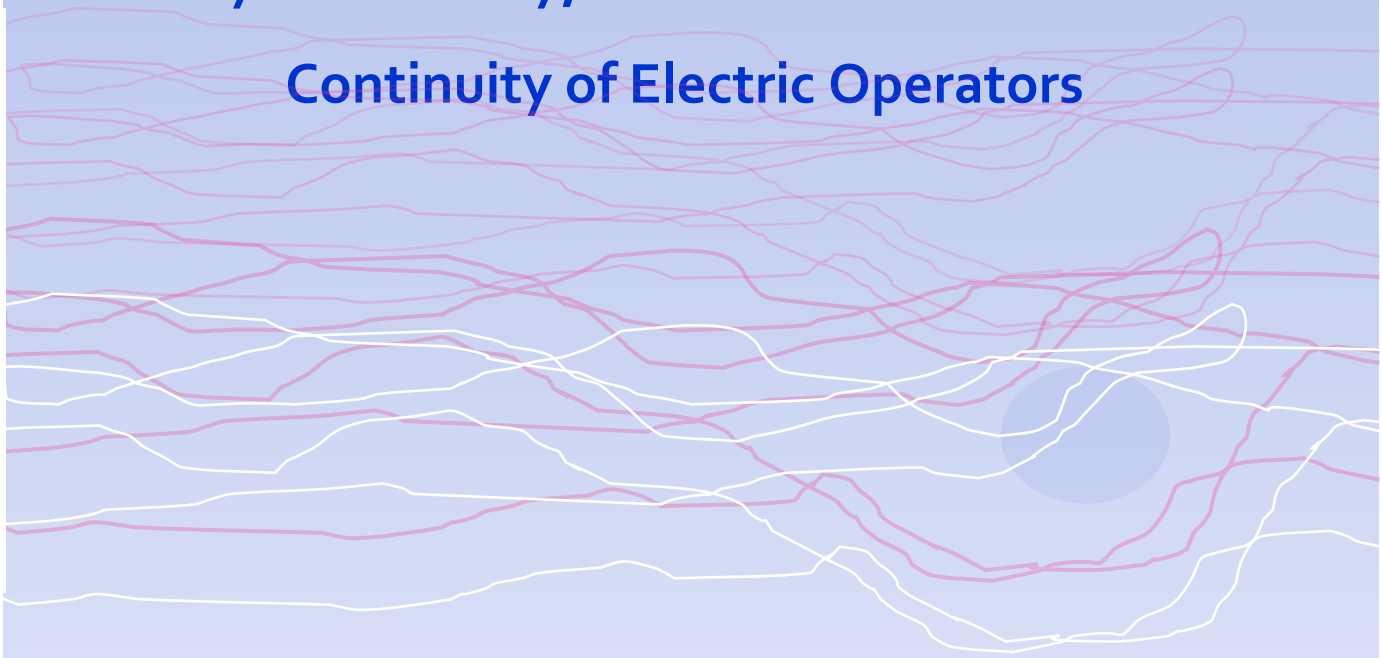
Principles, Guidelines and Good Practices for management of Cyber Security, Resilience and Business Continuity of Electric Operators



Issued by The National Observatory for Cyber Security, Resilience and Business Continuity of Electrical Grids

The National Observatory for Cyber Security, Resilience and Business Continuity of Electric Grids was created to develop a tool that allows a unified management of cyber security, to promote and implement collaborative initiatives, exchange information and research in the Generation sector, Transmission and Distribution of Electric Energy through the involvement of public and private partners.

The permanent work table that was formed in 2015 still carries out its activities concerning National Electrical Critical Infrastructures at all levels of the national Generation, Transmission and Distribution system (High Voltage / Medium Voltage / Low Voltage), with specific attention to the new Cyber Security set-ups of the modern National Grids, which presents ever-increasing nodes of Green Generation as well as modern Smart-Grid / Micro-Grid (Distributed Generation).

The present guideline is for the attention of national and European companies in the electricity sector, small, medium or large; it suggests objectives and methods for dealing with cyber security issues, in an integrated way and aligned with the NIS Framework and the National Cyber Security Framework, with international guidelines and standards; it also recommends the preparation of the most important safety checks to be implemented in strict agreement with the supply chain.

Its first effort is aimed at identifying methods that allow the involvement of Top Management, facilitating a common language between various company roles with different backgrounds and sensitivity on the topic, up to the definition of a common methodology for reporting to the members of the Board of Directors all IT risks related to Information Technology (IT) and Operational Technology (OT).

It also want to suggest how to improve exchange of information, how to share 'best practices' for enhacing awareness of the impact level of cyber risks in energy companies and in the energy sector as a whole.

It highlights the need for the energy sector to adopt a systemic approach, which assesses the problem through the control of the entire supply chain, in order to improve the protection systems and to limit any possible "domino effect" that could be caused by a failure in an area of the value chain.

The present guideline also seeks to reinforce the operators' awareness of how crucial it is to manage the process with correct planning of operational continuity management and highlights how Cyber security resilience must become an integral and indispensable part of the management system itself.

I would like to sincerely thank A2A, AIIC, ANSALDO ENERGIA, CISCO, DELOITTE, ENEL, IREN, LEONARDO, MISE, PANTA RAY, KASPERSKY and TERNA, who, in collaboration with the Polytechnic School of the University of Genoa, have allowed the creation of the first edition of the document.

The President of the Observatory
Prof. Paola Girdinio

Table of contents

1. Introduction and purpose of the document

The document presents the Cyber Security guidelines for energy sector companies, with reference to the NIST framework (National Institute of Standards and Technologies) and the technical standards related to the specific sector. The first chapters include both explanations, useful also for managerial roles, for better understanding of the risk context, together with recommendations for implementing countermeasures at organizational and operative levels.

2. What is Cyber Security and its Regulatory Context

This introductory section aims to provide examples of Cyber incidents occurred in the energy sector in order to highlight the importance of the implementation of effective countermeasures to counter cyber risk.

2.1. Introduction

We can affirm that in recent years the industrial and energy context have evolved towards ever more modern and digital technologies. In particular, Information and Communication Technology (ICT) is redesigning the industrial history of strategic infrastructures. We are currently facing the fourth industrial revolution, which includes an evolution of IT and OT networks by the integration of these two areas, which -from a technological point of view- are converging towards the "Internet of Things" (IoT). Therefore, with the increase of devices connected to the network and, in particular, with the arrival of IoT applications, together with various technologies and their integration (such as Cloud Computing and Big Data), inevitably a series of problems will follow, such as interoperability, safety and reliability of a new generation of strategic / critical infrastructures.

At the same time, the energy sector has lived and is still experiencing great changes to this day. In fact, the market liberalization is imposing a change in the choice of sources of energy generation in favor of renewables and is promoting an ever increasing level of interconnection between electric grids; as a result, this has generated a proliferation of energy operators of an increasing number of regions /countries.

Within this new reality, more digitized at both national and European level, cybersecurity plays a very important role and, therefore, is under the watchful eye of the major energy players (Generation, Transmission and Distribution), both national and European (in the future, the European Super Grid); all these players are part of a single body of critical infrastructures such as are electric infrastructures, which must -among other things- guarantee, on various levels of responsibility, the provision of a public service and the continuity of this essential service for all European regions/nations.

The International reference standards, Incidents and Countermeasures, refers to technical standards and guidelines regarding the safety of power generation, transmission and distribution systems; it was possible to carry out an analysis of NIST (National Institute of Standards and Technologies), NERC (Natural Environment Research Council), NIS (Network and Information Systems), NISTIR (National Institute of Standards and Technology Interagency Report), IEC (International Electrotechnical Commission), ISO (International Organization for Standardization), CIP (Critical Infrastructure Protection) standards.

This analysis was carried out considering the requirements of Reliability, Integrity, Confidentiality and Non-Repudiation, specified in the various regulations.

The importance of considering Cyber Security in a multidisciplinary way has emerged. In the energy sectors, and specifically in the electrical sector, the different areas of information technology, networking, automation and control of complex systems (SCADA, IEDs, ICS, DCS, HMI, PLC, ...) were considered.

This guideline suggests the definition and implementation of a multi-level security management model, applied to automation, control and supervision systems. The technological transformation of energy systems will culminate with the affirmation of so-called cyber-physical systems; in fact, during various meetings of

The National Observatory it was discussed how system evolution is reaching a first step of affirmation of cyber-physical systems, with consequences such as repercussions on the lives of all citizens who use essential services.

2.2. Specific Cyber Security requirements for electrical systems

While Critical Security Controls (adapted from SANS) and the NIST Framework apply to IT systems, cyber-physical systems (CPS) require a specific set of security checks, and the kind of protection is amplified by the critical nature of the systems themselves.

Furthermore, the order of importance of the "classical" requirements of Reliability, Integrity, Confidentiality and Non-Repudiation is different from that of IT systems (in which the attention for Confidentiality of information normally prevails).

Therefore, risk analysis and assessment activities cannot be limited to NIST Framework alone, but -in the energy sectors- they must necessarily include other security frameworks as well. In order to name the most significant ones, I shall recall NERC-CIP, ISA, IEC, and – obviously - NIST for CPS protection.

A clear integration of the NIST Framework is needed to ensure safety and resilience of industrial control systems and availability and maximum reliability of safety systems and procedures.

The need to raise safety levels is also due to the progressive introduction of new technologies, of both energy and ICT sectors (e.g. Cloud computing, wireless transmission systems, industrial IoT).

2.3. General aspects

The (complex) transformation of energy systems requires new approaches to network and system security. To do this, the following activities shall be required:

- integrated risk analysis
- risk and threat impact analysis assessment, aimed at safeguarding business continuity;
- analysis, by type of plant / site, of typical risks
- assessment and management of physical security risks
- assessment and risk management of technological vendors
- assessment and risk management of third parties (suppliers of products and services)
- adoption of integrated risk management models.

2.4. Previous requirements and interests

The needs front may be summarized by the following list of the additional requirements encountered during the recent analysis of regulations, guidelines and recommendations:

- communication security requirements in automation and control platforms based on Smart Grid model
- safety and security requirements for renewable energy production plants and systems
- security requirements for distributed energy resources (DER - Distributed Energy Resource)
- safety requirements of electric smart meters

2.5. Main actions to strengthen cybersecurity

These are some of the main applicable cybersecurity strengthening actions, recently announced at international level:

- use of additional physical protection capacities of plants (integrated safety)
- development and adoption of measuring capacities of availability and safety levels of plant control systems
- development and adoption of monitoring capacities of electrical transmission and distribution grids
- development and adoption of monitoring capacities of transmission systems availability
- development and adoption of security incident detection and reporting capacities
- verification test of networking robustness levels

- verification test of reliability levels of *IoT* installed devices
- verification test of readiness and adequacy levels of information technology/cyber defense plans.

3. An approach to Cyber Security for the electric sector

This section is dedicated to company management. It intends to provide a high-level overview on how to manage Cyber Risk in critical electrical infrastructures.

3.1. The role of Top Management in Cyber Risk Management

Businesses are increasingly the subject of sophisticated attack techniques and for this reason they have started to acquire increasingly significant technological and financial resources to improve their protection. The threats affect all companies: not only large, but also medium and small companies have become potential targets due to the presence of significant intangible assets and a lower level of protection.

Damages are not exclusively linked to theft of intellectual property, but also to company reputation. It is more and more frequent that, due to attacks, some managers lose their jobs.

The increasingly widespread rules of Corporate Governance require that managers should be responsible not only for the conduct but also for the protection of their activities.

For the reasons stated above, it is necessary that Board of Directors and top management of companies/institutions/organizations understand and evaluate these new risks, by balancing growth and market profitability with cyber risks mitigation expense for company protection. This task is already foreseen in the mandate of the Board of Directors who, also with the support of Control and Risks Committee, where present, is called to define the nature and level of risk compatible with company strategic goals, by taking into consideration assessments of all those risks that may become significant in company's perspective of medium-long term sustainabile activities. Furthermore, the Board is also called to assess the adequacy of company's organizational, administrative and accounting structure. All these principles are already contained in Borsa Italiana's self-regulatory code, only to name an example. There is no doubt that cyber risk should be assessed as a potential "main risk" for companies and public organizations, as highlighted in the 2014 Annual Report of the Presidency of the Council of Ministers on Italian Republic security policy.

There is no doubt that, given the scale and effects of cyber threat, this should be included among the major risks that each company and organization must nowadays evaluate and manage. As part of the implementation phase of these Corporate Governance principles - and in line with indications contained in the National Strategic Framework and in National Plan - companies should start, at Board of Directors' and top management's level- the activities /practices listed in the following paragraphs.

3.1.1. Cybersecurity as a strategic element in corporate governance policies

Corporate governance refers to the set of rules - of all levels (legislative, regulatory, etc.) - that regulate the management and steering of a company (or, more generally, of an organization, whether public or private) and includes the connections between the various actors involved (the stakeholders) and the goals of the organization itself. The main players are the shareholders, the *Board of Directors* and the management. More generally, an organization's governance encompasses a set of corporate rules, relations, processes and systems through which the trust authority is put in practice and controlled.

Corporate governance structure therefore expresses both the rules and processes by which decisions are made in a company, the ways by which corporate goals are set and the company instruments for achieving and measuring the results achieved.

All company areas contribute to the drawing up of those guidelines that define organization governance; in this sense cybersecurity must thus be evaluated from a “shared systemic vision viewpoint”, which is to say that cybersecurity must not be seen as a built-up or disturbing element within the company but- on the contrary- as a company element embedded in the company itself: in fact, as it is a fundamental aspect of company's risks definition process, it is one of the strategic elements through which corporate vision expresses itself.

Top management therefore prepares an integrated cybersecurity governance plan that involves all company functions and includes all areas of operational risk, that clearly defines roles and responsibilities, as well as proper assignment of roles \ responsibilities according to the principle of segregation of tasks. The plan must report three different levels of control: a first level, under the direct responsibility of a production/business function (Production, IT, Sales, etc.); a second level, under the responsibility of a security function, external to the production/business functions; and a third level, under the responsibility of an internal audit function (Audit).

The function responsible for second level controls must deal with the definition of corporate security policies and must verify their correct application (i.e verify security policies compliance).

Furthermore, top management will ensure that the integrated governance plan meets the following requirements:

- To align risk management to company's strategic goals
- To define, for each risk, the estimation of products and services delay, should the risk occur; the estimation must be shared among top management itself.
- To define an organizational model that provides coverage of the entire company's security processes and domains
- To define, within the organizational model, an integrated risk management process, i.e. a process that allows to frame, contextualize, evaluate and monitor risks, to respond to threats and attacks to assets, services and individuals, not only belonging to the organization itself, but also belonging to external organizations and / or to the State
- To allocate resources efficiently and effectively for a systemic business management that includes risk management
- To provide – in accord with criteria, metrics and methodologies of analysis shared among top management (such as System Dynamics) - risk management process's measurement, monitoring and reporting; in particular, such reporting will have to respond to the need to assess the level of effectiveness and efficiency of the organization in responding to risks, as well as highlighting – taking into account organization's dynamism and "systemic behavior" complexity levels - whatever changes to the company structure should be needed in order to better respond to risks themselves

Top management shall ensure that the governance model and the cybersecurity plan are in line with both the Enterprise Risk Management Plan and the Enterprise Crisis Plan.

In fact, impacts deriving from cyber threats are nowadays more and more frequently classified as "*crises*" and therefore added to the overall company crisis typology list; consequently, a coherent and integrated way of managing all threats as a whole- and their impacts - including cyber ones - is essential.

It shall therefore be necessary to use decision-making tools and methodologies which not only are based on an integrated system model (e.g. Model-based Governance) but also take into account all possible different typologies of company dynamics.

Among the aspects that are brought with ever greater force to the attention of the top management are risk management methods topics related to outsourcing or Cloud-based service contracts.

It is often believed - erroneously - that the ratifying of outsourcing or Cloud-based service contracts implies - compared to the signing of more "traditional" contracts that rely on services and data structures within the company - a greater amount of company risk transfer to third parties; on the contrary, the only difference consists in a different way of carrying out operational safety management, which, in reality, needs a much more careful assessment effort by both the top management, the CISO and all those organizational structures which are involved in the management of the service itself.

3.1.2. Roles and responsibilities

Proper corporate governance must be integrated; that is, it must carry a holistic vision, shared among members of its management, of interdependencies between different company functions and of impacts of problems arising in a specific function on cascade across other functions.

The Governance itself should provide for the definition of a proper organizational structure carrying an embedded process of continuous improvement within its own processes and policies; this therefore abates function managers' wrong mental models and progressively lead the organization to be of that kind of virtuous organization named as Learning Organization.

It is commonly known that "social" strategies of aggression have proved to be particularly effective in circumventing markedly technological controls; this is the case, for example, of strategies underlying the multifaceted phenomenon known as Insider Threat ; such strategies are to the detriment of security procedures purely focused on the introduction of IT materials coming from the outside of the company; another example are aggressions carried out through the concealment of external service personnel (as in the well-known case of Mall Target, in the USA).

Cybersecurity is therefore an issue that involves the entire company, from top management to operational structures, and, consequently, the company should be subject to systemic evaluation and continuous monitoring. Companies often consider it sufficient to assign cybersecurity management exclusively to their ICT structure, without involving business areas.

Although undoubtedly ICT plays a central role in security management, this kind of approach is by its own nature incomplete and it presents the organization with the possibility of a number of problems; we list some of them below:

- cyber risk is evaluated mainly from an information systems point of view, thus inadequate countermeasures are often provided as a result;
- it is implicitly assumed that there is a limited possibility of combining business needs with the entire organization's risk reduction needs;
- intrinsic organizational difficulties are introduced when security processes and countermeasures within different company functions (business, production, administrative, etc.) are implemented independently;
- safety management plans result to be partial;
- it is possible that security investments pressure on ICT investments: as a result, cuts in ICT budget frequently fall directly on cybersecurity budget.

In order to ensure complete coverage of the company, it would be advisable to leverage security functions of ICT division with "logical" security functions placed outside ICT; such functions generally report to the Chief Security Officer or Chief Risk Officer or - in some cases - directly to the Director General, Chief Operating Officer or Chief Executive Officer.

These logical security functions are guided by the CISO - Chief Information Security Officer.

This approach guarantees the respect of the principle of segregation of duties and responsibilities, and ensures the separation between first and second level security controls as well: the first level is charged to ICT or to business/production functions, the second to the CISO and/or to logical security functions.

3.1.3. The role of the CISO

The role of Chief Information Security Officer (CISO) is assigned by top management, who ascertains that it is assigned to a person with adequate skills and experience in the field.

Responsibilities of the CISO should be, among others:

- of starting-up and/or evolution of a corporate IT risk management plan; it is therefore necessary that risk be approached in "Enterprise" mode, according to ERM (Enterprise Risk Management) principles, for example the ISO31000 standard
- of risk evolution monitoring and associated plan adjustment
- of analyzing major incidents occurred, their impacts and actions issued in order to mitigate the risk of incidents' future occurrences
- of periodic reporting to top management
- of establishing a function which acts as connection between top management, company functions and national and foreign institutions

Within medium/large companies, such role should be assigned to a manager exclusively dedicated to these activities.

3.1.4. Integrated monitoring

Top management periodically assesses risks, once they have been identified, in accord with overall *ERM* and risk mitigation plan. Top management is called upon to express itself and decide on decisions related to cyber risk mitigation, acceptance and transfer strategies, just as is common practice management approach for handling all other company risk typologies.

3.1.5. Resources

Top management shall need to evaluate whether the proposed security plan is properly supported by adequate level of resources, i.e. whether planned economic effort and foreseen personnel for carrying out planned activities levels are adequately allocated. Decisions related to allocation of resources must be consistent and in line with company risk management plan (Enterprise Risk Management). Should residual risks occur, these must be adequately assessed; in case they aren't efficiently assessable with general guideline principles and methodologies, ad-hoc risk treatment plans shall have to be issued: top management shall be called upon for evaluation of different applicable countermeasure possibilities for reducing, avoiding, eliminating, or transferring risk.

3.1.6. Cybersecurity awareness and culture

Top management shall need to conduct activities for promoting of awareness and enhacing cybersecurity culture at all company levels. The *CISO* will prepare a program to increase internal and external personnel cybersecurity awareness with the scope to reduce risks arising from improper or incorrect deployment of information processes or of information-handling tools within the organization. Furthermore, trial tests may be planned - at internal, sectoral or national level- with the scope to measure and improve expertise and skill levels of both top management and company functions called to manage cyber events.

3.1.7. Fostering exchange of cybersecurity information and cooperation within organizations

Top management shall promote and support initiatives aimed at establishing or strengthening cooperative relations with organizations belonging to the same sector, as well as with institutional bodies responsible for contrasting cyber threat at national level. Membership to sectoral CERT -or to institutional CERT (such as Italian CERT Nazionale)- and cooperation with other companies allows for the improvement of understanding cyber threat, sharing best practices and tools for contrast of cyber threat or -in some cases- allows for the enhacement and development of common skills and expertise on cybersecurity within organizations.

3.2. Top Management's role in Risk Government: Borsa Italiana's self-regulatory code and Corporate Governance body of rules

Cybersecurity is a topic that, by its own nature, must be permanently at the attention of company's top management bodies' agenda; apical organization functions must thus be responsible for the implementation of an adequate level of commitment throughout all hierarchical and operational organization levels; which is to say, they must be responsible for setting that level of commitment which guarantees the organization to achieve its resilience and information asset monitoring-related goals. But what should be the role of apical organization functions when handling a topic which is constantly in danger of being under-estimated and erroneously classified simply as a "technological problem", which thus requests a technological -based approach reply alone?

Most important steering and deployment guidelines are listed below:

- Properly address cyber strategy: Top management, similarly as for other typologies of corporate risk, must steer cybersecurity strategy by the definition of company target cyber risk posture to be maintained (namely, by the definition of company Risk Appetite Framework - RAF), which takes into account main impact scenarios - such as damage to business systems, loss of confidentiality or availability of key information - up to impact on OT systems (Operations Control systems), such as

Industrial Control systems (so-called ICS/ Industrial Control Systems or SCADA systems/Supervisory Control and Data Acquisition systems).
As a result, each business unit's top managers shall deploy – within their own perimeter of systems and data - overall company cyber strategy, thus issuing a set of detailed cybersecurity goals specifically related to their area, namely business unit top managers shall define goals which ensure complete support of company needs, provide ad-hoc input information for information system profiles definition technical assessments activities, and carefully balance revenue - deriving from the reaching\ maintaining of the target company risk posture - with related company cyber risk mitigation effort, expressed both in economic and headcount terms.

- Ensure and verify that, within the entire company, governance and reporting activities are aligned with/ compliant to cybersecurity strategy: Security Policies are certainly Governance activities' core element; security policies' body of rules establishes how cyber defense strategy is deployed, and Cybersecurity Strategic Plan is based on such rules: the Cybersecurity Strategic Plan is a "programmatic" document, namely it states security goals together with related resources and time boundaries needed for goal achievement. In more "advanced" company scenarios, reporting activities related to cyber risk may be carried out in an integrated way along with reporting activities for other types of business risks; in any case, reporting activities for cyber risk should carry a duality of scopes: on one hand, to provide a measure of status of defenses and of effectiveness of protection measures adopted, on the other hand, to measure the level of achievement of strategic plan goals, in terms of time, cost and quality.
- Boosting company cybersecurity awareness: Promotion of company cybersecurity should be favored at all company levels, thus it may be divided in
    - Top Management
    - Business Owner
    - Both internal and external company stakeholders (i.e. which include all elements of company supply chain)
- Enhacing company cybersecurity awareness means promoting - among company employees and/or company stakeholders - of mindfulness of which should be ones' own correct cyber security behaviors, namely of those behaviors which are compliant to security practices, in order to avoid that employees or stakeholders themselves may perform tasks in such a way as to cause a flaw in corporate cyber security defenses. Incorrect behaviors - such as, for example - managers sharing their own personal access credentials with fellow staff, employees using personal e-mail addresses or Cloud-based services for forwarding or storing company information or using social media or instant messaging services (in primis, whatsapp) for communication of confidential information - must be banned as, not only they may cause a breach in cyber security defenses per sé, but may also increase cyber attack or cyber incident probability of occurrence level, because of incorrect behaviors spreading throughout all company levels through their emulation.

4. Cyber Security role in business continuity and risk management system

The latest edition of the Horizon Scan Report - published annually by the Business Continuity Institute - states that the main concerns of Business Continuity Managers are usually cyber-attacks (88%) and data breach threats (81%). The Cyber Resilience Report itself - published every year by the same institute - shows that, in the last 12 months, 66% of all organizations have suffered from at least one cyber-attack, while a surprisingly high percentage (15%) have suffered from more than ten attacks.

It is clear, then, that it is becoming an increasingly important topic for business continuity and risk management professionals as they work to safeguard their organization's resilience against cyber incidents and attacks.

The energy sector – especially in its electric subsector - is no exception: the world is becoming increasingly digital, and so are the threats we electric operators must face. Within a broader context of careful business continuity planning and appropriate risk management practices, protecting organizational resilience from cyber-inflected critical events has never been so crucial.

With such new risk scenarios and the electric sector's increasingly complex supply chain – which is now characterized by an intense use of information technology – electric operators must therefore set up Business

Continuity and Risk Management Systems capable of ensuring operational continuity – especially of energy supply processes - even in the face of disruptive, cyber-inflected critical events.

Business continuity, in this sense, can be understood as an electric operator's capacity to maintain service at predefined adequate levels following an incident. The Business Continuity Management System's scope does not only include an organization's ICT, but also its people, its buildings and work-site, its assets, and its suppliers. We therefore advise electric operators to name and empower a Business Continuity Manager to establish a Business Continuity Management System.

Specifically, and with continuous improvement in mind, we advise electric operators to define, implement, and maintain the following:

- Business continuity and risk management organizational policies that clearly define the scope and the governance model of their Management Systems - this may be achieved through the assignment of competent organization personnel to such tasks and through top management's commitment to a constant improvement of the organization's ability to prevent and respond to cyber-inflected critical events;
- A program for constant personnel awareness training, i.e. organizing sessions aimed at embedding business continuity, risk management and cybersecurity topics and skills within organizational cultures;
- A business impact analysis that identifies, qualifies, and quantifies the urgency of each activity undertaken by the organization, and that assesses the impact over time on the delivery of products and services of a critical activity disruption;
- A continuity requirements analysis which aims to clearly define the type and quantity of resources the organization needs to restore a service after an interruption, and a threat analysis to detect possible points of failure and unacceptable risk concentrations (focusing especially on cyber threats);
- Operational continuity solutions and cyber threat mitigation measures that are always consistent with the organization's objectives;
- A constantly updated Business Continuity Plan that clearly and efficiently delivers the set of documented procedures designed to either guide the organization in its response or recovery to a cyber-inflected incident or - after a cyber-inflected crisis – in its resumption or restoration of activities to predefined satisfactory levels. Typically, such plans describe the resources, services, and activities needed to ensure the continuity of the activities of critical business functions;
- A constantly updated Disaster Recovery Plan – itself an integral part of the Business Continuity Plan described above - that establishes the technical and organizational measures needed to ensure the correct functioning of the organization's data centers and of the relevant IT procedures featured in non-production work-sites;
- An annual program of simulated cyber incident exercises and tests aimed at training the organization's efficient and efficacious response capabilities to such incidents and, at the same time, aimed at identifying possible limitations of the organization's Business Continuity and/or Disaster Recovery plans – the goal being the continuous improvement of the organization's Management System.

Furthermore, an organization's Internal Audit function should periodically report the results of its independent analysis to the Board of Directors - at least once a year is recommended. The goal is to verify and measure the organization's level of compliance to the following international standards and methodologies:

- ISO 22301:2012 Societal security --Business continuity management systems -- Requirements;
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements;
- ISO 31000:2018 Risk management -- Principles and guidelines.

4.1 The Business Impact Analysis (*BIA*)

The **Business Impact Analysis (BIA)** is that process which analyzes an organization's activities and the effects that an interruption of the same could have on the organization itself. The BIA is the foundation on which a Business Continuity Management Program is built, as it is the tool that identifies, quantifies, and qualifies the impacts over time of a process disruption. The BIA also provides data useful to determine appropriate business continuity strategies, because it allows an organization to identify and classify critical processes according to how urgently they need to be recovered.

Although there is no standard approach for collecting data when executing a BIA, professionals - either wishing to execute this process for the first time or needing to conduct it periodically as part of their Management System - should take care that the following requirements and BIA elements are respectively met and featured:

- Before beginning the BIA, the Business Continuity Management Program's scope and the organization's critical processes perimeter needs to be clearly defined;
- Well-defined time intervals – previously approved by Top Management – as a means to quantify the consequences of product/service delivery interruption;
- A qualitative and/or quantitative description of various impact levels (from a product/service interruption) over time; this kind of information will serve as a clear, data-driven basis on which Top Management can base its decision regarding which activities to prioritize following a disruption;
- The BIA methodology employed should be the same throughout the whole organization, to ensure that different processes are comparable, and should be as rigorous as possible so that process-owners are empowered to report their data as objectively as possible.

We can say that an organization has conducted a successful BIA process only if its BIA complies with a few key principles. All the collected data must, for instance, be exclusively relevant and pertinent; impacts must be described and measured in such a way as to be sufficiently realistic while still allowing for a decent margin of error; and the personnel conducting the BIA must avoid the temptation to evaluate impacts based on their likelihood. This last point is key: the BIA **is not** a risk analysis.

The **ISO TS 22317:2015** is the international methodological standard for a Business Impact Analysis. It proposes a well-defined and detailed methodological approach to the BIA that consists in a set of activities which, when correctly deployed, allow an organization to obtain useful results for the creation of business continuity strategies and tactics aligning with the organization's objectives.

Prerequisites for conducting a good BIA include, above all:

- The ex-ante definition of an analysis perimeter, consistent with the scope of the Business Continuity Management Program;
- The definition and communication within the organization of clear roles and responsibilities for the development of the impact analysis and of risk and threat assessment activities to safeguard business continuity;
- A well-defined top-level mandate behind the organization's BIA activities, demonstrating strong Top Management support for BIA project activities;
- The allocation of adequate personnel to develop the impact analysis, and risk and threat assessment activities to safeguard business continuity, thereby training these personnel to be in-depth BIA experts.

Moreover, the BIA's role, at a first stage, is to:

- Identify the organization's priority products and services, namely those products and services for which there a detailed impact analysis of a product/service interruption is needed;
- Determine the organization's impact categories (typically, these are economic/financial, commercial, legal/regulatory, and reputational) and their criticality level thresholds;
- Select the most appropriate data sources for the data collection process;
- Organize interviews, workshops and questionnaires for the data collection process.

A first-stage BIA is typically called an Initial BIA; in addition to the points listed above, an Initial BIA will also need to include the organization's Maximum Tolerable Period of Disruption (MTPD) indicator.

A detailed impact analysis can only come after the Initial BIA phase's conclusion. Indeed, it is only now that the organization has identified the scope of products and services, processes, and activities that will be the object of subsequent BIA activities.

The organization must conduct the impact analysis on a plurality of different analysis levels, listed below:

- **The organization's product and service level**: the organization's products and services are analyzed with the aim to establish an MTPD indicator for each group of products / services, determine their Minimum Business Continuity Objective (MBCO) indicator, and define a draft version of their Recovery Time Objective (RTO) indicator;
- **The organization's process level**: the organization's processes are analyzed with the goal of outlining an MTPD indicator for all those processes included in a critical product / service area, of determining their Minimum Business Continuity Objective (MBCO) indicator, and of establishing a draft version of the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) indicators
- **The organization's activity level**: the organization's activities are analyzed to verify the correctness of the above-listed indicator values, previously determined for both products/services and processes, and to collect business continuity requirements in terms of personnel, sites, economical resources and suppliers. At this level, then, the Business Impact Analysis focuses on in-depth data collection and on the detailed analysis of the business continuity requirements (i.e. data related to resources, sites, technology, equipment, suppliers, etc. needed for the achievement of the desired business continuity targets).

Once data collection activities are concluded, it is crucial to consolidate all the results achieved thus far; this allows the organization to compare critical processes by looking at their specific levels of urgency. A data consolidation moment is essential for choosing strategies and operational continuity tactics in line with the organization's objectives.

In sum, a BIA's objectives are as follows:

- to detail and describe the impacts over time of a product / service disruption, should it take place;
- to establish a maximum tolerable interruption or product / service disruption period (namely, ratify the Maximum Tolerable Period of Disruption - MTPD indicator)
- to ascertain an organization's recovery priorities for critical processes;
- to identify which process interdependencies and which internal and/or external resources the organization needs to meet binding SLA (Service Level Agreement) requirements.

Specifically, a Maximum Tolerable Period of Disruption (MTPD) is the amount of time before a critical product and or service disruption becomes unacceptable, i.e. the amount of time before the disruption begins to threaten the organization's very survival.

4.2 Risk Management and its evolution to Dynamic Risk Management

As already previously said, organizations are today called to face constantly evolving scenarios of cyber risks. In such context, the starting point is to define what a "risk" is: a risk is the effect of uncertainty of a goal achievement (ISO Guide 73: 2009). With such definition of "risk" it is evident that a risk may reveal positive implications too: should these occur, we call them opportunities. For the ends of the present guideline we shall limit our analysis to the case in which "risks" are linked to events with potential negative implications only.

It is also important to ask oneself what a risk is within the cyber world: a "risk" in the cyber world is a potential event linked to the loss of confidentiality, integrity or availability of data or information; such loss could imply negative impacts on the organization itself, on the population, on other organizations or - particularly relevant for the ends of the present guideline - on the nation as a system.

A risk in the cyber context arises when a vulnerability of a system - or of single elements of the system - meets a threat (cyber threat) and such threat has the means to "exploit" the specific qualities of the vulnerability itself, namely to cause an impact.

Just as we have provided a definition of "risk", we need now to define what a "threat" is: a threat is defined as "the potential cause of an undesirable event, which may cause harm to individuals, a system or an

organization" (ISO 22300: 2012).

It follows that the "cyber risk" topic shows characteristics of significant complexity, thus needing the definition of a "structured" approach which allows for the analysis of "cyber risks" in terms of efficient identification, measurement, management and monitoring activities of cyber risks themselves; such approach aims to enhace organization awareness on "cyber risk" and, at the same time, to support and guide the organization when it needs to take decisions on "cyber risk".

A proper risk analysis is therefore a mean through which it may be possible to identify the main criticalities, vulnerabilities and possible applicable countermeasures to be deployed for reducing risk exposure within organization's mission critical environments.

We have a variety of different reference cyber risk management methodologies and approaches (e.g. NIST 800-30, ISO27005, IRAM2), but they all express the common need to identify at least the following set of steps:

- Identification of the scope of intervention and its related context: Within such activities, the organization's in-scope critical processes' perimeter shall be assessed; consequently, the related cyber context -given the identification of such perimeter - shall be assessed; finally, the risk assessment data level detail of in-scope critical processes shall be defined.
- Execution of risk assessment: Within such step, activities aim to identify cyber risks, countermeasures for such identified risks, and to assess a both quantitative and qualitative analysis of risk level associated to each target element of risk analysis perimeter.
- Identification of risk management and/or acceptance plans: Within such step, activities aim to identify plans for risk mitigation, treatment or transfer; such plans must include countermeasures - both specific or compensatory - as well as insurance policies - or other means for risk transfer - and ratios for evaluation of residual risk acceptance.
- Risk monitoring and\or risk reviewing: Within such step, activities aim to analyze and eventually update risk level values and show progress of implementation status level of on-going cyber risk plans. Such monitoring and\or reviewing activities should be deployed periodically and\or on the basis of occurrence of specific triggering events, such as, for example, the event of a change within company strategies: this would be the case of a decision taken within the organization which implies the switching of application typology environments from insourcing to Cloud-based typology.
- Risk communication, consolidation and counseling: Within such step, activities aim to identify - for each evaluation issued - the adequate stakeholders needed for correct risk evaluation and consolidation within each specific organization function; consequently, risks - identified by previous steps described above - will be efficiently "described" and communicated by such identified stakeholders to each specific function risk owner.

All the above steps aim to guarantee overall identification, assessment and monitoring of cyber risks; furthermore, for each identified cyber risk, the above steps guarantee the issuing of:

- the related **inherent risk** value level (namely, the value level of risk beared by the organization at "beginning" of analysis, when planned countermeasures are not yet in place)
- the related **current residual risk** level (namely, the residual risk level beared by the organization at the current date of analysis, when a quota of planned countermeasures are already in place)
- the related **future residual risk** value level (namely, the residual risk level beared by the organization at a "future" date, when a planned quota of countermeasures - not yet in place at the current date of analysis - have been deployed; such yet- to be- deployed planned countermeasure quota should be such as to bring the current risk level value to be considered as "acceptable" by the organization at the planned "future" date of analysis).

Risks are constantly assessed by comparing their updated current residual risk level value with the updated organization risk attitude level value at time of analysis. As a result, risks that are such as to carry a residual risk value level which exceeds the updated organization risk attitude level value shall be managed by adding to the plan the putting in place of additional countermeasures, with the aim to reduce its estimated residual risk level value to an acceptable level.

It is important to highlight that the risk attitude (or risk appetite) topic does not apply to cyber issues only, as it is a topic which applies to management of all types of risks beared by the organization.

In fact, in order to manage cyber risks successfully, it is necessary to manage cyber risk in the same way as is done for other types of organization risks; consequently, cyber risk management should be at the attention of the CCR (Risk Control Committee) and/or of the BOD (Board of Directors): this would allow for top management to coherently evaluate the body of all possible organization risks as a whole and, consequently, efficiently manage investments for addressing mitigation, reduction or risk transfer needs.

In order to reach this end, not only must all risk typologies be included in the analysis, but they must be described and reported on by the means of coherently uniform methodologies and ratios also: therefore, cyber risk must be described and reported on in the same way as all other risk typologies (i.e. strategic, financial, etc.) are.

An extremely effective mean for the pursue of such goal is the effort to align cyber security risk management process with Enterprise Risk Management (hereinafter ERM) process. The ERM is the corporate process through which the organization defines its methods of representation of each organization risk type; furthermore, the ERM process allows for the organization to define its method for representing, consolidating and formalizing the organization's risk appetite level, as well as its method for structuring organization's risk identification, assessment and treatment activities.

In order to report to the CCR and\or to the BOD all different types of risk by the same unique format, namely a format which uniquely represents all different types of business risks and thus allows for the highlighting of differences between cyber risk level value and that of other types of risks (which are managed within the ERM process), a common integrated methodology is necessary: namely, a methodology that allows for the analysis of business risks on the basis of measurement of their related impacts - by a unique scale which applies to all company areas - and on the basis of other parameters - shared throughout the organization - and which are in line with the corporate ERM process fundamentals.

The questions of which specific reference methodology for cyber risk management should be chosen and of what should be the level of data detail for describing the risk elements under analysis may then be made by the organization, by taking into account both the current level of risk management corporate maturity and the level of complexity of the context under analysis.

While for the choice of what should be the applied methodology, as anticipated, many sources of international prestige are available to draw from, for the choice of what should be the level of detail of data, an extremely well-weighted analysis must be done, as the specificities of the business context should be taken into account.

The choice of what should be the minimum element of risk evaluation - namely of the level of detail of data for risk analysis (risk data granularity) - must be such as to allow for coherent evaluation of both elements belonging to the IT or the OT context: this ensures that both IT and OT elements are analyzed with a similar level of detail, which thus allows for IT and OT perimeter risk assessment results comparison, joint representation and joint reporting to the CCR and\or the BOD.

Generally speaking, it would be reasonable to think that risk evaluation should be done on the basis of the basic element of all digital systems, be it IT or OT: the single data element.

However, carrying out risk assessments on each data element not only turn out to be complex (as it implies the need to census all data and all "routes" that such data follow, both inside and outside of its supporting infrastructure), but it would give start to a too high number of assessments for any organization to bear also.

It is therefore necessary to identify elements of adequate dimension level for risk analysis; purely by way of example, IT applications and systems related to a specific sub-area of the production process within OT area (these are described in IEC62443 language) may be chosen as the basic elements on which to perform cyber risk analysis activities.

In the case of the electric context, the division of the perimeter in zones is perfectly reasonable, because of the extreme heterogeneity of the context itself: for example, within Generation, the generation sources carry distinct characteristics and peculiarities; within Transmission, a geographically extended perimeter carries communication channels of considerable length; finally, within Distribution, the territory carries a need of great capillarity, especially localized in some areas only.

Risk assessments must be carried out periodically for each identified target and responsibility for the performance of such assessment activities must be borne by the organization's function which centrally

carries cyber security responsibilities at company level (typically, the CISO, as Risk Owner of cyber topics).

In order to correctly quantify a risk, the fundamental parameters to be determined are two: impact and probability. Risk is, in fact, defined through the formula R = I x P (where R, I and P stand for, respectively, Risk, Impact and Probability).

The topic of impact assessment has already been discussed extensively in the chapter on business continuity.

On the contrary, for the probability topic, it is appropriate to make the following considerations related to the specific case of cyber context:

- Risk probability is calculated only when the occurrence of an adverse cyber event is considered. This is due to the fact that a failed cyber attack attempt is not considered as a risk because a failed cyber attack would carry no impact
- Risk probability is directly correlated to the probability of occurrence of a cyber event and to the probability of presence of vulnerabilities within the system.
  The risk probability topic is extremely complex in cyber context due to the fact that - on one hand - there is not enough historical data describing cyber events to be used for the creation of ad-hoc mathematical predictive models that would thus be able to reliably identify frequency of occurrence of such events; on the other hand - each single device connected to a network may be a possible target of cyber attacks, carried out by a very large number of different threats;
- Risk probability is generally lower the lower the probability of vulnerabilities; furthermore, probability of vulnerabilities is correlated to probability of threats, but not all existing threats may exploit all existing vulnerabilities.

To reduce vulnerabilities it is necessary to implement countermeasures, which can “follow” the controls defined by international standards, such as, for example, the IEC 62443 and the IEC 62351 standards for the OT context. Such controls, in fact, guide the choice of which countermeasures need to be implemented within specific areas of cyber security topic (such as Identity and Access Management, Event detection and Incident Response, etc.). Controls must in any case be fine-tuned within the organization, according to which are the specific threats relevant to the organization itself.

In order to define risk probability and collect information on risk impact, it is thus recommended that cyber risk Risk Owner interacts with managers responsible of IT and/or OT Security as well as with managers responsible of Business Continuity, in order to collect and share all appropriate and adequate information on impacts.

A risk management model that addresses threats must take into account the variability over time of types of existing threats and\or of characteristics of existing threats themselves; this implies that organization's cyber risks need to be dynamically updated also.

A process which includes dynamic threat analysis within its risk assessment model may be structured in the five steps described below:

- Source Monitoring step: Within the present step, activities aim to "monitor" information coming from "additional" sources, such as sources related to Cyber Threat Intelligence, Regulatory Authorities and International Organizations; such "additional" sources set needs to be defined before the beginning of the present step. Methods for source monitoring and frequency of source monitoring itself depend on what is the object type for which the source under analysis provides information on (e.g. a source related to Cyber Threat Intelligence would produce information on a daily basis, while a source related to a Regulatory Authority would update its information only after months). It is important to consider that world-wide electric operators' context has seen cyber risk management topic be on the cutting edge for years (NERC CIP regulations for North America is a clear example); therefore "maturity" level of - and reliability level of- available Cyber Threat Intelligence sources may now be considered rather high.
- Identification step: Within the present step, on the basis of the information so far obtained, aim to identify the threats to be of interest for analysis; such identification must rely on previously defined and validated threat profiles and\or following the occurrence of a specific event or the increase of a cyber threat trend.

Examples of such events or cyber threat trend increase may be:
○ electricity sector Ransomware Campaign event
○ a trend increase in malware of predictive maintenance sensors (e.g. of sensors used within the IIoT sector)

- Characterization step: Within the present following step, activities aim to identify what are the characteristics of cyber events in order to define its category. Classification of a cyber events to a specific category is done on the basis of models that take into account what are the specificities of its characteristics. For example, a threat may be characterized by such attributes which may be correctly modelled through a threat model carrying variables providing information on:

  ○ Threat Entity Goal Orientation (i.e. actors, motivation, interest)
  ○ Threat Entity Capabilities (i.e. resources, skills)
  ○ Threat Entity Modus Operandi

- Correlation step: Within the present step, activities aim to correlate the cyber events' characteristics with the risk assessment elements and criteria. Such correlation should be based on the use of mapping tables / mapping models and data updating logics. Threat characteristics are then cross-checked with the criteria which have been used for threat probability calculation during static risk assessment; therefore, they are cross-checked also with the criteria which have been applied for choosing countermeasures: both already implemented countermeasures and those which still need to implemented in the future are considered.
- Risk updating step: Within the present final step, activities aim to update risk level values and report on their variation over time. A probability threat variation determines a recalculation and eventual updating of risk level value: should this imply a risk level value variation, it shall be necessary for the organization to undertake additional actions for risk treatment.

Regarding sources management and source monitoring activities, it should be pointed out that it is difficult to appoint the responsibility of such activities to specific Risk IT or OT Owners. For this reason, and in such cases, the CERT may be appointed the task of supporting and guiding the dynamic data management process activities, by collecting and analyzing data coming from Cyber Threat Intelligence sources with the aim to identify threat events which carry impacts on risk assessment elements; at the same time, the CERT may carry the role of properly engaging risk managers.

5. Computer Emergency Readiness Team (CERT)

Within the electricity sector context it is increasingly important to define an integrated approach for preventing and managing cyber security incidents. Such approach should aim to improve "cyber readiness", namely, the ability to proactively prevent cyber threats, in such a way as to avoid negative -as far as possible - significant impacts on employees, assets, issued services and, generally speaking, on company competitiveness and reputation.

The CERT, to be considered mainly as a "Cyber Emergency Readiness Team", is the organization structure that carries the mandate of implementing such approach and, at the same time, of protecting organization's own "Constituency" by guaranteeing an adequate level of service issuing.

Organization "Constituency"-within the energy context- must not be understood as organization's employees only, but as organization's assets -included production facilities, distribution grids, buildings - and all sources which contribute to company service provisioning too; particular attention should be payed to organization's critical infrastructures and to those which issue essential services.

The CERT functional model consists of several key components that are supported by a broad set of tools, services and features, which, working together, enable CERT to fulfill its mission and achieve its goals.

Among the important aspects of a CERT's mission, we may certainly highlight the following non-exhaustive list:

- To monitor cyber incidents' occurrence, thus contributing to enhace continuous improvement process of IT security controls and countermeasures management
- To analyze cyber incidents in order to mitigate their impact effects and to reduce and\or limit their future occurrence

- To coordinate cyber incidents' response activities, by involving both internal company stakeholders and external counterparts (e.g. national CERTs)
- To issue reports for company functions and management
- To enhace organization culture on security incident management, by organizing and deploying ad-hoc simulation tests and exercises within personnel organization

CERT's goals should be linked not only to more "technical" aspects - such as may be the reducing of the number of cyber incidents which may occur - but to more "business" aspects also - such as may be the reduction of cyber incidents' impacts on company assets, services, reputation and competitiveness.

Such goals may be achieved by:

- Management, coordination, support and monitoring of both cyber security incidents and of cyber security prevention and response processes' maturity level
- Creation and reinforcement of a "trusted community" within the company, which involves significant external counterparts;
- Start-up of a "communication channel" between CERT and the corporate Communication Function, in order to manage organization's communication of incidents versus both internal and external media
- Monitoring of "recovery" activities, which are needed following security incidents' occurrence
- Gathering and sharing of information related to which are potential company threats; particular focus should be given to gathering and sharing of information related to which are external threats able to exploit organization's own internal weaknesses.

The following processes are included in CERT's perimeter:

- **Cyber Incident Response process:** This is the key process for prevention of, detection of, responding to and recovering from cyber security incidents. Such process must be carried out with a systematic and structured approach, thus implying constant communication of information between internal and external stakeholders; it must include, at the least, the steps listed below:
  - "Preparedness and Prevention"
  - "Detection"
  - "Analysis"
  - "Response"
  - "Recovery"
- **Threat Monitoring process:** This is the process for collecting and managing of "privileged" information related to cyber threats, to cyber threats' "actors" and/or "carriers"; it is the key process for effective and efficient prevention of and response to security incidents, should the information gathered and managed within the present process be correctly "translated" into effective and applicable actions for avoiding, mitigating or handling of potential security incidents.
- **Information Sharing process:** This is the process which aims to implement "trusted" communication activities between all different actors involved; such activities should be based on principles of "need-to-share" and "need-to-know".
- **Impact Simulation process:** CERT deploys simulations of threat impact, on the basis of threat and vulnerabilities withheld by CERT itself, with the aim to understand prehemptively the best defense strategy to be applied
- **Training and Testing process:** Periodic ad-hoc exercises are deployed for training cyber security staff (e.g. Cyber War Gaming and Red Teaming) and for testing efficiency and effectiveness of the existing response procedures. Results of such activities are measured in order to evaluate effectiveness level of prevention, response and recovery measures put in place.

6. Implementing countermeasures in the critical electrical infrastructures context

Critical Infrastructures related to electrical systems may be classified hierarchically according to criteria of dimension and complexity:

- Large classical-technology thermal generation plants
- Distributed hydroelectric generation systems
- Distributed renewable generation (DER)
- Energy transmission and distribution systems (which involve thousands of primary substations and hundreds of thousands of secondary substations).

Tele-controlled systems and distributed systems make use of telecommunications infrastructures and protocols, therefore they are exposed to all risks which are related to such context; however, nowadays not even large plants may be operated on independently, without telecommunication: system security, networks and protocols are, in fact, essential elements of plant operation.

Possible threats may, furthermore, be conveyed also through "not-connected-to the network " means such as through removable media or devices returned after maintenance. Access to systems by external personnel may also represent a further threat source.

It is necessary to take into account the different needs of the following three contexts: a highly centralized one (related to thermal power plants), a highly distributed one (related to hydroelectric plants which are all remote-controlled), and finally the renewable generation plants' context. It is therefore necessary to develop appropriate and ad-hoc strategies for each of these three single contexts.

Within the context of industrial systems, systems carry a life cycle much longer than that of computer systems. It is therefore necessary for the organization to work with manufacturers in order to make them include cyber safety measures within their products from the outset, as well as to make them apply appropriate cyber security countermeasures to older already existing information systems, thus ensuring their predicted life cycle duration.

Tele-controlled network of distribution grids area presents us with an even more complex context, as not only are hundreds of thousands of primary and secondary substations involved, but the electronic counter infrastructure is even more detailed also. As we approach the "leaves" of such system, the order of magnitude of objects of analysis grows, and - with it - the need to identify a specific strategy for handling cyber safety.

It is therefore necessary not only to operate as far as possible with tools currently available but also support development of innovative solutions, for example support regulatory bodies develop more secure versions of remote control and automation protocols.

The fight against cybersecurity threats is deployed through the adoption of appropriate countermeasures, technically called "controls". For "control", therefore, we intend an action -carrying either an organizational and\or technical nature - which is able to reduce the risk level associated to a threat resulting an effective attack with impacts.

Security controls are subject to continuous evolution and classification through the development of numerous international standards. There are therefore some "security frameworks" that group controls on the basis of a set of categories and application areas.

The reference framework adopted within the present guideline is the "Framework for improving Critical Infrastructures Cybersecurity V1.0/NIST/February 12 – 2014", together with its updated revision V.1.1 .

NIST framework is based on a "risk based" approach, namely, an approach which puts in relation priority and level of adoption of security controls with criteria of risk analysis; the framework is structured in the following elements:

- **Core Framework element**: This is a set of cyber security activities, desired results and references, applicable to critical infrastructures. Security controls which are described in the Core Framework are classified on the basis of five levels (or scopes) , which concur to realize cyber security, named: Identify, Protect, Detect, Respond, Recover.
  Each level name intuitively suggests us already what are the control types analyzed within each level itself; furthermore, the order with which such levels are listed is just as significant too.

Control types analyzed within Core Framework are described in such a way as to be at first glance of general level, but - in any case - they refer also to specific application standards for different contexts of Critical Infrastructures (e.g. for the electricity system).

- **Framework Implementation Tiers element:** This element allows for the definition of a method by which to assess maturity level of deployment of Core Framework controls within the organization under analysis; maturity levels of deployment are from Tier 1 to Tier 4.
- **Framework Profile element:** This element describes the security profile that the organization has decided to implement, once it has - on the basis of risk analysis - evaluated its business needs and related business continuity requirements. Generally speaking, it may be possible that a single organization may carry more than one such "profile", depending on how many different, specific contexts are within the organization itself. Furthermore, profiles may be classified as "current" or "goal" profiles; such classification allows for the identification and tracking of cybersecurity posture improvement path. In general, each profile includes a set of controls, which carry a related maturity level.

Bibliography

- IEC 62351 – "Power Systems Management and Associated Information Exchange – Data and Communications Security"
- IEC 62443 – "Security for industrial automation and control systems"
- 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security
- CYBERSECURITY, Critical Infrastructure. Framework for Improving Critical Infrastructure Cybersecurity. 2014.
    - HILDICK-SMITH, Andrew. Security for critical infrastructure scada systems. SANS Reading Room, GSEC Practical Assignment, Version, 2005, 1: 498-506.
- FORCE, JOINT TASK; INITIATIVE, TRANSFORMATION. Security and privacy controls for federal information systems and organizations. NIST Special Publication, 2013, 800: 53.
- STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, 2011, 800.82: 16-16.
- PCI DSS Standard.
- ISO/IEC 27001:2013 Standard.
- ISO/IEC 27002:2013 Standard.
- ISO/IEC 27005:2011 Standard.
- Business Continuity and Crisis Management:
    - ISO 22301:2012 Societal security -- Business continuity management systems – Requirements
    - ISO 22313:2012 Societal security -- Business continuity management systems -- Guidance
    - ISO/TS 22317:2015 Societal security -- Business continuity management systems -- Guidelines for business impact analysis (BIA)
    - ISO/TS 22318:2015 Societal security -- Business continuity management systems -- Guidelines for supply chain continuity
    - BS 11200:2014 Crisis Management. Guidance and good practice
    - "The BCI Good Practice Guidelines – 2018" issued by the Business Continuity Institute
    - "BCI How To Guides" issued by The Business Continuity Institute
- Risk Management:
    - ISO 31000:2009 Risk management – Principles and guidelines
    - ISO/IEC 31010:2009 Risk management -- Risk assessment techniques
- Organizational Resilience:
    - ISO 22316:2017 Security and resilience -- Organizational resilience -- Principles and attributes

Reference websites

- Homeland Security - Cyber Security Publications: https://www.dhs.gov/cybersecurity-publications
- Business Continuity and Crisis Management:
    - The Business Continuity Institute: www.thebci.org
    - Disaster Recovery Institute: www.drii.org
    - Continuity Central: http://www.continuitycentral.com/

- Risk Management:
  - The Institute of Risk Management: https://www.theirm.org/
  - Committee of Sponsoring Organizations (COSO) of the Treadway Commission: https://www.coso.org/
- Organizational Resilience
  - Horizon Scan Report, issued by the Business Continuity Institute (BCI): http://www.thebci.org/index.php/download-the-horizon-scan-2017
  - Cyber Resilience Report, issued by the Business Continuity Institute (BCI): http://www.thebci.org/index.php/obtain-the-cyber-resilience-report-2016

Main documental sources

- NIS Directive, The Directive on security of network and information systems, adopted by the European Parliament on 6 July 2016 Directive (EU) 2016/1148;
- European General Data Protection Regulation (GDPR);
- NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) Plan
- CONSEJO NACIONAL DE OPERACIÓN – CNO - Colombia Acuerdo 788 dated 03/09/2015;
- Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas " from Spain Government – dated 28/04/2011;
- Ley 5/2014, de 4 de abril, de Seguridad Privada, regulate the performance and provision of private security activities and services;
- National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cyber Security", version 1.0 February 2014;
- Research Center of Cyber Intelligence and Information Security (Sapienza Università di Roma) e Laboratorio Nazionale CINI di Cyber Security (Consorzio Interuniversitario Nazionale per l'Informatica), "2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security", versione 1.0 Febbraio 2016.

Main recent web documental sources 2017/2018

- Council of European Energy Regulators (CEER): https://www.ceer.eu
- EURELECTRIC: http://www.eurelectric.org
- European Network for Cyber Security (ENCS): https://encs.eu
- European Network of Transmission System Operators for Electricity (ENTSO-E): https://www.entsoe.eu
- EPRI: https://www.epri.com
- SEPA: Smart Electric Power Alliance -- https://sepapower.org
- IEEE - Cybersecurity of Energy Delivery Systems: http://www.ieee-ecce.org
- IEC - International Electrotechnical Commission: http://www.gridstandardsmap.com/
- Interoperability Strategic Vision:

  https://gridmod.labworks.org/sites/default/files/resources/InteropStrategicVision2017-04-11.pdf
- EU Commission Task Force for Smart Grids:

  https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force.