5.2 Criticality assessment:

5.2.1) Critical infrastructure and asset list:

A criticality assessment is a systematic work to identify and evaluate important or critical assets, and the impact of an attack. It helps specialists calculate the relative importance or value of assets and divide resources up amongst the most critical assets.

It is essential to determine the results of loss or damage to important systems and assets (including loss of time), as well as the effort and control and management functions needed to solve the problem. For cyber assets, some of these damages could be loss in confidentiality, integrity or availability. Measuring criticality determines the importance of the asset. For example, damage to essential assets or loss of symbolic assets would denote a big importance.

Assessing criticality can involve some subjectivity. The energy sector is inherently vulnerable and should be considered as critical infrastructure and key assets.

To classify assets, it is necessary to evaluate if a loss of confidentiality, integrity or availability caused by cyber-attacks could reduce the security of the electric system. A useful classification could be based on the following:

- Level 3: Assets associated with safety, which should be protected from malfunction of assets of minor importance. Redundant security controls and other mitigating measures should be applied. These assets can supply information to assets in lower levels, but not receive information from them.
- Level 2: Assets which are not directly related to security, but may cause big damages or are connected to assets at level 3. These assets should not receive information from lower levels, but they can receive it from level 3 or supply it to level 1. Security controls and measures to reduce vulnerabilities can be applied.
- Level 1: Independent assets or systems which cannot impact on the safety and are not connected to any network. The need for security controls and measures to reduce vulnerabilities depends on the impact of cyber-attacks on the asset itself.

In accordance with NIPP assessment, Internet can be used as a key source of information, available for all sectors and comprising domestic and international assets within the Information and Communication technologies. D.H.S. works with the S.S.A.s and C.I.K.R. partners to develop methodologies to identify cyber assets, systems and networks that can have consequences if they are destroyed, exploited or incapacitated. In this way, the dependence of the sector on cyber assets can be assessed. If a valid cyber identification methodology has already been developed by a sector, the N.I.P.P. ensures that it follows the N.I.P.P. risk management framework.