**Pestana Maria**

**Messias Ricardo**
*EDP Distribuição (EDP Group), Lisbon, Portugal*

# Identification of National Critical Infrastructures - DSO comply with European Council Directive 2008/114/EC

## Keywords

critical infrastructure, threats, vulnerabilities

## Abstract

The subject addressed in the paper is about the identification of National Critical Infrastructures (NCI). The focus is the result of the responsibilities of EDP Distribuição, the Portuguese mainland Electrical Distribution System Operator (DSO) serving over 6 million customers in a regulated business with clearly defined tasks, to comply with the transposition to the Portuguese legislation of the European Council Directive 2008/114/EC. Having EDP Distribuição under their responsibility several assets and systems which are essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, the ones considered national critical were selected, from a set of more than 400 main premises. Has been identified their major threats and vulnerabilities, which resulted in emergency response procedures named "Operator Security Plan".

## 1. Introduction

EDP Distribuição is the holder of the concession to operate the Distribution Electric Power Network in High Voltage (HV) and Medium Voltage (MV), and holds the municipal concessions for the distribution of electricity in Low Voltage (LV).
As result from Distribution System Operator (DSO) responsibilities it was required its compliance with the Portuguese legal requirement (decree-law no. º 62/2011 of May 9th), which was transpose from the European Directive 2008/114/EC. This document establishes procedures for identifying and protecting infrastructure essential to health, safety and welfare of society in economic and social sectors of energy and transport.
It was required by the National Authorities (1) the identification of the National Critical Infrastructures (NCI) under EDP Distribuição responsibility, (2) the safety and security assessment and the need of improvements and (3) the submission of emergency response procedures, named "Operator Security Plan" (OSP), for each of those infrastructures.
As critical infrastructure was considered an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and that its disruption or destruction would have a significant impact.

## 2. Identification of the NCI

### 2.1. Assumptions

The EDP Distribuição organization includes four types of units; Operational, Commercial, Technical and Management support. The field operations are organized in six grid departments and one maintenance departments distributed throughout the country being solely responsible for the interventions in 404 HV/MV substations, 63.223 MV/LV substation and 220.400km of cables (*Table 1*).

### 2.2. Critical Infrastructures

Given the large number of assets managed by EDP Distribuição, there was a need for prioritization of those assets, especially given the scope of this Directive.
Thus, facilities were identified taking into consideration the country priority services, namely substations feeding a significant number of customers whose activities guarantee a public service

such as airports, hospitals, television, radios, water pumping stations in a total of twenty-six substations.
However, it wouldn't make sense, indicate these equipment without to designate other which support the service played by substations, and that, without them, the service could be compromised, such as 2 Dispatch Centres, that enable the supervision and operation of the HV, MV and LV grid.
Besides, the twenty-six HV/MV Substations and two dispatch center of EDP Distribuição, was also considered other facilities managed by another company within the EDP Group, namely the Contact Center sites.
The Contact Center has two sites, located in different regions. This facility performs the management of customer contacts, enabling the consumer's interaction with EDP, routing the data gather in those contacts reporting grid failures to the Dispatch, through IT systems.
In addition to this installation, the EDP Distribution activity is supported by a in complex IT systems and applications, which are of vital importance to the company and, was also considered the main Data center, operated outside the EDP Group.
Based on these assumptions, which were made by the company, there were rated thirty-one national critical infrastructure, and wherein two of them were facilities not belonging directly to EDP Distribuição, for purposes described above, but still are essential for the activity of the Distribution System Operator (DSO).
The four different types of infrastructure are summarized in *Table 2*.

## 3. Vulnerabilities and threats for each NCI

One of the requirements of the 'Operator Security Plan' is the identification of the vulnerabilities and threats associated within the infrastructure. This identification enables to raise the risks, given that when an existing threat can explore an existing vulnerability the asset is at risk.
By definition, we have, *Threats* as any events or actions, not yet implemented but likely to be played by an agent with intent and ability to execute, contrary to the achievement of one or more objectives of any entity (from a state or an international public organization, to communities or individuals) through material or moral damage.
*Vulnerability* is any weakness or fragility, intrinsic or induced in a given asset (infrastructure, in the broad sense, and everything containing) or those responsible for their protection, which can be exploited by threat to inflict harm on it. That is, if a certain weakness is not likely to be exploited by the threat, it does not get to be a vulnerability.

*Table 1.* Grid Departments - Field organization

| | **EDP Distribuição - Grid Departments** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Indicators** | **Norte Area** | **Porto Area** | **Mondego Area** | **Tejo Area** | **Lisboa Area** | **Sul Area** | **Total** |
| km2 (x 1.000) | 17.3 | 3.6 | 21.4 | 17.6 | 3.0 | 26.2 | **89.1** |
| km grid (x 10.000) | 47.1 | 28.6 | 43.5 | 36.5 | 30.4 | 34.3 | **220.4** |
| MV/LV Substations | 12 152 | 9 612 | 11 286 | 11 299 | 9 496 | 9 378 | **63 223** |
| HV/MV Substations | 58 | 57 | 61 | 76 | 84 | 68 | **404** |
| Customers (x 1.000) | 1045 | 1 109 | 862 | 801 | 1 665 | 669 | **3377** |
| Municipal | 59 | 27 | 69 | 57 | 18 | 48 | **278** |
| FTE | 526 | 461 | 315 | 343 | 475 | 345 | **2465** |

*Table 2.* NCI identified

| **National Critical Infrastructures** | **N. º** | **Direct responsibility** |
|---|---|---|
| HV/MV Substations | 26 | EDP Distribuição |
| Dispatch Centre | 2 | EDP Distribuição |
| Contact Centre | 2 | EDP Group |
| Data Center | 1 | Outside EDP Group |

*Table 3.* Vulnerabilities list

| **Vulnerabilities** | | | |
|---|---|---|---|
| v1 | absence of information redundancy | v12 | inadequate capacity management |
| v2 | allocation of inadequate permissions to users | v13 | inadequate cryptographic keys management |
| v3 | anti-virus outdated for protection against malicious code | v14 | Inadequate human resources management (internal and external) |
| v4 | availability of technical resources | v15 | Inadequate technical resources management |
| v5 | bad work environment | v16 | inadequate surveillance facilities |
| v6 | change control inappropriate | v17 | inadequate monitoring systems |
| v7 | copies uncontrolled information | v18 | inadequate knowledge passage |
| v8 | destruction storage means without deleting data | v19 | ineffective lifecycle features management |
| v9 | failure / lack of access control mechanism | v20 | uncontrolled Internet downloads |
| v10 | failure in the access management | v21 | lack of alternative facilities |
| v11 | inadequate maintenance facilities | v22 | lack of backups |

This study was developed internally by a work team that included experts in the different areas of activity involving several departments consisting of operational ones (Maintenance and Dispatch) and support departments (Automation & Remote Control, Information Systems, Safety). All were crucial and even essential for the proper development of the work presented herein.
In the first phase, there have been identified twenty-two vulnerabilities, which could affect the four types of analyzed facilities (see *Table 3*).
Thus as a result of this survey, we have the information about how many and which threats can be exploited by the vulnerabilities.
Instead of simply crossing the path by which the vulnerability could be exploited, with the 4 defined infrastructure types (Substations, Dispatch, Contact Centre and Data Centre).

*Table 4***.** Threats list

| **Threat** | | | |
|---|---|---|---|
| t1 | accidental change data of the information system | t24 | malicious code |
| t2 | application errors | t25 | misappropriation |
| t3 | bomb threat | t26 | misuse of audit tools |
| t4 | breach of contractual relations | t27 | misuse of information systems |
| t5 | breaking of law / regulatory | t28 | pandemic |
| t6 | Damage caused by third parties activities | t29 | pollution |
| t7 | damage during the penetration test | t30 | power supply interruption |
| t8 | records destruction | t31 | social engineering |
| t9 | media deterioration | t32 | strike |
| t10 | disclosure of passwords | t33 | terrorist attacks |
| t11 | failure of communication links | t34 | theft |
| t12 | equipment failure | t35 | thunder / lightning |
| t13 | utilities failure (water, electricity, gas, ..) | t36 | unauthorized information system access |
| t14 | falsification of records | t37 | unauthorized network access |
| t15 | fire | t38 | unauthorized changes of records |
| t16 | flood | t39 | unauthorized software installation |
| t17 | fraud / Sabotage | t40 | unauthorized or untested code use |
| t18 | human error | t41 | unauthorized physical access |
| t19 | industrial espionage | t42 | unauthorized use of licensed materials |
| t20 | information leakage | t43 | unauthorized software use |
| t21 | Interception Information | t44 | unavailability of persons |
| t22 | loss of support services (PES) | t45 | user identity concealment |
| t23 | maintenance errors | t46 | vandalism |

*Table 5***.** Likelihood

| **Likelihood** (to occur Threat) | **Description** |
|---|---|
| Very Likely | There is occurrence of records on a regular basis, at least once every 6 months. |
| Likely | There are some instances of records, typically associated to a time between 6 months to 24 months. |
| Unlikely | There are some instances of records, typically associated to a time between 24 months to 60 months. |
| Very Unlikely | Is not expected to happen |

*Table 6***.** Impact

| **Impact** | **Description** |
|---|---|
| Very Severe | Destruction / unresponsive of the critical infrastructure element. |
| Severe | The responsive element is engaged between 50% and 75%. |
| Moderate | The responsive element is engaged between 10% and 50%. |
| Slight | The responsive element is committed to 10%. |

It was considered that the infrastructure in question should be viewed in an integrated manner considering four main pillars: people, installation, communications and systems.
We now have a more complete view of each facility, knowing how each vulnerability can be exploited by a number of threats, which could affect the infrastructure in one or more pillars.

## 4. Risk assessment Methodology

Considering the analysis indicated above there was performed a risk assessment per facility taking into account the four pillars (people, installation, communications and systems).
For this, we used the risk assessment methodology, wherein the risk assessment analysis in the particular vector of the infrastructure is equal to the product of the probability of threat (*Table 4*) by the impact severity (*Table 5*) if the threat to materialize, equation (1).

$$Risk = Likelihood \times Impact \tag{1}$$

For the determination of the risk, that results from the evaluation of the probability of materializing threat(s) on an infrastructure and the consequences, was use a qualitative analysis performed as indicated in the risk matrix, *Table 6*, being the risk rating described in *Table 6*.

*Table 7.* Risk Matrix

| **Likelihood** (to occur Threat) | **Impact** | | | |
|---|---|---|---|---|
| | Slight | Moderate | Severe | Very Severe |
| Very Likely | High | Very High | Very High | Very High |
| Likely | Moderate | High | High | Very High |
| Unlikely | Acceptable | Moderate | High | High |
| Very Unlikely | Acceptable | Acceptable | Moderate | Moderate |

*Table 8.* Risk Description

| **Risk** | **Description** |
|---|---|
| Very High | The element should not be used until control measures are introduced to reduce the risk. |
| High | The risk reduction measures must be implemented to urgently, within a set period of time and you may need to apply specific control measures until the situation is corrected. |
| Moderate | A risk reassessment should be made to establish additional control measures. Risk control measures should be implemented within a set period of time and its effectiveness should be controlled. |
| Acceptable | May be required additional control measures. You must ensure that the existing control conditions are applied and maintained. |

The risk assessment methodology was applied to each distinct pillars (people, facilities, systems and communications).

## 5. Operator Security Plan (OSP)

Using the detailed analysis described above, where the infrastructure was analysed considering the safety and security aspects, thirty-one OSP were prepared following the structure defined by the National Civil Protection Authority (ANPC) and the Office Internal Security Coordinator (GSI).
It was decided internally that these plans take into account the specificities of infrastructures which are strategic ones that establish communication and coordination between the different security plans and other existing documents within the company. This way we managed to potentiate, the internal documents that are already developed by Organizational Units and Business Units in this area.

## 6. Results

As result, the main vulnerabilities were identified in a comprehensive manner in each infrastructure under review, the main vulnerabilities which were found to be inadequate monitoring systems and inadequate management of human resources (internal and external), see *Figure 1*.

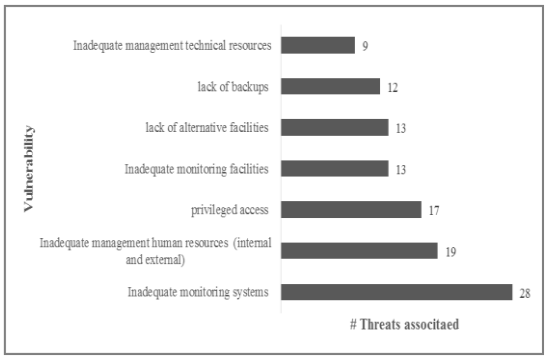


*Figure 1***.** Main vulnerabilities

However, the threat that most often appears, related to the vulnerability of our facilities, is theft, unauthorized access to the information system, damage caused by third parties and sabotage and fraud, see *Figure 2*.

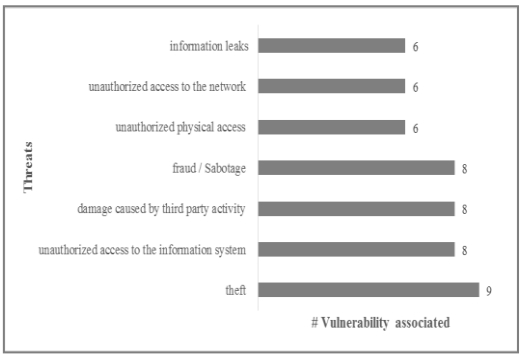


*Figure 2***.** Threat vulnerabilities

This analysis reflects the fact that most of the facilities are isolated and dispersed throughout the territory and that, on the other hand, given the size of the company, there is a large component of outsourcing working directly on the premises.
In addition to the thirty-one OPS, which were structured by the template suggested by national authorities, were also developed internally by the working group, plus two more types of documents that support the plans:

- *The specific impact assessment report* for each infrastructure indicating the main vulnerabilities and threats associated, risk analysis for the four pillars (people, facilities, systems and communications), and its action plan with mitigation measures for the risks identified, which implementation is assigned to the responsible for each infrastructure and;
- *The Communication model and coordination* within the OSP, given that these

infrastructures require special monitoring. This model creates a response structure and coordination when an incident occurs in these facilities. Stating the decree-law to the need of a "Security Liaison Officer", which connects with the national authorities, this model establishes the relationship between the "Security Liaison Officer" and the company's organizational structure.

## 7. Conclusions

Through this article, it is emphasized that all infrastructure should be analyzed as a whole, considering the different areas. Each infrastructure does not only include systems or communications, but is also an installation with its specific physical structure and its specific people safety problematic.

The multidisciplinary team was undoubtedly a major contribution to a correct characterization of infrastructure, enabling a more concrete, realistic and integrated analysis of the different views of experts on each infrastructure.

The preparation and submission of the Operator Security Plans internally enable and put in place a set of recommendations and action plans which the result are taken from the risk assessment, in order to minimize the identified infrastructure risk.

At a later stage, has been identified, the need to develop a set of exercises and tests that validate the interconnection, communication and the cooperation between both critical infrastructures and national authorities, that will eventually enable to achieve continual improvement and a higher degree of organizational and societal resiliency.

## References

[1] Almeida, A. (2011). *A Multi-criteria Methodology for the Identification e Ranking of Critical Infrastructures*.

[2] Commission Staff Working Document on a new approach to the European Program for Critical Infrastructure protection Making European Critical Infrastructures more secure, SWD (2013) 318 final.

[3] Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

[4] Decree-law no. º 62/2011 of 9 May 2011. Daily Republic n. º89, Series I, 2011-05-09.

[5] International standard, "Societal security - Business continuity management systems - Guidance", ISO 22313:2012 (E), First edition 2012-12-15

[6] International standard, "Societal security - Business continuity management systems - Requirements", ISO 22301:2012 (E), Corrected edition 2012-06-15

[7] ISO 27001/ISO 22301 Knowledge base: http://www.infosecpedia.info/threats-vulnerabilities.

[8] Rossella M. (2014). *Methodologies for the identification of Critical Information Infrastructure assets and services.* European Union Agency for Network and Information Security

[9] Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*