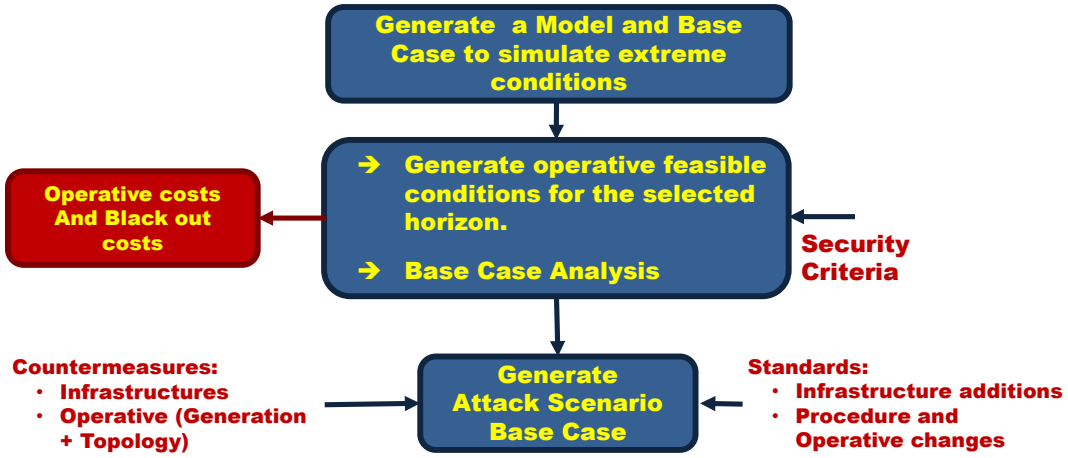
After including these standards and countermeasures, the system is ready to support the incidents.

3.1.5 *Apply the emergency or attack scenario to the Base Case*

Again, at the beginning of the scenario, the consequences of the malicious attacks (or of other extraordinary conditions) will be applied.

Here again, as a result of this scenario some services may be lost: final electricity users and/or control capacity. If the Standards and the countermeasures work as designed, the operative cost could be higher but the impact of the emergency conditions will be lower than in the previous case.

With this simulation we will obtain the impact of the extraordinary conditions into the system and the potential costs of the situation generated.



As a result of the simulation we will obtain the new operative costs and the cost for the system and their clients of the emergency situation generated.

3.1.6 *Evaluation of Standards and Countermeasures*

With the information provided in the different situations, it is possible to evaluate the response of the standards and countermeasures during and after incidents and the costs generated and avoided.

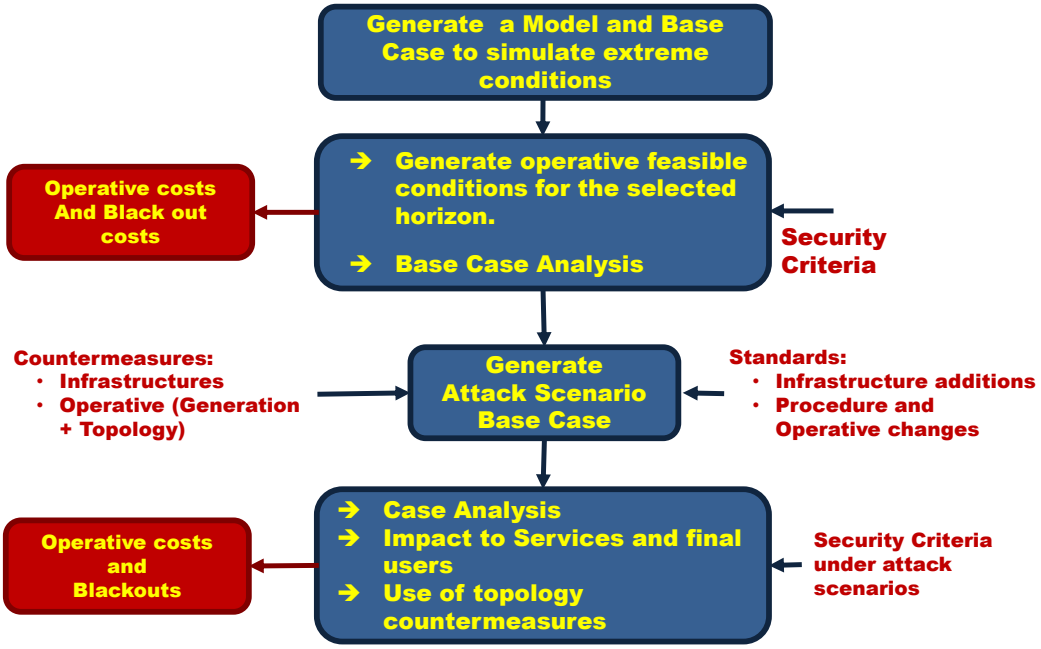
Some aspects will be considered in the evaluation:

i. In case of blackouts generators, energy carriers, distributors or operators may have some negative economic impacts. These losses are small and limited to the damages to the infrastructure, which can be limited for the utility considering insurances coverage but the full cost will be considered as country cost, no matter which is the final company affected.

ii. The operative costs are increased by the measures and this is a permanent cost, either if there is an emergency condition or not.

iii. The incident has a probability to take place not a certainty. So the benefits to provide countermeasures and standards will be collected only if the incident takes place.

iv. It is possible to study the impact of countermeasures for the incident used to design them but this standards and countermeasures will have also potential benefits for other incidents different the ones included in the design.



3.2 Procedure adapted to Physical Layer

The physical layer, as described above, is formed by those elements that are connected to high or low voltages to bring the electric energy from the power plants, or interconnections, to the final electricity user. As part of this physical system the auxiliary elements needed for a secure operation are also considered, especially the protections system.

The physical laws that describe the electric networks, and more particularly the Ohm and Kirchhoff laws, are simple and easy to formulate. This circumstance will allow generating a mathematical model of the network.

The problem generated by the very high number of equations to solve has been answered by different mathematical theories from an approach method like Gauss-Seidel and later improved by Newton-Raphson and its later additions, so nowadays some direct calculations are starting to be available.

In any case these models allow calculating voltages in all nodes and flows in all branches, in both sides, taking as inputs the physical characteristics of the electric system, the loads and generations.

This capacity to dispose of mathematical models of the network allow obtaining the results required and answering to *"what if"* questions.

3.2.1 *Initial scenario and Base Case Model*

The first step is to define the network model in relation to the base case which will represent the expected conditions of the network for the study horizon.

The main values to be included in the model are:

a. The network expansion or modifications planned for the horizon of the study. That is:
   - New substations
   - New Lines and Transformers
   - New Power plants

b. Estimate the most probable topology for normal system operation.

c. Forecast the load and its distribution among different types of loads in the system (the ones that follows the demand curve or not). Place the load in the appropriate nodes.

d. Balance the expected load and the most probable generation profiles, forecasted for the study horizon.

e. Verify the appropriate convergence of the model with the estimated data.

3.2.2 *Verify the security criteria and calculate operative costs*

The Grid Code or the Operation Procedures are the rules fixed by the regulator that specify the type and minimum quality of operation expected from the System Operator. In this set of rules, among others, there

are the security criteria that establish the network conditions after an incident for the surviving of the system will any time.

The most common criterion is the loss of a single element associated with its probability in case of incident, also known as "n-1" criteria or "list of contingencies", which corresponds to a list of incidents that the system must survive.

In this point we need to guarantee that this criteria is fulfilled.

To do so, the "Contingency Analysis" program can be used. This process consists in the simulation of all contingencies included in the list and verifies that after the incident, the system is satisfying the conditions established in the Grid Code (voltages and flows after the incident).

If the system fails to survive to one or more of these contingencies, the Base Case will be modified in order to meet the criteria. Acceptable modifications are:

a. Modify Voltage profile using Voltage control elements: Reactive generation in power plants, shunts devices…
b. Topology changes
c. Active power relocation…

If the system survives to all contingencies, the Base Case is accepted and considered as the starting point.

Once the system fulfils the normal security criteria, the generation costs for the system, considering the power plants in service, will be considered the Operative Cost for the Base Case.

The output of the simulation program (Load Flow) will specify the operating point of each one of the Power Plants Units required. This information is very useful to calculate the operative costs.

In this case some regulations are based in generation costs and other in generation prices have to be considered. To select one or the other will be based in the regulation and represent the real cost of the generation for the system and paid by clients, Distribution Companies or Commercial entities.

This value will be saved and used later for evaluation.

3.2.3 *Apply the emergency or attack scenario to the Base Case*

At the beginning of the stable and tested Base Case we will apply the Emergency or Attack Scenario.

This scenario formulated in general terms (shut down Substations A and B) must be translated to a Load Flow language. (Shut down of lines AB1, AB2, AC1… and Transformers A1, A2… and units B1, B2…). This will generate a new case ready to be simulated in the Load Flow.

As the protections system is not modelled, it must be simulated outside the system. In consequence, we will verify that:

i. Lines with overload (Calculated > Maximum acceptable after incident) will be assumed that overcurrent protection, reverse time, will work and will be also removed from the case.
ii. Transformers overload, same treatment that in the previous case.

iii. Under and over voltages. If there are automatic control means, we must correct the manually voltage, otherwise, these elements will be removed from the case.

iv. Verify the swing bus values. If exceed significantly, the capacity of the real groups connected that power plants in secondary regulation will be set at their value, controlling the excess of generation in the swing bus.[3]

Once the above conditions are fulfilled, the simulation of the special network conditions will indicate how much clients are not attended in their demand of electric power.

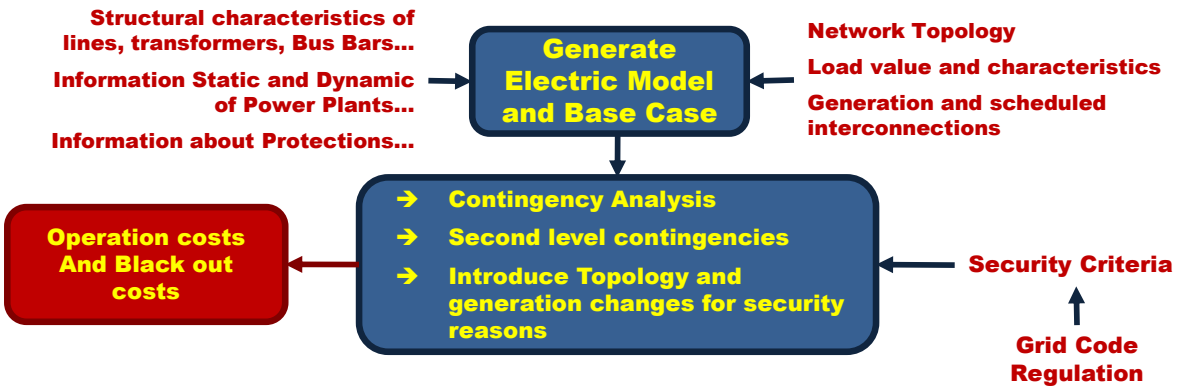
The data about the incident will consider the unavailability time of each element removed from the system during the test. The elements removed as overloaded or by low/high voltage, will be considered as removed to protect them and are considered disconnected but available for restoration.

We will consider that the elements can be restored when available and included in the restoration.

This will generate restoration cases with a certain frequency (every 15 minutes?) and each case will give a new value of unattended demand. It will be taken into account that the load, attended and unattended, will vary with the time so in each case the load will be readjusted.

Between two consecutive cases, it is normal to consider that the previous conditions are maintained and in consequence the power lost will be maintained at least until de next calculation, giving the energy lost during the period.

The economic evaluation of the energy lost during the incident, from start until 95% of the load is recovered, as impact to the utilities, generators and final energy users, will be considered as the cost of the incident.



[3] Please note that the swing bus must be located in such place not to distortion the flows before and after the incident and if it is possible, simulating the reaction of the interconnected systems. In this case the swing bus contribution will simulate the interconnected systems contribution to balance the load – generation system after the incident.

3.2.4 *Apply Standards and countermeasures to the Base Case*

As said above there are different types of countermeasures or standards and there are three circumstances in which they are applied:

i. The one that assumes the reinforcement of the electric infrastructure (new substation, new lines…) must be included in the new model. These infrastructures are assumed to be in service permanently and operate as any other one. Their cost (full investment or financial costs for advancing the commitment) will be considered as permanent in the system.

ii. The one that takes into account a new operating point, will be considered also as permanent and always applied (more primary and secondary reserves, more short circuit power, exporting instead of importing…). These special operating conditions normally will be applied only in the case that the threat or meteorological conditions suggest an increase of the probability of the incident. The cost will be considered only during this period.

iii. The ones to be applied in case of incident, normally oriented to have a faster restoration, the implementation cost will be considered permanent and the operative cost only during the incident.

Once the countermeasures have been installed in the system, we need to verify that they fulfil the security criteria under normal conditions, as indicated in point *"3.2.2. "Verify the security criteria and calculate operative costs."*, including the final calculation of the operative costs.

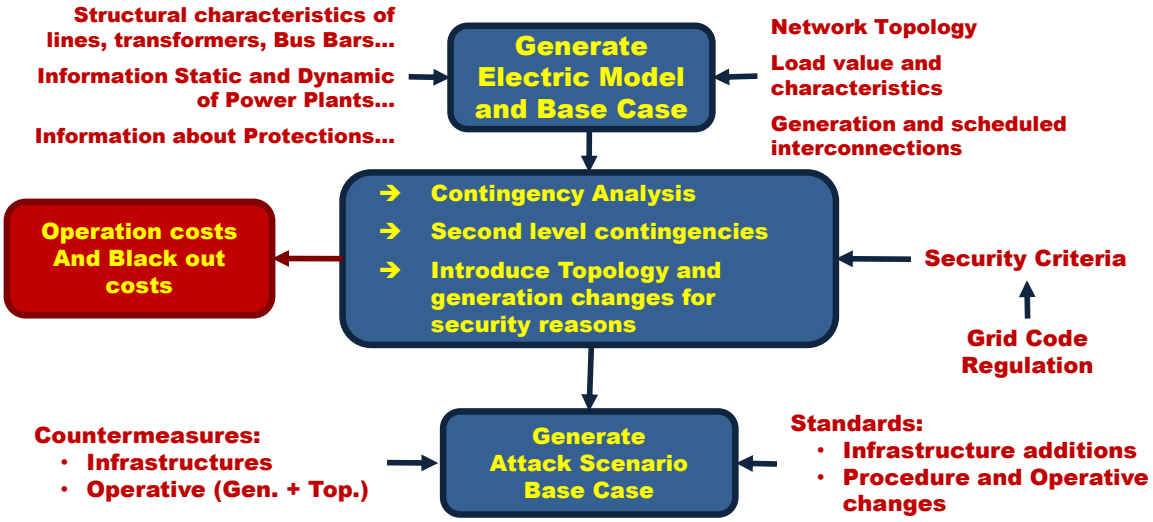
3.2.5 *Apply the emergency or attack scenario to the Base Case*

In this step the operations indicated in step "3.2.3. Apply the emergency or attack scenario to the Base Case"

The final result will evaluate the impact of the incident into the network equipped with standards and countermeasures. The impact, if the countermeasures and standards are adequately designed, will be lower than in the Base Case.

The difference will be the positive impact of the actions taken to reduce the incident impact.

When calculating the impact of the countermeasures, we have to care about that there is no certainty that the emergency conditions or the malicious attack will take place. They are only preventive measures.



3.2.6 *Evaluation of Standards and Countermeasures*

The output of the different simulations performed during the analysis reports the following information that could be used in the evaluation process:

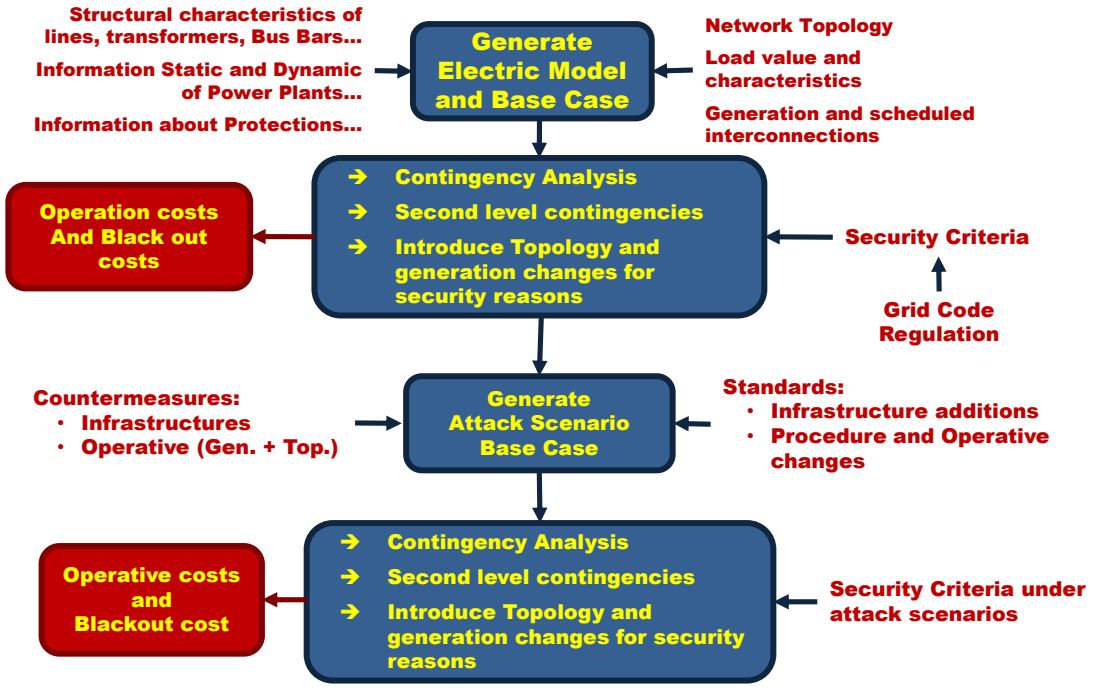
i. Operative cost in the Base Case.

ii. Operative cost when the countermeasures and standards are applied.

iii. Impact on the clients in the case of an incident without the countermeasures and standards.

iv. Impact on the clients in the case of an incident with the countermeasures and standards in service.

v. Investment cost of infrastructure countermeasures and operative costs of operational countermeasures and standards will be facilitated externally to the simulations, as input.



3.3 Procedure Adapted to Cyber Layer

The Cyber layer, as described below, is formed by the IT systems oriented to control de electric system and their components. Some of these systems are oriented to control the substation as local operation capacity while other, as Control Centres, are oriented to a remote control of the system.

Power Plants of any kind have their own local or remote control system becoming a separate level in the control hierarchy.

In the last years there has been an increasing interest in the security of process control and SCADA systems. Furthermore, recent computer attacks, such as the Stuxnet worm, have shown there are parties with the motivation and resources to effectively attack control systems.

Previous work has proposed new security mechanisms for control systems, but few of them have explored new and fundamentally different research problems for securing control systems when compared to securing traditional information technology (IT) systems. In particular, the sophistication of new malware attacking control systems – malware including zero-days attacks, rootkits created for control systems, and software signed by trusted certificate authorities – has shown that it is very difficult to prevent and detect these attacks based solely on IT system.

Most of the efforts for protecting control systems (and in particular SCADA) have focused on safety and reliability (the protection of the system against random and/or independent faults). Traditionally, control systems have not dealt with intentional actions or systematic failures. There is, however, an urgent and growing concern for the protection of control systems against malicious cyber-attacks.

In the case of physical systems, the models can be based on mathematical approaches and their results. In the case of Cyber systems, there is not a mathematical model to represent it and propose scenarios to be solved. The models must be more conceptual than mathematical ones and the results will be also based on conceptual analysis.

Incidents in the Cyber Layer may have two consequences on the electric system:

a. Incident is contained to the Cyber layer, modifying or deleting data bases or even causing damage to the hardware. In this case the model will be conceptual and the impact of incidences will be evaluated in the same way.
b. Incidents impact into the physical layer. In this case there will be a need to use the physical model to understand the real impact of the incidents.

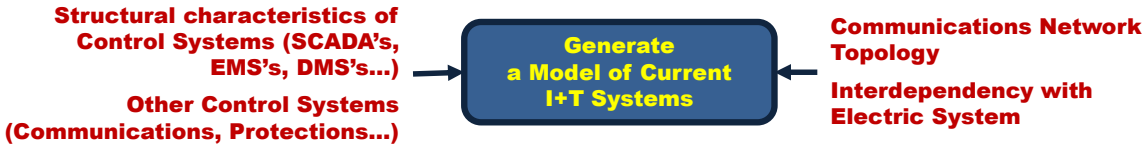
3.3.1 *Initial scenario and Base Case Model*

The IT system model will be adapted to the needs of the analysis to be performed. In general it could be based on two aspects:

a. Hardware based in order to understand potential damage to the equipment, with or without backup systems.
b. Conceptual based on the functionality and capabilities of the system in order to simulate actions of cyber-attacks as worms and others.

The model will have the extension suitable to the incident under study: Substation System, Power Plant control systems, Control Centres…

Communications are basics to understand the capacity of the system and the vulnerabilities. As a consequence the communications will be part of the model.

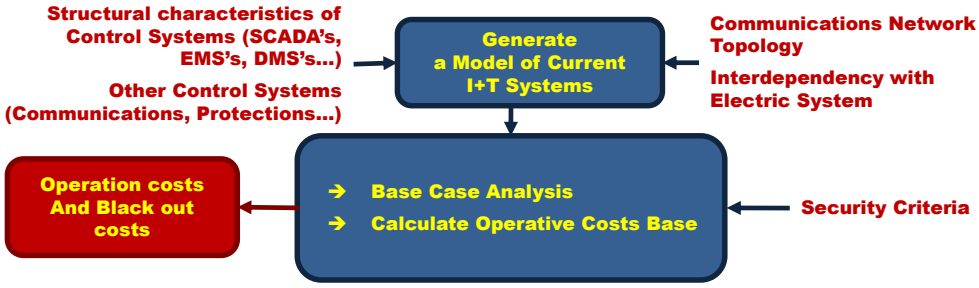


3.3.2 *Verify the security criteria and calculate operative costs*

Some security criteria for Critical Infrastructures Control Centres could be established by regulators or administrative authorities. In this case the fulfilment of these rules will be verified as a first activity.

If the system does not fulfil these criteria, these criteria will be implemented and the potential cost ignored in the study.

An evaluation of operative costs will be estimated.

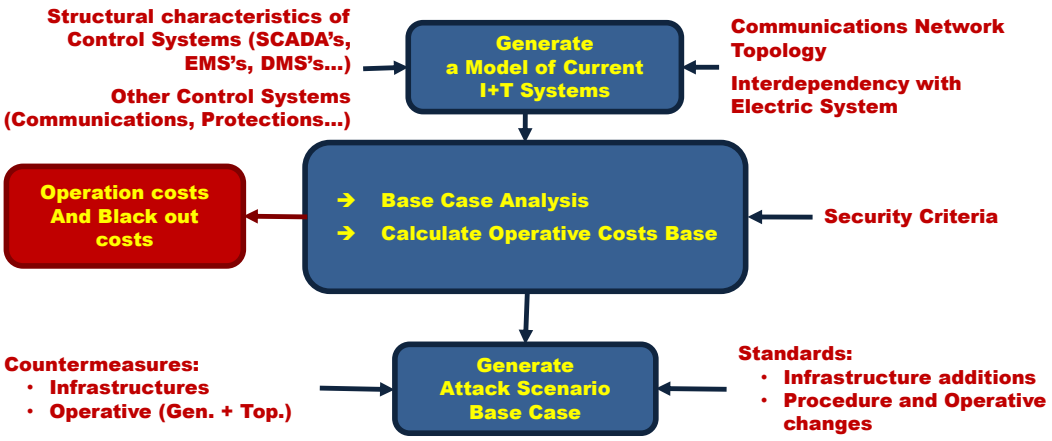


3.3.3 *Apply the emergency or attack scenario to the Base Case*

On the basis of this model, the attack scenario will be executed.

Two analysis will be done as a result of this scenario:

a. Verify the damages caused into the Cyber network and evaluate the impact.
b. Verify if the incident will cause impact into the physical layer (open breakers, modify protections set points…). In this case the physical model procedures will be used to calculate the impact on final users.



3.3.4 *Apply Standards and countermeasures to the Base Case*

As said above there are different types of countermeasures or standards and there are three circumstances in which they are applied:

i. The one that assumes the reinforcement of the electric infrastructure (new substation, new lines…) must be included in the new model. These infrastructures are assumed to be in service permanently and operate as any other one. Their cost (full investment or financial costs for advancing the commitment) will be considered as permanent in the system.

ii. The one that takes into account a new operating point, will be considered also as permanent and always applied (more primary and secondary reserves, more short circuit power, exporting instead of importing…). These special operating conditions normally will be applied only in the case that the threat or meteorological conditions suggest an increase of the probability of the incident. The cost will be considered only during this period.

The ones to be applied in case of incident, normally oriented to have a faster restoration, the implementation cost will be considered permanent and the operative cost only during the incident. Once the countermeasures have been installed in the system, we need to verify that they fulfil the security criteria under normal conditions, as indicated in point "3.2.2. "Verify the security criteria and calculate operative costs", including the final calculation of the operative costs.

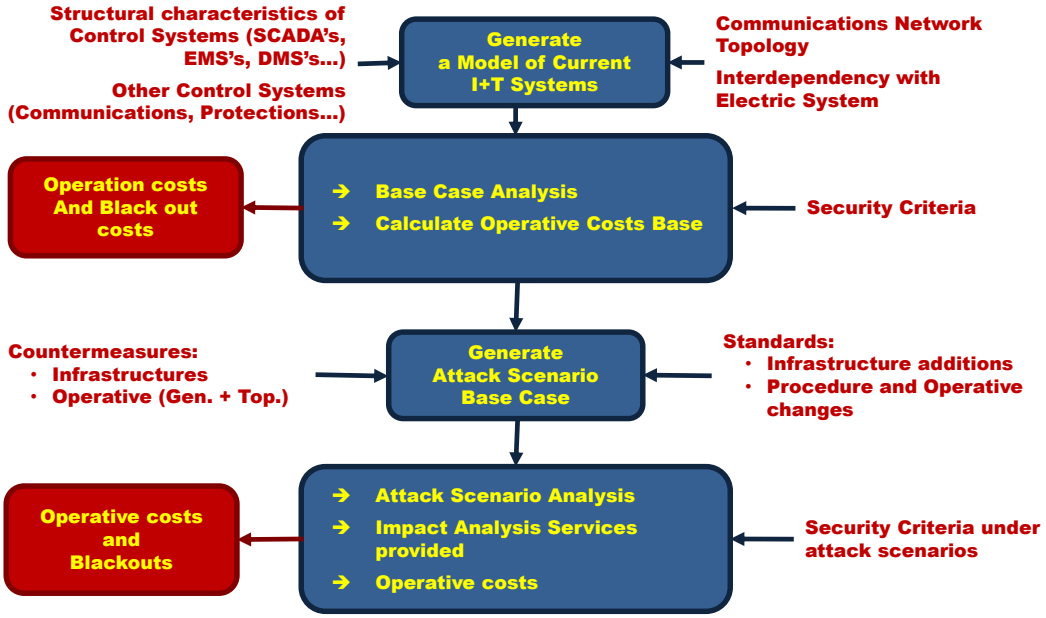
3.3.5 *Apply the emergency or attack scenario to the Base Case*

The attack scenario will be executed with the model now including the countermeasures and standards,.

Two analysis will be done as a result of this scenario:

a. Verify the damages caused into the Cyber network and evaluate their impact.

b. Verify if the incident will cause impact into the physical layer (open breakers, modify protections set points…). In this case the physical model procedures will be used to calculate the impact to final users.



3.3.6 *Evaluation of Standards and Countermeasures*

The output of the different simulations performed during the analysis reports the following information that could be used in the evaluation process:

i. Operative cost in the base case.

i. Operative cost when the countermeasures and standards are applied.

ii. Impact on the cyber and physical layers in case of an incident without the countermeasures and standards.

iii. Impact on the cyber and physical layers in case of an incident with the countermeasures and standards in service.

iv. Investment cost of countermeasures and operative costs of operational countermeasures and standards will be facilitated externally to the simulations, as input.

4. COUNTERMEASURES AND STANDARDS TO IMPROVE CYBER ATTACKS

4.1 Standards

As it is argued comprehensively in report D1[4], so far the most relevant and mature standards concerning cyber security of power system controls appear to be:

a. The two NIST standards providing guidance for establishing secure industrial control systems (ICS):
   - the NIST SP 800-82 guidelines for establishing how to secure Industrial Control Systems, including SCADA, DCS and other control system components such as Programmable Logic Controllers (PLC).
   - the NIST SP 800-53 especially emphasizing security controls concerning software development and change management.

b. the ISA/IEC-62443, formerly ISA 99. This is a set of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems. These standards concern general issues, such as foundational information including concepts, models and terminology, and specific requirements concerning Policies and Procedures and technical Systems and Components.

c. the NERC cyber security standards and guidelines CIP-002 through 009 related with the North American bulk (i.e. transport) electric system. These include:
   - provisions for identifying critical cyber assets;
   - developing security management controls;
   - training;
   - perimeter and physical security;
   - incident reporting and response planning, and recovery plans.

All those standards recommend similar guidelines concerning cyber security of ICSs. In particular, the latter provide a comprehensive scheme concerning cyber security of bulk power system controls including:

- Hardening, that is the process of checking and securing a system, through the adoption of specific techniques to reduce the system surface exposed to attacks;
- Malicious software prevention dealing with attacks made by malicious code;
- Configuration Management, i.e. the process to monitor, track, review and more generally manage all system information, including all hardware and software;

[4] Ugo Finardi, Elena Ragazzi and Alberto Stefanini, *Considerations on the implementation of SCADA standards on critical infrastructures of power grids*, CNR-Ceris, Rapporto Tecnico Anno 8, N° 47, Novembre 2013.

- Cryptographic and key management techniques to ensure confidentiality, authentication and integrity of information being exchanged over an untrustworthy network;
- Backup and Recovery provisions to ensure protection against operation disruptions caused by either accidental events or intentional actions through the implementation of sound routinely back-up procedures and testing;
- Network security provisions concerning network segregation and layered protection in relation to the defence-in-depth principle;
- System acquisition, development and maintenance provisions dealing with secure contracting and procurement of control systems components and associated services;
- Personnel security controls dealing with roles and responsibilities during all phases of people's employment, from initial applicants' screening to leave. These ensure that employees, contractors, visitors, third parties etc., understand their responsibilities so as to reduce the risk of theft, fraud and misuse of critical facilities;
- Training and awareness as a key component of a sound Security Plan to constantly refresh personnel conducting critical infrastructure-related job about their duties, responsibilities and expected behaviour to prevent any vulnerability from being exploited by an adversary;
- Physical and environmental security addresses protection of process control assets from physical and environmental hazards as well as damage, misuse and theft;
- Business Continuity Management procedures to restore business operations after either a minor or a major disruption;
- Incident Management which include procedures and activities to let the organization respond in a timely and effective manner to either intentional or accidental events which may result harmful for the normal and secure operation of the control system facilities;
- Compliance and Improvement provisions about improvement of the organisation's security plan for any possible enhancement which may be learnt during the security design and implementation;
- An Access Control procedure to ensure that only appropriate entities have valid accounts and proper access privileges to physical premises, control networks and systems.

4.2 Countermeasures

Countermeasures are defined as actions taken to offset some actions.

In the electric system, countermeasures are actions and changes introduced in the system to limit the extension or deepness of a malicious attack or extreme natural conditions.

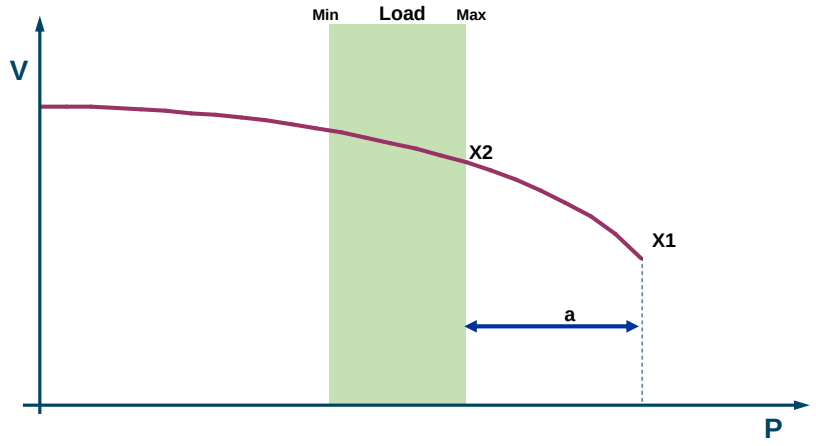
Countermeasures can be:

a. Preventive: those one that are placed before the incident and will be in service permanently. Two types can be considered:
   - Infrastructure: Expansion or reinforcement of the electric infrastructure. Once committed, it will be kept in service.
   - Operative Procedures: More severe security criteria and more operative margins. Do not require the measures to be permanently in service, only when the threat is higher.

b. Corrective: Procedures and actions to be placed after the incident in order to speed up the restoration process, which will reduce the duration of the incident.

4.2.1 *Effects of Countermeasures into System Performance.*

The transmission limits of any electric system, can be represented in the VP (Voltage Power Curve). The limit of the curve, represented by point X1 in the graphic, represents the maximum capacity and the voltage collapse point.

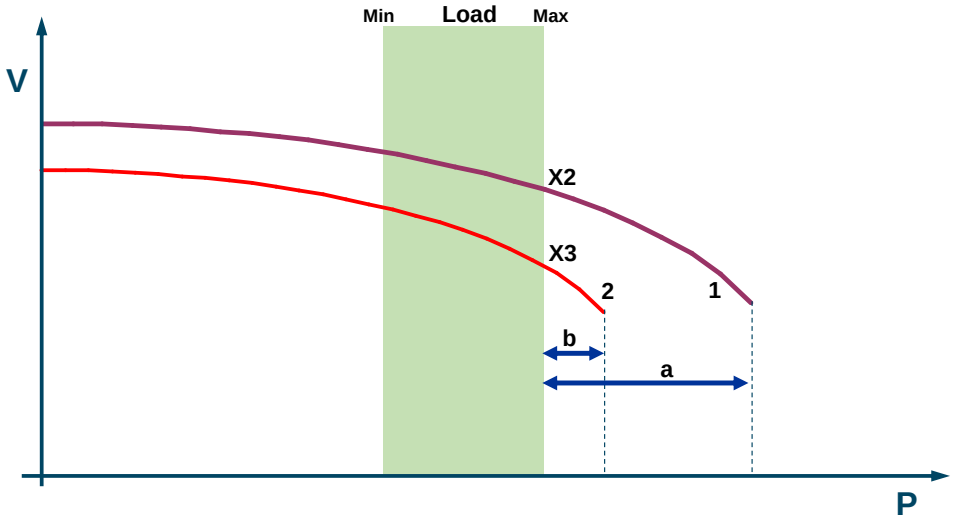


The shadowed zone represents the operating area under normal conditions, when during a day (or any other period) the load fluctuates between a minimum and a maximum. In this last case, the operating point is X2.

This situation leaves an operative margin indicated by arrow "a".

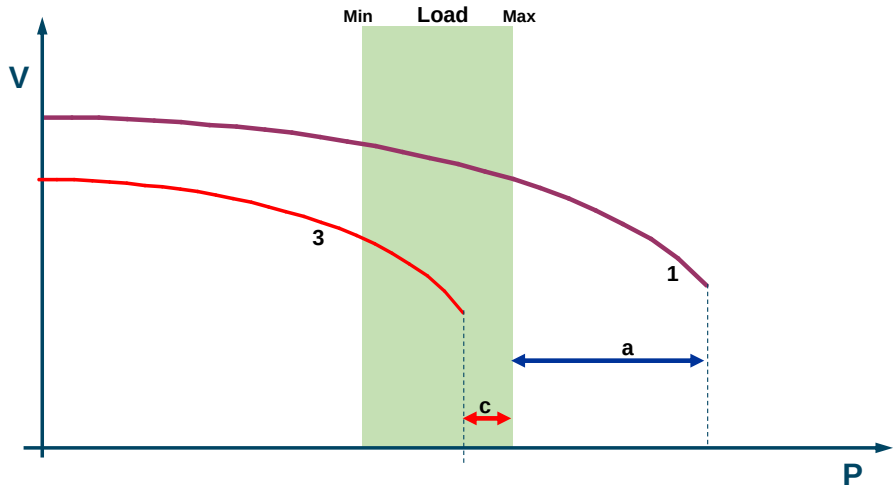
Under this conditions if a contingency (incident included in the security criteria[5]) takes place the system is supposed to survive to the incident maintaining the service to all the clients. The security criteria are included in the Grid Code or Operating Procedures and it's normally a responsibility of the TSO to guarantee the system survivability after those incidents.

[5] The list of contingencies is formed by those elements that has a certain probability or higher to take place. Normally consists in the loose of one line, or one generator or one transformer. incidents with a lower probability are excluded: loose a Busbar or two simultaneous elements.

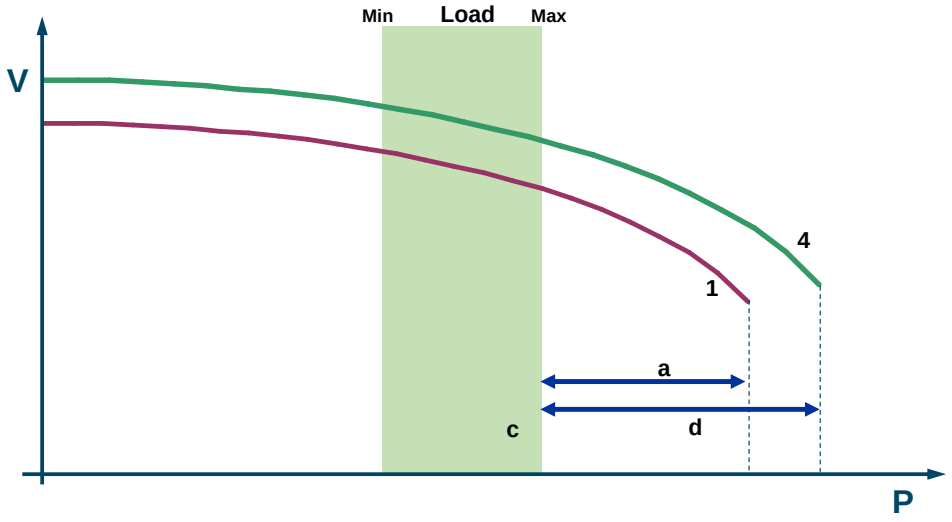


In the VP Curve this new network conditions are reflected by a new curve, in our case curve 2 and the operating point moves from X2 to X3. The system survives but the operating margin is now b instead the former a.

In the case of a second contingency or a simple incident not included in the list, the system may or not survive. In this last case, the operating point is now below the maximum expected load which will take the system to voltage collapse, if extra measures are not taken like a load shedding of a magnitude c or more.

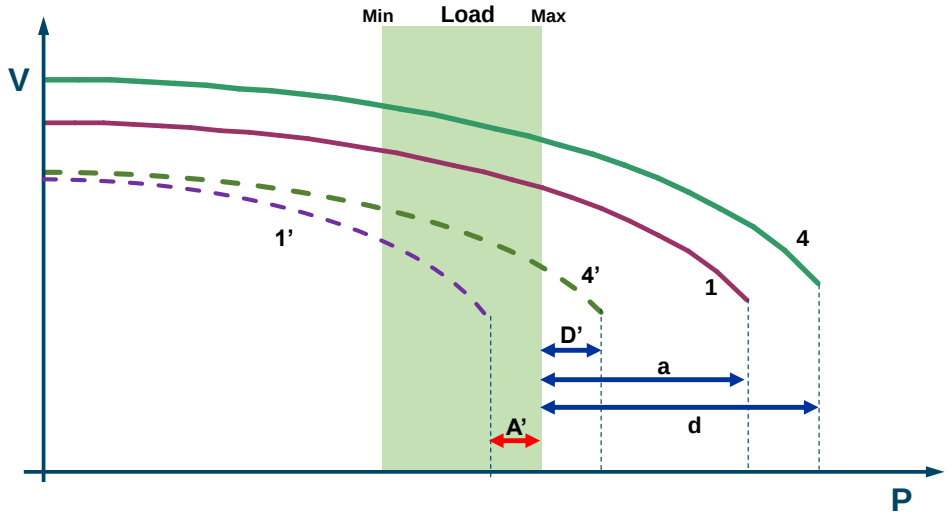


To provide the system with more security and survivability, some countermeasures will be taken. Those countermeasures will move the VP curve to a more secure region.



In this case Curve 4 represents the system with some countermeasures applied. The system is now prepared to survive to some incidents which was not able to do it before.

As a way of example, if now we apply the same incident, more severe that the ones expressed as contingencies, the results could be as follows:



After the incident Curve 4 moves to Curve 4', surviving to the incident nut former curve 1 moves to Curve 1', producing a blackout.

A countermeasure can be designed to support certain types of incidents or being more generic.

At the same time it could be composed by infrastructure expansion or by operation protocols.

4.2.2 *Cyber System*

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
Security policy and procedures										
1	Security policy and procedures	No		x		x				
Organizational security										
2	Management policy and procedures	No		x		x				
3	Management accountability	No		x		x				
4	Baseline practices	No		x		x				
5	Coordination of threat mitigation	No		x		x				x
7	Termination of third parties access	No		x		x	x	x		
Personnel security										
8	Personnel security policy and procedures	No		x		x		x		

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
9	Position categorization	No		x		x		x		
10	Personnel screening	No		x		x		x		
11	Personnel termination	No		x		x		x		
12	Personnel transfer	No		x		x		x		
14	Third-party personnel security	No		x		x	x	x		
Physical and environmental security										
20	Monitoring physical access	No		x		x		x	x	
22	Visitor records	No		x		x		x	x	
23	Physical access log retention	No		x		x			x	
31	Alternate work site	No				x		x		x
32	Portable media	No		x		x	x	x		
33	Personnel and asset tracking	No		x		x			x	
35	Information leakage	No		x		x			x	

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
37	Physical device access control	No		x		x		x		
System and services acquisition										
40	Life-cycle support	No		x		x				
43	Software licence usage restrictions	Yes		x		x	x	x		
46	Outsourced control system services	No		x		x	x			
47	Developer configuration management	No		x		x				
48	Developer security training	No		x		x				
49	Supply chain protection	No		x		x				x
50	Trustworthiness	No				x				
51	Critical information systems components	No		x		x				
Configuration management										

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
52	Configuration management policy and management	No		x		x				
53	Baseline configuration	No		x		x				
54	Configuration change control	No		x		x	x	x		
55	Monitoring configuration changes	No		x		x			x	
56	Access restriction for configuration change	No		x		x	x	x		
60	Addition removal and disposal of equipment	No		x					x	
61	Factory default authentication management	No		x		x	x	x		
Strategic planning										
65	Interruption identification and classification	No		x		x				x

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
68	Testing	No		x		x				x
69	Investigating and analysis	No		x		x				x
70	Corrective action	No		x		x				x
71	Risk mitigation	No		x		x				x
72	System security plan update	No		x		x				x
73	Rules of behaviour	No		x		x		x		x
74	Security related activity planning	No		x		x				
System and communication protection										
75	System and communication protection policy and procedures	No		x		x				
77	Security function isolation	No		x		x	x	x		

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
78	Information in shared resources	No		x		x			x	
79	Denial of service protection	No		x	x	x	x	x		
81	Boundary protection	No		x		x	x		x	
82	Communication integrity	No		x	x	x	x			
83	Communication confidentiality	No		x	x	x			x	
84	Trusted path	No		x		x			x	
85	Cryptographic key establishment and management	No		x	x	x				
86	Use of validated cryptography	No		x	x	x				
87	Collaborative computing devices	No				x			x	
88	Transmission of security	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
89	Public key infrastructure certificates	No		x		x				
90	Mobile code	No		x		x	x			
91	Voice over Internet protocol	No				x				
93	Security roles	No		x		x		x		
94	Session authenticity	No		x	x	x	x			
100	Honeypots	No				x			x	
101	Operating system independent applications	No				x				
102	Confidentiality of information at rest	No		x		x			x	
104	Virtualisation techniques	No				x				
105	Covert channel analysis	No				x			x	
107	Transmission preparation integrity	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
108	Non-modifiable executable programs	No		x		x	x	x		
Information and document management										
112	Information classification	Yes	Energy Low	x		x			x	
115	Information and document retrieval	No		x		x				
116	Information and document destruction	No		x		x			x	
117	Information and document management review	No		x		x				
118	Media marking	No				x		x	x	
119	Security attributes	No				x				
System development and maintenance										

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
120	System maintenance policy and procedures	No		x		x				
121	Legacy system upgrade	No		x		x	x	x		
122	System monitoring and evaluation	No		x		x			x	
123	Backup and recovery	No		x		x				x
125	Periodic system maintenance	No		x		x		x	x	
126	Maintenance tools	No		x		x			x	
Security awareness and training										
130	Security awareness and training policy and procedures	No		x		x				
131	Security awareness	No		x		x		x		
132	Security training	No		x		x		x		
133	Security training records	No		x		x				
135	Security responsibility testing	No		x						x

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
Incident response										
136	Incident response policy and procedures	No		x		x				x
139	Incident response training	No		x		x				x
140	Continuity of operations plan testing	No		x		x				
141	Continuity of operations plan update	No		x		x				
142	Incident handling	No		x		x				x
143	Incident monitoring	No		x		x			x	
144	Incident reporting	No		x		x			x	x
145	Incident response assistance	No		x		x				x
147	Corrective action	No		x		x				x
148	Alternate storage site	No		x		x				x
150	Alternate control center	No		x		x				x
151	Control system backup	No		x		x				x

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
152	Control system recovery and reconstitution	No		x		x				x
Media protection										
154	Media protection policy and procedures	No		x		x		x	x	
155	Media access	No		x		x		x	x	
156	Media classification	No		x		x		x	x	
157	Media marking	No				x		x	x	
159	Media transport	No		x		x		x	x	
160	Media sanitization and disposal	No		x		x		x	x	
System and information integrity										
161	System and information integrity policies and procedures	No		x		x	x			
162	Flaw remediation	No		x		x	x	x		
163	Malicious code protection	No		x		x	x	x		

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
164	System monitoring tools and techniques	No		x		x			x	
165	Security alerts and advisories and directives	No		x		x			x	
166	Security functionality verification	No		x		x			x	
167	Software and information integrity	No		x		x			x	
169	Information input restrictions	No		x		x	x	x		
170	Information input validation	No		x		x	x	x		
172	Information output handling and retention	No		x		x			x	
173	Predictable failure prevention	No				x				x
Access control										

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
174	Access control policy and procedures	No		x		x	x	x	x	
175	Identification and authentication policy and procedures	No		x		x	x	x		
176	Account management	No		x		x	x	x		
177	Identifier management	No		x		x	x	x		
178	Authenticator management	No		x		x	x			0
179	Account review	No		x		x			x	
180	Access enforcement	No		x		x	x	x		
181	Separation of duties	No		x		x	x	x		
182	Least privilege	No		x		x	x	x		
185	Device identification and authentication	No		x		x		x		
186	Authenticator feedback	No		x		x			x	
187	Cryptographic module Authentication	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
188	Information flow enforcement	No		x		x			x	
189	Passwords	No		x		x	x	x		
190	System use notification	No		x		x			x	
192	Previous logon (access) notification	No		x		x			x	
193	Unsuccessful login attempts	No		x		x			x	
194	Session lock	No		x		x			x	
198	Access control for mobile devices	No		x		x	x			
203	User-based collaboration and information sharing	No				x			x	
Audit and accountability										
205	Audit and accountability policy and procedures	No		x		x			x	
206	Auditable events	No		x		x			x	

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
207	Content of audit records	No		x		x			x	
208	Audit storage capacity	No		x		x			x	
209	Response to audit processing failures	No		x		x			x	
210	Audit monitoring, analysis and reporting	No		x		x			x	
211	Audit reduction and report generation	No		x		x			x	
213	Protection of audit information	No		x		x			x	
214	Audit record retention	No		x		x			x	
215	Conduct and frequency of audits	No		x		x			x	
218	Security policy compliance	No		x		x			x	
219	Audit generation	No				x				
220	Monitoring for information disclosure	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
Monitoring and retrieving of control system security policy										
222	Monitoring and retrieving control system security management policy and procedures	No		x		x				
223	Continuous improvement	No		x		x				
224	Monitoring of security policy	No		x		x				
225	Best practices	No		x		x				
226	Security accreditation	No		x		x	x	x		
227	Security certification	No		x		x	x	x		
Risk management and assessment										
228	Risk assessment policy and procedures	No		x		x				
229	Risk management plan	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
230	Certification, accreditation and security assessment policies and procedures	No		x		x				
231	Security assessments	No		x		x			x	
233	Plan of action and milestones	No		x		x				
234	Continuous monitoring	No		x		x			x	
236	Risk assessment	No		x		x				
237	Risk assessment update	No		x		x				
238	Vulnerability assessment and awareness	No		x		x	x	x		
239	Identify, classify, Prioritise and analyse potential security risks	No		x		x				
Security program management										
240	Information security program plan	No		x		x				

.	Type of protection	Current state regulations and standards for the ICS systems		Standard describing security			Control over device / system or distortion of his work		Whether lack of security allows free exploration and deepening of attack?	Whether lack of security increases the unavailability of the system?
		Requirement of application security	Source due	ISO 27001/ISO 27002	IEC 62351	NIST 800-53	Whether lack of security can be used in remote attack?	Whether lack of security can be used in local attack?		
241	Senior information security officer	No		x		x				
244	Information system inventory	No		x		x				
245	Information system security measures of performance	No		x		x				
248	Risk management strategy	No		x		x				
249	Security authorization process	No		x		x				
250	Mission/business process definition	No		x		x				

5. PROCEDURE FOR THE ITALIAN CASE STUDY

The Italian case study will analyse a hypothetical informatics attack to a power generation plant built according the design methodologies applied till few years ago.

5.1 The Industrial Control System

The structure of Industrial Control System (ICS) Network in a Generation Power is composed by two subsections:

a. the Client/Server Network that connects all HMI Client Stations of the SCADA and all auxiliary servers from the common services.

b. the Control Network which connects controllers, OPC Servers (Front End Servers) and Engineering Work Stations.

A redundant server (on which the SCADA software is installed) works as gateway to interconnect Client/Server and Control networks and may also work as HMI Client Stations. Front End Servers on control network communicate with the devices on field using, in general, proprietary protocols and make the collected data available, in general, on OPC standard protocol.

5.2 Vulnerability analysis and attack scenarios

Industrial processes controlled and monitored through Supervisory Control And Data Acquisition (SCADA) computer systems are affected by vulnerabilities that can be exploited.

With reference to Deliverable 2 “Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria”, an analysis of vulnerabilities will be performed in order to define the most suitable scenarios taking into account parameters such as probability, impact on the production process, and so on.

For example, the following scenarios could be taken in consideration:

a. Attack performed infecting the computers of a control system with a generic malware able eventually to replicate itself on the network;

b. Attack performed in order to saturate the network traffic and affecting the entire functionality of the control system. This would cause the loss of control of the process itself.

5.3 Evaluation of the impact on the Electric Grid

To evaluate the consequences of this event on the electric grid (or better on the electric system), it can be assumed that the attack takes place in a particular bad situation, both as spatial and temporal location. A hacker could be waiting for the proper moment to attack by monitoring some grid conditions.

In order to identify the proper case study, we must consider that European TSOs act all together in order to limit the damage caused by a single event (N-1 grid security criterion).

It could also be assumed that the procedure of load rejection fails. This will delay the restart of that power plant causing delays on the return to normality.

In order to evaluate the socio-economic impact of the blackout, it is necessary to define the daily load profile for all the users in the selected region in the unperturbed case and in the case of blackout.

It should be first set the day on which the attack occurs. Once set the day and the hourly load profile, it must be established the load profile for each major category of users: agriculture, industry, commercial (services/tertiary), residential. In order to obtain an accurate assessment of the effects of a power failure for a given period, will also be evaluated consumption for different subcategories of industry and commercial/services.

Daily load profile without attack will be extrapolated, if necessary, by means of realistic assumptions.

5.4 Evaluation of the socio-economic impact

Blackout cost evaluation is a complex issue. The main difficulty relies on the fact that it is not possible to have market prices to estimate the economic value of electric supply continuity. Nevertheless, in the economic literature several methods have been developed to infer the cost of electricity interruption not mutually exclusive.

A careful evaluation of the pros and cons of the available methods is necessary. The strategy will be chosen in order to have best fitting in our hypothetical blackout scenarios involving all the users' types.

5.5 Standard analysis and countermeasures definition

Adoption of standards and identification of countermeasures to be compliant with them is the first step to prevent cyber-attacks.

Impact of an attack may be more serious and may involve financial losses and loss of public confidence, damage to equipment and environment, and endangerment of public and employee safety.

Standards describe uniform engineering or technical criteria, methods, processes, and practices and may actually be a regulatory requirement.

The confusing proliferation of standards and guidance for electric power system cyber security makes difficult to quickly determine what is required by them.

For this reason the state-of-the-art of security practices will be analysed and the countermeasures developed and achieved by leading international bodies and institutions which have been focused and engaged on such a subject first and more heavily, with reference to Deliverable 1 "Considerations on the implementation of SCADA standards on critical infrastructures of power grids".

The most significant standards according the considered use case will be evaluated, with particular reference to the following ones:

a. NIST provides guidance for establishing secure industrial control systems (ICS). Particularly, it releases guidelines for establishing how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).
b. ISA/IEC-62443, formerly ISA 99, is a set of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).
c. NERC (North American Electric Reliability Corporation) mainly works on cyber security standard and guidelines related with secure bulk electric system. Particularly, the so-called NERC-CIP standard approach, deals with the implementation of the necessary security practices to meet the compliance requirements.

In the considered Use Case, countermeasures against risks will be analysed according to the above mentioned standards and use case plant parameters. They will ensure that the plants can sustain the attack and maintain the operation continuity. This includes all ICT components, which directly deals with energy conversion process monitoring and control such as SCADA systems. The security of this system is of paramount importance since attacks may directly influence the security of supply.

5.6 Evaluation of the costs of countermeasures

When the countermeasures are established, it will be possible to estimate the total effort of security countermeasures implementation in terms of monetary costs.

The evaluation will be related to a large company engaged in generation, distribution, and selling electricity in more countries. The cost will take into account both organizational and technical aspects. Both the capital costs (capex), related to a first implementation of security policies, assets and technology, and annual operational costs (opex), related to operation and maintenance will be considered.

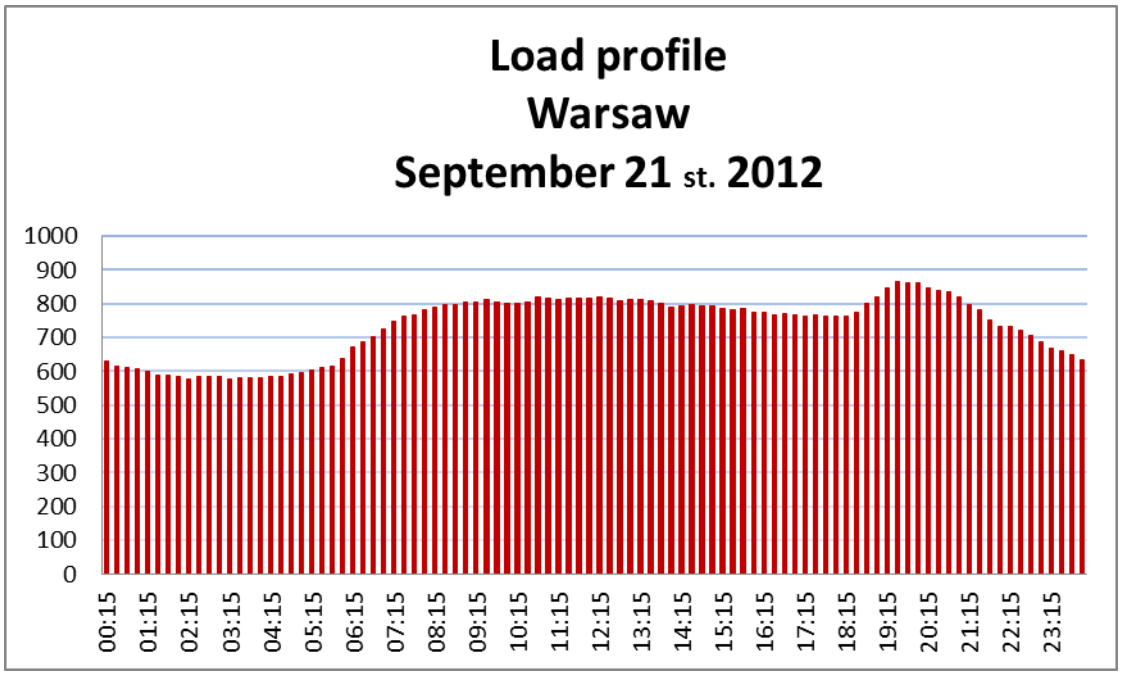
In order to have useful figures to extrapolate the cost of security implementation at European level, two basic situation will be considered: the first one is for a company with substantially no security policy implemented; the second one is for a company with a medium/high level security policy, i.e. a realistic situation for the major utilities operating in Europe.

6. POLISH TEST CASE. PROCEDURE FOR TESTS ON THE CYBER LAYER: CONTROL CENTRES

The Polish case study describes simulations of hypothetical cyber-attacks on three substations, critical for security of power supply for Warsaw agglomeration, which would result in cascading loss of power supply in entire Warsaw city.

Carrying out successful attack on three substations is possible when an attacker gain access to them resulting in possibility of execution of malicious code, issue invalid command or control damage ICT systems gathered there.

For the purposes of our study, a specific period of time has been assumed: 21 September, 10 a.m. – 16 p.m., on Friday, which will result in a hypothetical 6-hour break in the power supply in Warsaw agglomeration.

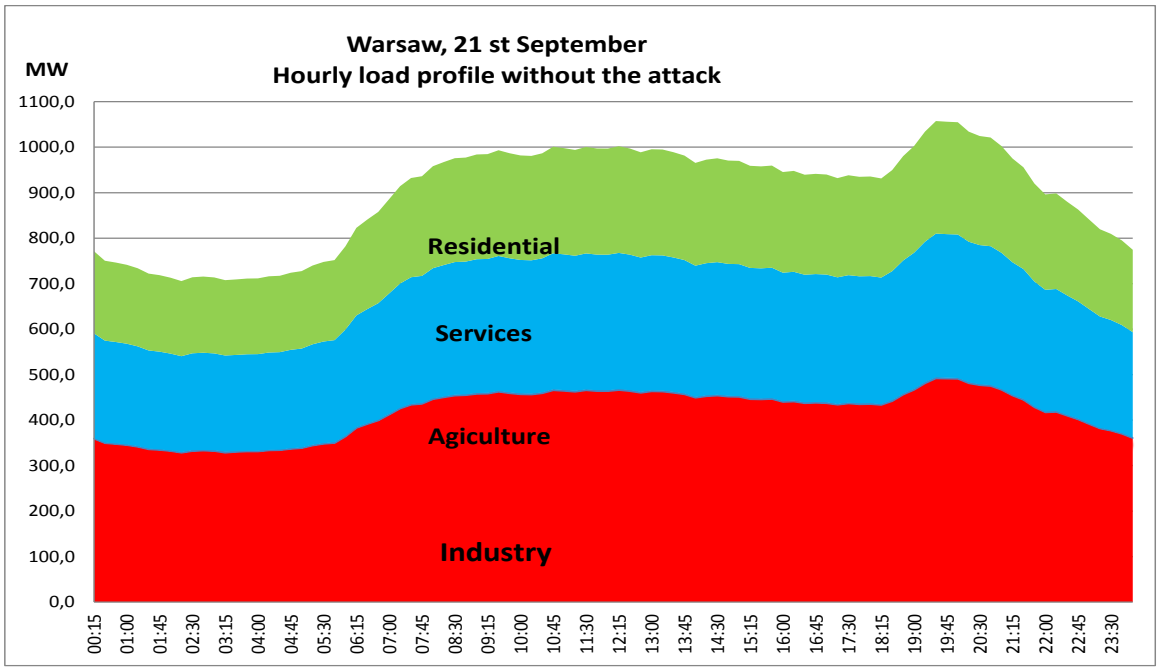


The daytime load is always maintained above 705 MW, reached the minimum at 2.30 am with the value 705,6 MW and maximum above 1057,5 MW at 7.30 p.m. during the evening peak.

Hypothetical attack for Warsaw critical 3 substations, and electricity interruption in Warsaw for purposes of Polish case studies affected on different customer group and has different consequences on them.

Taking into account the ratio between the annual consumption in Warsaw and in Poland, structure of energy consumption in Poland as well as the number of working days the consumption load profiles for 21st September for main categories of users: industry, agriculture, services (commerce and public services) and residential have been estimated.

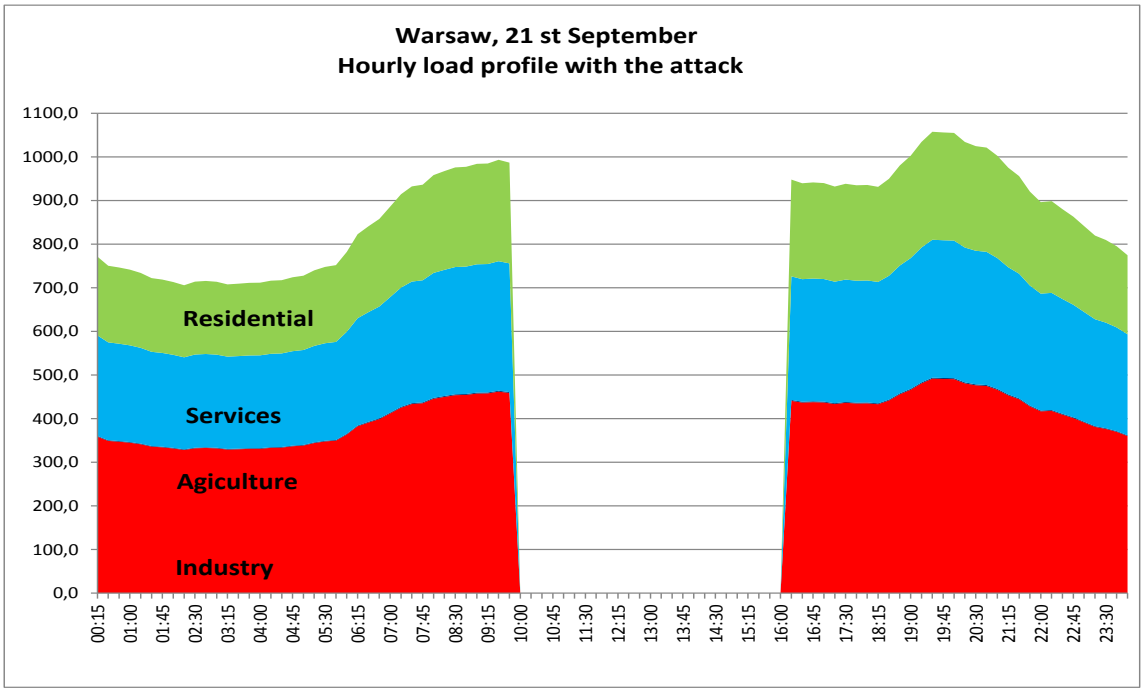
Hourly load profile without the attack.



Total electricity not supplied due to blackout between 10 a.m. to 4 p.m. equal to ca. 5904 MWh. Electricity was not delivered to the following customers:

- industry and service– 4552 MWh,
- households – 1340 MWh,
- agriculture – 12 MWh.

Hourly load profile with the attack.



For the Polish case study analysis the following security standards: the ISO /IEC 27000, the NIST SP-800-53 and the IEC 62351, have been identified as particular relevant.

ISO 27001/27002 - Information Security Management Systems series of standards, with code of practice for the security of information technologies. Also its extension - ISO/IEC 27019 - Information technology — Security techniques — information security management guidelines for process control systems specific to the energy utility industry - the systems and networks for controlling and supervising the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes, which allowing the energy utility industry to implement a standardized information security management system was presented.

ISO 27001 is based on British standard BS 7799, first edition was on 2005 in Great Britain and has been revised by ISO/IEC 27001:2013. Polish version of ISO 27001 was published on 2007, and is known as PN-ISO/IEC 27001:2007.

ISO 27001/27002 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It set out also requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

This standards point to the need for risk analysis as a basis for decision-making to define list of applied security. It focuses on security of information - to achieve suitable level of confidentiality (in relation to risk analysis), availability and integrity should translate to appropriate technical and organizational security measures. ISO does not include scenario implementation, leaving an organization to develop its own countermeasures.

NIST SP-800-53 – Information Security, Recommended security Controls for Federal Information System and Organizations and dedicated to Industrial Control System (ICS) - ICS SP-800-82 – Guide to Industrial Control Systems Security, define mandatory, what kinds of countermeasures have to be running in order to achieve appropriate level of security, and also provide implementation of ready scenarios.

ICS SP-800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities and sources of incidents to these systems, as well as provides recommended security countermeasures need to apply to mitigate the associated risks.

IEC 62351 - Power system management and associated data exchanges – Data and communications security. The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Power Systems Management and Associated Information Exchange is responsible for developing this standard series.

The scope of the IEC 62351 series is information security for power system control operations. This is a standard for enhancing other communication standards and architectural operating in the field of energy (in

particular, the IEC 61850, the IEC 60870 and DNP3) for guidance in such areas as communication security and access control.

The main objective of IEC 62551 review was to examine to what extent will increase safety of operation of ICS as result of works associated with construction of ICT security only at the lowest levels of functional ICS SCADA (e.g. power stations).

The most recommended way to increase level of security is comprehensive implementation of countermeasures. The list of countermeasures implementation of which could result in detection and interruption or minimize consequences of attacks according to the above scenarios was prepared.

7. TEST RESULTS EXPECTED INFORMATION

Two types of information will be made available for the Results Evaluation:

a. Information facilitated together with the attack scenarios
b. Information obtained as a result of the simulation during the study.

7.1 Information Complementary to the Scenario

The following information is descriptive of the scenario and complementary to it:

a. Scenario description including:
    i. Title and short description of the scenario.
    ii. Date and time.
    iii. System conditions before the incident. In case of physical studies will include: Load and generation profiles and system topology.
    iv. Load evolution and generation priorities.
b. Incident Description including:
    i. Incident description
    ii. Elements affected and that become unavailable due to the incident.
    iii. Time[6] to recover each one of the elements unavailable in the system.
c. Standards and countermeasures. For each one of them:
    i. Investment cost
    ii. Description if the action is taken only because the threats or is an advancement of already planned actions.

iii. Operative costs, apart from potential increase in generation costs that will be detected in the simulations

7.2 Information obtained from the Simulations

From each one of the simulations in the physical system, the following information could be obtained:

a. Power not served to the clients.
b. Operating cost, as the generation in each unit.

Please note that physical simulations could be necessary to be executed even in cases of cyber-attacks. The end objective of any malicious activity is cause damage and have notoriety, especially in the mass media. These objectives will not be accomplished by a simple incident in a control centre. The Control Centre can be destroyed but if this does not affect the service, will not cause any damage to the general public and country economy and will attract no attention to the mass media.

---

6 It could be convenient fix a time unit to be used during the studies. The value of the unit will be function of the expected total duration of the incident. Any consideration will be a function of this unit.