CRITICALITY ANALYSIS FOR NETWORK UTILITIES ASSET MANAGEMENT

Juan F. Gómez Fernández, Pablo Martínez-Galán Fernández,
Antonio J. Guillén López, Adolfo Crespo Márquez

Universidad de Sevilla
Department of Industrial Management, School of Engineering,
Camino de los Descubrimientos s/n. 41092 Seville, Spain.
juan.gomez@iies.es, ajguillen@us.es, adolfo@us.es

Corresponding author: Antonio J. Guillén López, ajguillen@us.es

ACKNOWLEDGEMENTS

This research work was performed within the context of Sustain Owner ('Sustainable Design and Management of Industrial Assets through Total Value and Cost of Ownership'), a project sponsored by the EU Framework Program Horizon 2020, MSCA-RISE-2014: Marie Skłodowska-Curie Research and Innovation Staff Exchange (RISE) (grant agreement number 645733 — Sustain-Owner — H2020-MSCA-RISE-2014); and the project "DESARROLLO DE PROCESOS AVANZADOS DE OPERACION Y MANTENIMIENTO SOBRE SISTEMAS CIBERO FISICOS (CPS) EN EL AMBITO DE LA INDUSTRIA 4.0", Ministerio de Economía y Competitividad del Gobierno de España, Programa Estatal de I+D+i Orientado a los Retos de la Sociedad.DPI2015-70842-R, financed bycon FEDER (Fondo Europeo de Desarrollo Regional)

ABSTRACT

This paper describes the design and the implementation of a process of strategic assets criticality analysis for companies within the sector of Distribution Network Services Providers, also named Network Utilities. Assets criticality analysis is based on business value drivers/factors and it is a risk-based evaluation of assets, considering potential impacts of their failures on value-provided sustainability. In this sense, the proposed methodology is aligned with ISO 55000 family of standards approach, and therefore it must be understood as practical asset management tool. A hierarchy of assets ranked according with value and risk will come out of this process, which represents a fundamental result serving as input of the subsequent steps of the asset management process, including maintenance and renewal/reinvestments decisions. Specific attention is paid to particular network utilities issues, characterizing assets in these companies, and the services that they provide (topology influence, reputational impact, operational losses, etc.). All these aspects are discussed in the paper, along with the development of the criticality analysis process.

Keywords: Network utilities, Asset Criticality, Asset Management, Risk-value Assessment Maintenance Optimization, Operational Reliability, ISO 55.000

1 INTRODUCTION

The process of “maintenance strategic management” [1] in a company coordinates and integrates all fundamental maintenance management activities in order to achieve the department objectives[2,3], aligned with the company goals. To ensure proper maintenance department focus and to provide consistency to the maintenance actions, this process has to standardize, coordinate and control activities. This is done by producing effective and efficient actions plans[4]. A fundamental part of this process is to determine priorities for the execution of assets maintenance activities, i.e. what assets should have priority within a maintenance management program. Based on predefined objectives and through proper action plans, the “strategy management process” should determine concrete policies and procedures to focus the efforts on critical issues.

On the other hand, in line with the ISO 55000 series of standards (and before with PAS 55[7,17]), companies are increasingly concerned about the value of their assets. Understanding the value generated by an assets is a key pillar of these standards, and asset’s value drivers will be not only technical aspects, but also other aspects[37] such as financial, environmental and social results, quality of service, etc. In this sense, and in order to take suitable decisions, the strategic management process we are referring to must assess and manage the value generated by the assets[38].

The purpose of any asset is to provide value to the organization and its stakeholders[7]. In asset management, the concept of value considers all those aspects (obtained or expected to be obtained from an asset) that provide any kind of benefit (expressed in specific terms) to the organization. The definition of both, asset and value, are complementary to each other. Indeed, asset and value are two concepts closely related, and it can be said that there is no sense of one without the other.

Although, the search of this convergence is a challenge in case of Network Utilities, that relies on network infrastructures whereby services are directly provided by physical interconnection, to customers in their homes, dwellings or working places. This infrastructure is often organized and composed of high number and different types of assets arranged and interrelated in a hierarchical form, replicated and geographically dispersed and in non-optimal environmental conditions by distribution areas or jurisdictions[19]. Due to the numerous deployed assets over a wide distance between generation and customer, in order to conduct the services, the connections among assets are harmonized according to the customer demanded capacity (based on levels of capacity aggregation). Consequently, in these companies, the “asset” has not to be treated in an isolated way[39,40], the variety of possible interconnections among them could materialize the offered “value” by the company in a different sense encompassing the company strategic objectives.

Complex networks of assets can make difficult to translate the two topics (value and risk) and manage both quantitatively easily, where assets are manipulated and kept operating at peak performance around the clock, 24 hours a day, in order to transfer the resources (water, gas electricity, information, etc.) to customers (households, commercial or industrial companies with different service necessities). Networks utilities need to assess the contribution of the network not only focusing on network's availability, reliability and quality of service[41], but also focusing on the losses of the expected value that can decrease revenues and increase costs[6]. In this sense, Rubio-Loyola et al (2015)[18] discuss the need for optimization of the business value of the network infrastructure, modelling the way the performance of services offered by network operators has a direct impact on its reputation, on its revenue due to new customer subscriptions, and also on penalties that can apply when services are not provided to an acceptable quality level.

With the motivation of align maintenance policies in network utilities companies, with the company strategy, this paper proposes a criticality assessment methodology in order to materialize the "value" provided by the network of assets, and with the aim of determining the strengths and weaknesses due to the network topology. At the same time, a risk-based perspective is searched, serving the methodology as a tool to adapt criticality according to changes, not only on relevant aspects of this business, but also on "network configuration of assets". Thus, to operate the network, we must consider demand, and also the environmental risk, that has a great influence in the delivered services[19]. Therefore, two are the main purposes in this research:

- A quantitative methodology to assess the value and risks due to assets, aligned with the company strategies,
- Adaptability and flexibility of the methodology according to changes in network configuration, assets reliability and business aspects.

Asset criticality assessment can combine in a very practical way both concept: value and risk. Then, we first have to deal with the problem of determining asset's criticality within the network with a systematic method to establish priority (when scheduling maintenance work with limited resources[8] using key performance drivers), considering factors related to the value management such as business impact, need urgency, etc.[9], and second according to the evaluation of predictable and/or unpredictable circumstances that may happen (with probability) due to an asset or its neighbouring assets. That is, asset's criticality in network utilities should be determined from a risk perspective in order to assess the network value, it has to surveillance not only asset reliability but also its financial and non-financial impacts during all the asset life cycle[11].

There are different methods in literature, most of them explored by Crespo et al. 2016[12], in order to assess asset's criticality, some based on qualitative techniques or others based on quantitative techniques depending on the available and trusted information and data. The more information and data, the more quantitative the analysis can be, and the less information and data, the less consistency and more difficult the analysis can be. Thus, in order to decide maintenance actions to mitigate risk in a cost-effective and efficient manner, a level of high-quantification is desirable from a risk management of the network and its value.

With this purpose, it is proposed a process of assets criticality supported on the quantified process defined by Crespo et al. 2016[12], combining assets maintenance strategies to business value in a network utility companies, with network topology analysis according to importance of the associated risks, in order to prevent or to eliminate the most important risks[15], providing a systematic basis for deciding what assets we can assume[16] (ranked) with a certain maintenance management program[12].

The main objective of the proposed criticality analysis is to determine the importance and consequences of potential failure events within the operational and topology context in which they work[13], prioritize or rank ("probability-risk number"-PRN[14]) assets or maintenance actions according to importance of the associated risks.

In order to address this purpose, this paper is structured in four sections. In Section 2, an introduction about the importance of the network conservation and its consequences is presented from a business point of view, as basis of the network infrastructure evaluation. Then in Section 3 the proposed criticality analysis process for network utilities is developed in a mathematical model considering different network topologies and applying it in real case about a telecom network utility. Finally conclusions are shown in Section 4 of the paper.

2 NETWORK INFRASTRUCTURE EVALUATION

The network capacity has to be regulated and diversified, and the dispersed assets has to be operated for adaptation to customers demand. This normally requires very demanding technical activities to sustain the contracted service level agreements. Services are consumable with a tangible component based on resource consumption and an intangible component based on service experiences. That is, there is also an intense and long lasting relationship through a diverse range of interactions with customers and consequently, that determine the customer satisfaction. These companies are exposed to many types of hazards, such as natural hazards, component aging and failure, sharp load demand increase, climatic changes, intentional attacks. Besides, any service failure could be propagated in a massive way, making vulnerable the network by:

- Physical degradation or destruction,
- Disruptions and congestions,
- Attacks or
- Disasters.

And usually, the safety margins preventively designed may not be sufficient to cope with the expected and, most of all, unexpected stresses arriving onto the systems, which emerge from small perturbations that cascade to large-scale consequences[22].

As we have mentioned, network assets prioritization has to encompass "risk-based" and "business value-oriented" assessment methods (aligned with ISO 55000 approach), searching adaptability to any the network topology it has to contain as additional criteria locational and hierarchical connections among assets.

In reference to risk-based assessment, many authors concentrate their efforts in evaluating significant interactions (called critical incidents) that provoke positive and negative feelings of customers concerning service issues, such as those related to the ability to respond to contingencies, the reliability and the security of the service, safety and environmental preservation, etc[20]. Consequently, we combine the probability of an failure event as critical incident with the impact that event would cause, then Risk=PxC, where P is probability and C is consequence[21]. And in reference to business value-oriented, to effective control of the business sustainability, consequences evaluation method allows consider not only operative impacts, but also reputational, environmental legal, financial, etc.

Following the “risk-based” and “business value-oriented” assessment of assets, the most frequently evaluated criteria are summarized and classified now according to the evaluation of maintenance contribution in Gómez and Crespo (2012)[20] and Zio (2016)[2] in the following categories:

1. Business economic (cost & benefits) criteria: basically on monetary assessment of consequences, such as loss of earnings, loss of earnings in risk, loss of customer earning in risk, life-cycle-cost, market drivers, etc.
2. Operation criteria: such us communication, control, human and organizational factors, logistics, etc.
3. Service quality criteria: over the performance in the delivered services, such us availability, response time, reestablishment time, reliability, validity attributes of the end-user service, capacity class specific parameters, maximum services usage volume considering capacity class, means of supervising and reporting SLAs, etc.
4. Industrial Security, evaluating possible impacts in the asset integrity or surrounding assets or infrastructures (i.e. specific physical assets such as: production processes installations and machinery, manufacturing facilities, plants, infrastructure, support systems, etc.).
5. Legal criteria, in two ways, such as monetary settlements or as H&S / Environmental requirements (pollution, sustainability, etc).
6. Geographical coverage of the service, by levels of aggregation and based on information about connectivity performance gathered (forwarding and backwarding).
7. Location parameters, that can influence in the asset risk, such us geographic conditions, accessibility for maintainability, operating environment conditions, or geographical influence to or by third parts.
8. Connectivity criteria of the assets in the network: searching path diversity focus on network survivability and resiliency. In relation to Graph theory based on connectivity and cascade propagation of failures, searching robustness and redundancy.

Each of these criteria can represent components of the value of the network exploitation and be expressed by qualitative, quantitative or semi-quantitative methods. The main difficulty of this methodology is to select the proper criteria to represent consequences, the weight of them and the consistency among them and their scale values[12]. The selection of these parameters is crucial for adjustment to the company strategy and for the complexity of the criticality evaluation process. A very complex process can drive to bad results (missing information, unreliable assessments, incoherencies in asset evaluation, etc.), and even pushing the organization to desist before the end of the process.

Based on failure events as critical incidents, their likelihood of occurrence provide a narrow relationship between network conservation and provided value to customers by levels of aggregation, determining the level of required maintenance actions, in order to properly sustain the service level agreements over time. The quantification of the likelihood of the event is employed in our model as frequency factor. Thus, the methodology multiply the failure probability or frequency by the severity of it[24,25] in each asset. Accordingly, the right frequency factors and severity effects, to be considered in the criticality analysis, have to be determined respectively in relation to uncertainty (probability) appearance, and the negative or undesirable terms with respect to the planned objectives or standard behaviours in terms of losses, damages, injuries. Obviously, all of them, based on available information about the assets.

Therefore, to assess the real severity in a network, we have to consider vulnerability and resilience under the dynamic complexity with interactions among nodes through link dependences with other neighbours (Network Topology). Therefore, network criticality should not only consider reliability but also the ability to recover from disruptions, minimizing the impact on health, safety, security, economics and social well-being[23]. That is, not only functional, but also topological.

The adopted process for Criticality, aims a practical analysis of the network and the individual assets, supported by the concept of risk, but quantitatively as possible due to two reasons:

- First, in order to facilitate decision-making and continuous improvement[26] based on results linking the problems' effects to their root causes.
- Second, in order to link decisions with risk-cost-benefit analysis, *"the knowledge of costs aids managers to justify investments…and assists them in monitoring the effectiveness of the effort made"*[27].

3 CRITICALITY ANALYSIS PROCESS DEVELOPMENT

From now on, it is described the process to get the criticality evaluation of the different assets in the network, defining the mathematical model that support the process and applying it in the practical case step by step. In Figure 1 a series of stages are shown, which will be sequentially introduced in different sections to follow in order to properly manage criticality assessment and that may be used to support decision making process inside each one.

The generic process for criticality assessment that will now be proposed and defined, consist of eight sequential stages and integrates other models found in literature: reinforcing the idea of priorization based on risk, it is developed over the Woodhouse PRN[21] (Probability-Risk Number) linking the frequency of the causes to the effects of them (severity) and, over the quantified matrix representation and implementation steps sequence of Crespo et al. (2016)[12]. Each stage is used to order and facilitate the decision making processes to follow.

The procedure to follow in order to carry out an assets criticality analysis following "risk-based" and "business value-oriented" perspectives could be then depicted as follows:

1. Define scope of the analysis over the available data;
2. Determine infrastructure model for asset hierarchizing and their relations;
3. Define the real infrastructure according the before determined model:
4. Establish the severity factors to take into account and the number of asset severity levels to establish;
5. Obtain the frequency as factor of probability and its quantified levels to apply;
6. Decide the relative importance of each severity factor;
7. Evaluate the consistency of the severity and frequency factors distribution;
8. Establish the overall procedure for the identification and priorization of the critical assets.

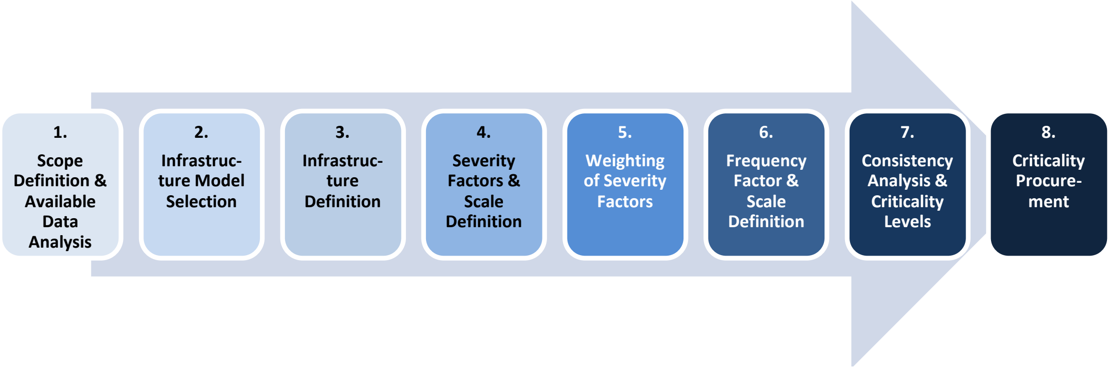


Figure 1. Criticality Analysis Process Development

3.1 SCOPE DEFINITION & AVAILABLE DATA ANALYSIS

In order to represent the analysis process and the mathematical model implementation, a practical case for telecommunication network is introduced step by step.

The scope of the process consists on identifying the risks of the network and providing relative priorities for mitigation plans to address them in a cost-effective and efficient manner. By doing so we ensure that maintenance actions are effective, that we reduce the direct and indirect maintenance cost due to a failure in a node of the network, in this example a telecommunications network.

The use of quantitative vs. qualitative techniques to assess criticality will largely depend on the company culture and management's comfort level with numbers vs. opinions. This process assumes a certain information and knowledge of the network to analyse. Of course, the more information and data, the more quantitative the analysis can be.

To ensure the required level of information and knowledge about the systems and their historic behaviour within the network services development, the analysis include the following information sources:

- Criticality Analysis team: diverse experts involved in the operational context of networks (operations, maintenance, processes, safety and environment).
- Engineering data: technical characteristic about assets and the systems where they are integrated, including data for functional loss effect evaluation.
- Operational data: including current failures frequency and functional loss effect regarding operation and capacity impacts.

3.2 INFRASTRUCTURE MODEL SELECTION

In this stage, the different levels of asset hierarchization are defined to model the real infrastructure. The selected infrastructure model in this example is organized and interrelated in four main parts: generation, where the services are generated; transmission, where the services are transformed and transported to remote areas by connections with huge capacity; distribution, technical sites to disperse the services within each area; and customer links, to supply the services to the customers.

3.3 INFRASTRUCTURE DEFINITION

Our practical case focuses on the first hierarchical level of a telecommunication network, the transmission level which is defined in Figure 2 with eight nodes connected among them.

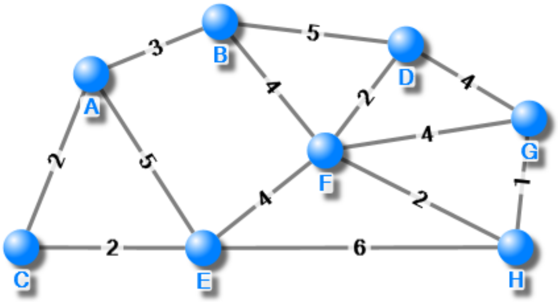


Figure 2. Practical case Telecommunications Network Topology

The idea of distinguish between 3.2 and 3.3 stages is to facilitate the re-utilization of the infrastructure models in different criticality assessment projects or companies, linking the severity factors to the hierarchy level of the infrastructure model instead of the assets. The criticality process can use the same severity levels for all the different hierarchy levels of the infrastructure model or define different ones in each hierarchy level.

3.4 SEVERITY FACTORS AND SCALE DEFINITION

On the basis of above mentioned categories of most frequently evaluated criteria, a proper and deeper analysis to extract the relevant aspects adjusting these to the telecommunication network use case is realized in meetings with the participation of the diverse experts involved in the operational context of networks (operations, maintenance, processes, safety and environment). As a result of the meetings, pre-selected most relevant factors to compose the assessment of different criteria were the followings:

1. Business-oriented parameters:
    - Loss of earnings as monetary assessment of consequences. Focusing the criterion on system functionality in all the failure downtimes.
    - Life-cycle-cost, including the estimation of all the corrective costs per failure.
    - Market drivers as bad reputation due to failures, provoking loss of customers and/or company image.
    - Market segmentation of customers in classes, by reporting income to the company, corporate image or strategic / social importance.
2. Operation and Management parameters:
    - Accessibility to repair the asset in its own site.
3. Service quality and Performance parameters:
    - Unavailability as accumulated service downtimes due to failures.
    - Unreliability centred on the probability of functional failure occurrence.
    - Capacity usage from designed maximum or nominal capacity as the basis of service aggregation from customers to the core of the network or generation nodes.
4. Industrial Security:
    - Evaluating possible impacts of cascading service outages.
    - Evaluating possible effects in surrounding assets or infrastructures.
5. Legal environmental and H&S parameters:
    - Monetary H&S / Environmental consequences. According to the principle of European new environmental legislation, those who harm the environment, will pay to clean it. These issues also affect customers and society's perception of the company, loss of customers and/or company image.
6. From Geographical coverage of the service by levels of aggregation:
    - Technical coverage of the asset and,

- Number of customers supported by it.

7. From Location parameters:
    - Reachability easily not far away from the maintenance office, due to long distances among network components.
    - Geographical or Environmental influence in the asset risk, such us earthquakes, mudslides, steep vegetation.
8. Connectivity parameters:
    - Betweenness of nodes oriented to centrality importance of in the network and path diversity.

Criticality mathematical notation is summarized below per each asset (node-r) in a network:

r : $1 \ldots k$ element or asset analysed,
i: $1 \ldots n$ criteria to measure severity of an element functional loss,
j: $1 \ldots m$ levels of possible effects of a functional loss for any criteria,
M_i : Maximum level of admissible effect for criteria i, with $M_i \leq m, \ \forall i$,
MS : Maximum severity value,
S_{ij} : Severity of the effect j for the severity criteria i,
pe_{rij} : Potential effect j of criteria i for the functional loss of element r,
S_r : Severity of the functional loss of element r,
w_i : Weight given to the severity criteria i by experts, with $\sum_{i=1}^{i=n} w_i = 1$,
e_{ij} : Effect j of the severity criteria i,
v_{ij} : Fractional value of effect j for the severity criteria i,
z: $1 \ldots l$ categories of functional loss frequency,
af_z : Average frequency of functional loss for frequency level z,
ff_z : Frequency factor for frequency level z,
fe_{rz} : Boolean variable with value 1 when z is the level of the observed frequency of element r functional loss, 0 otherwise,
f_r : Value for the frequency of the functional loss of element r. f_r^y : It is f_r including proportionality,
C_r : $S_r \cdot f_r$:Criticality of element r,
f'_r: New probability of the effect j of criteria i for the failure of r,
S'_r: New observed severity of the functional loss of element r,
C'_r: New criticality of element r,
$CNPV$: Customer Net Present Value,
q_a : Proportional ratio of CNPV as mean corrective cost per failure,
n_{cr} : Concerned customers per failure of element r,
T: Mean life time cycle of CNPV,
n_{pr} : Average market coverage ratio of customers in the area of element r,
q_p : Proportional ratio of CNPV in publicity to compensate bad reputation,
t_r : Average reestablishment time of the element r, and $t_{contract}$ is defined reestablishment time per contract,

$\bar{t}$: Average reestablishment time in all the elements of the network,
$P_a(t)$: Abandon probability per customer related to the offered reestablishment time by the contract,
$\rho(t)$: Boolean variable indicates with $\rho=1$ that $t_r > t_{contract}$, and with $\rho=0$ otherwise,
LE_r : Loss Exposure Criterion Cost of element *r*,
h_{ESr} : H&S / Environmental consequences level of the element r,
P_{accr} : Probability of occurrence of an H&S / Environmental accident due to a failure of element r,
ES_r : Environmental and Safety Criterion Cost of element *r*,
SI_r : Social Importance Criterion Cost of element *r*,
$b(r)$: *Betweenness* coefficient of the element *r*,
$\dot{B}$: Maximum betweenness in the network,
$d(k,s)$:Number of shortest paths that pass through the element *r*,
$d_{k,s}$: Number of all the shortest paths that connect elements *k* and *s*,
x_r: Remaining capacity in terms of customers of element *r*,
n_f: Number of failures with service interruption in the network
γ_{xy}: Proportionality Factor due to extra degradation by locational conditions in the zone of element *r*.

3.4.1 Severity Factors Definition

The number of selected severity criteria has to be reduced as much as possible, not making complicated model implementation and the interpretation of the results. But, other hand, criteria have to be enough to describe accurately the reality of the network and avoiding dependence among factors. Authors recommend, from our experience, to aggregate all the factors using from four to six criteria. From the analysis above, the determination of the final severity criteria to include have been realized in four criteria to compose the model for this case:

a. Loss Exposure Criterion (LE)
b. Environmental and Safety Criterion (ES)
c. Network Security Criterion (NS)
d. Social Importance Criterion (SI)

Searching quantification on mathematical formulae, allowing correct interpretation of importance of each criterion, specialized meetings of experts are realized for each criterion.

a. Loss Exposure Criterion (LE)

This criterion has to concreted the amount of economic losses due to functional breakage[18], not only the direct losses on earnings, but also corrective costs and bad reputation resulting in indirect losses of customers:

- Direct costs:
    - Corrective costs: Which summarizes all the costs in materials, human resources, supplies and including depreciation per failure in order to show the contribution to

the life-cycle cost. Then for an asset (node-r), these costs are concretized as a part (q_a) of the Customer Net Present Value (CNPV) per each concerned customer (n_{cr}) and failure, considering CNPV as the mean of all the correspondent to this asset.

Corrective costs of node r = $n_{cr} \cdot q_a \cdot \mathrm{CNPV}$ (1)

- Loss of earnings: Due to the operational reliability of the network, the potential impact of a functional loss of an asset is reflected by the service interruption, being proportional to time, to the unavailability of the service per failure related to the service re-establishment time (t_r) against the total time (T) of customer life-cycle, and so determining the discounting Customer Net Present Value (CNPV) per each concerned customer (n_{cr}) and failure.

  Loss of earnings of node r = $n_{cr} \cdot (t_r / T) \cdot \mathrm{CNPV}$ (2)

- Indirect costs: Failures decrease customer satisfaction, transmitting bad propaganda into the market (up to 10 partners[28]), modifying customer perception of service quality (up to 44% of customer losses[29]). Then for an asset (node-r), bad propaganda due to failures could have effects over current customers or potential customer:
  - Effects over current customers. In this case, current customers (that have suffering failures) could decide to abandon the service with a certain probability $Pa(t_r)$ related to the service re-establishment time (t_r) against the offered by the contract or existing standard market service level agreements (SLA). We will rely on a 2-parameter Weibull distribution and Maximum Likelihood Estimation (MLE) to obtain the Weibull equation that reflects the probability to abandon $Pa(t_r)$ per customer and per each failure based on the mean service re-establishment time (t_r). In addition, they can transmit bad propaganda to other customers, decreasing their satisfaction.

    Indirect costs in impacted customers by failures = $n_{cr} \cdot Pa(t_r) \cdot \mathrm{CNPV}$ (3)

  - Effects over potential customers. Market reputation is crucial to acquire new customers. The transmitted bad propaganda outside the company to potential customers, could decrease their intention to contract the services. The cost estimation of acquiring a new customer influenced by bad propaganda is twice than a non-negative-influenced customer[28,29].

The influenced customers and potential customers are estimated through the market coverage ratio of customers (n_{pr}) in the area of technical influence of the asset. Thus, the number of customers is a part of the influenced ten partners by bad propaganda, and the cost of loyalty is half of capturing new influenced customers, and concretized as proportional ratio q_p in publicity inside the CNPV to compensate the bad reputation but only when the t_r is higher than the offered by the contract $t_{contract}$. Although the influence on these partners only comes up when the re-establishment time is major than the offered by the contract ($t_{contract}$). The Boolean variable $\rho(t_r)$ indicates with $\rho=1$ that $t_r>t_{contract}$, and with $\rho=0$ otherwise, $t_r<= t_{contract}$.

$$\text{Indirect costs of influenced partners} = n_{cr} \cdot q_p \cdot CNPV \cdot 10 \cdot (2 - n_{pr}) \cdot \rho(t_r) \quad (4)$$

Consequently, for each asset, (see Equation 5) the direct corrective costs are sum of the corrective cost and loss of earnings over the CNPV per the impacted customers, and the indirect costs due to the exposed customers in risk to abandon the service over the re-establishment time (t_r), and the associated indirect costs of influenced partners.

$$LE_r = CNPV \cdot n_{cr} \cdot \left[\left(q_a + \frac{t_r}{T} \right) + \left(P_a(t_r) + \rho(t_r) \cdot (20 - 10 \cdot n_{pr}) \cdot q_p \right) \right] \quad (5)$$

b. Environmental and Safety Criterion (ES)

Based on Legal parameters, H&S / Environmental consequences of an asset (node-r) can be produced by failures, and they can harm the environment or people. To evaluate this perspective, we have employed the Wireman (1998)[30] method, which has been wide used to evaluate these risks, reducing the consequences categories in the following levels h_{ESr} (based on MIL-STD-882C standard[31]):

- Catastrophe; numerous fatalities; damage or penalty over $500,000.
- Critical fatality, damage or penalty $100,000 to $500,000.
- Extremely serious injury (amputation, permanent disability); damage or penalty $10,000 to $100,000.
- Minor cuts, bruises, bumps; minor damage or penalty 1,000 to $10,000.

Although, in a failure event, the risk about H&S / Environmental or penalty could appear or not, that is, there is a probability that the accident occurs once the failure has occurred (P_{accr}). Therefore, the reduced and modified levels of probability for this risk are four:

- Quite possible (has an even 50% chance) with a $P_{accr}=0.5$.
- Remotely possible with a $P_{accr}=0.1$.
- Conceivable (has never happened after many years of exposure) with a $P_{accr}=0.05$.
- Practically impossible (has never happened) with a $P_{accr}=0.01$.

$$ES_r = h_{ESr} \cdot P_{accr} \quad (6)$$

c. Social Importance Criterion (SI)

As it is said before, in network utilities, is crucial not only from an economic perspective, but also from a social perspective. In this line, critical and strategic customers are usually more exigent in service performance and quality, and we should consider the indirect costs due to their dissatisfaction. Consequently, this criterion is related to the consequences of bad reputation, transmitted by critical customers. Besides, the supplied services become but even more critical in emergencies due to important accidents or disasters that can impact heavily in society. Consequently, the importance of critical customers does not have to be evaluate only with an increment of CNPV, but to be assessed taking into count the overall impacts of a bad supply of services to them, that could detonate high bad reputation in the society. Impacts go beyond the repair costs and penalties, because it has to consider the impact in market value, and so if the continuity of supplied services is crucial facing catastrophes. The economic impact on the fair market value (FMV) of our critical customers could be almost 15% in a year[34].

Subsequently, we have considered an amplification factor of the criticality when social sites or large enterprises are supplied by the asset, because it provides services that are key to support the performance of the own social service. Taking this into account.

Depending on the type of customers, the associated consequences costs to this criterion, have been related to the amount of earnings in risk plus the necessary publicity to recover the market image due to bad reputation and the losses in the capital stock during a year (up to 15%). Accordingly, the supplied services by assets are grouped into different customers classes, considering the strategic importance of failures in the same line of the H&S / Environmental evaluation SI_r, aligning the consequences cost of each level with the consequences categories of ES criterion h_{ESr} with a remote probability P_{accr} = 50% of chance:

- More than three social sites or large enterprises, failure impact estimated over $250,000. Social Sites: such as public administrations, hospitals, fire station, transport stations, airports, military buildings, ports, etc.
- Less than three social sites or large enterprises with failure impact between $50,000 to $250,000.
- More than 10 Medium and Small enterprises with failure impact between $5,000 to $50,000.
- Less than 10 Medium and Small enterprises or regular customers with failure impact less than $5,000.

d. Network Security Criterion (NS)

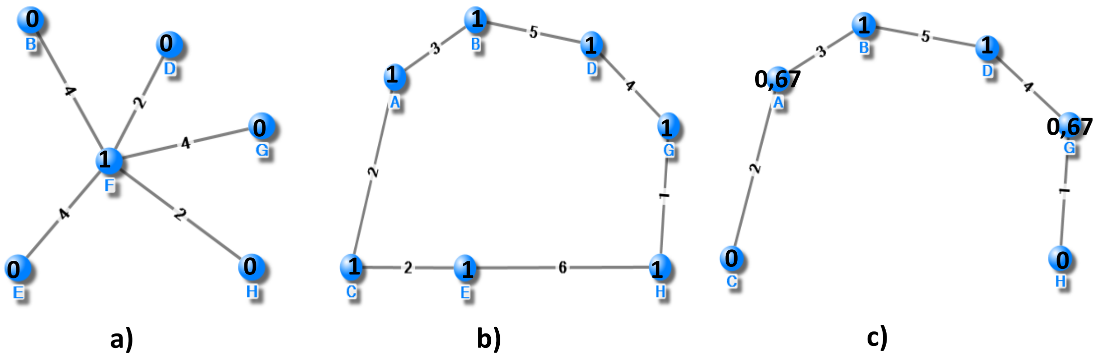
In Network Security criterion, we have tried to summarize the possible impacts of cascading service outages and the possible effects in surrounding assets or infrastructures. For this purpose, this criterion correlate them with parameters about network topology, seeing that networks are dynamic and suffer several configuration and operational changes. Network topology is the logical representation of the network as a combination of nodes linked by edges (distances among nodes), and in line with the purpose of showing the dynamic importance of a node to transport the services from a vulnerability point of view[32,33], there is a graph coefficient that can be derived for an asset (node-r):

- Betweenness coefficient of a node is the numerical representation of robustness and redundancy in a network, but not only evaluating the connections of the node, but also the connections that its neighbours as shortest path. Betweenness centrality describes if a node have a high number of shortest paths from the rest nodes on the graph, and if a failure impacts in a node with a high betweenness, there is a high probability to cut the network into multiple unconnected nodes. This coefficient is based on communication flow and with this parameter we search how a node is able to assist to others or to be assisted by the neighbours to deliver services in case of failures and, evaluating cascade failures, and also how its neighbours can survive receiving services from it. It is a good measure of the centrality in a network and the capability to route services from other nodes in emergency cases.

We have compound the network security criterion based on betweenness centrality graph coefficient in a normalized way, using the maximum betweenness number of graph nodes $\dot{B}$. This coefficient evaluates the shortest paths that pass through the node r from al the total number of shortest paths between every other pair of nodes, (see Equation 7 where d(k,s) is the number of shortest paths that pass through r and $d_{k,s}$ is all the shortest paths that connect k and s nodes.

$$b\,(r) = \left[\sum_{k \neq r \neq s} \frac{d(k,s)}{d_{k,s}} \right] \;/\; \dot{B} \tag{7}$$

In order to show the properties of this coefficient, the following Figure 3 presents the values of betweeness coefficients in typical network topologies (star, ring, in a series) derived from Figure 2, Figure 3-a, 3-b and 3-c respectively; as a token of centrality importance of the node. Where in the centrality value is well represented in the node F in Figure 3-a, equals centrality value in a ring topology for all the nodes in Figure 3-b, and maximum centrality value in nodes B and D in Figure 3-c. The correspondent betweenness coefficients of the network of the Figure 2 is in Figure 4-a.



a) b) c)

Figure 3. Betweenness coefficients examples.

From a survival point of view, the betweenness coefficient ranks the nodes according to their influence in the neighbours, higher values (near to 1) indicate multiple redundant edges to be reconfigured to support their neighbours in case of node failures, see in Figure 4 over the network of the Figure 2.

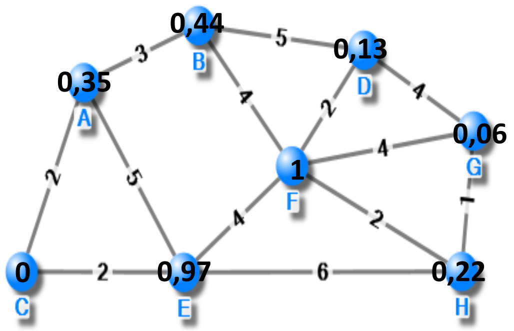


Figure 4. Betweeness coefficients in network example.

The topological importance of the nodes in a survivability point of view can be shown by betweenness coefficients, and for this objective, the cost of consequences due to bad redundant paths configuration is considered an opportunity cost because these could be utilized in emergency cases to support failures of their neighbours. Therefore, the remaining node capacity (x_r) in terms of possible customers (CNPV) could support other nodes in the mean re-establishment time ($\bar{t}$) against the total time (T) of customer life-cycle for all the failures with service interruption (n_f) in the network. In a failure event, the support of other node could appear or not, that is, there is a probability that the support occurs once the failure has occurred in the node, so betweenness coefficient is as a probability for the occurrence of this support due to redundancy by paths.

$$NS_r = CNPV \cdot b(r) \cdot x_r \cdot n_f \cdot \frac{\bar{t}}{(T)} \tag{8}$$

3.4.2 Scale Definition of Severity Factors

In a second step, the levels inside each criteria have to be established in the used scale in this model, from 0 to 100. Although, firstly, it is necessary to define the "*non-admissible*" effects for some criteria which represent those consequences, referred to a specific defined criterion, that are considered unacceptable by the organization. Therefore, this level of impact can be identified as that saturate severity assessment, thus those assets where "*non-admissible*" effects can appear will have the maximum severity 100 (the top level of this criterion). Besides, in any criterion we could consider as the lower level *"No Affection (N/A)"* effect if it is needed.

With these considerations, description of levels of the four severity criteria are included below:

- Loss Exposure Criterion (LE): Based on Pareto analysis as in frequency levels, we have developed 4 costs categories depending on the cost distribution and finding averages costs and the corresponding factors for each effect classification level:
    - Very High (10%),
    - High (20%),
    - Medium (20%) and
    - Low (50%).
- Environmental and Safety Criterion (ES): Based on William T. Fine (1971) factors, where the risk score is defined in three levels: Immediate (correction required; activity should be discontinued until hazard is reduced), Urgent (requires attention as soon as possible), and Possible or acceptable (hazard should be eliminated without delay, but situation is not an emergency). As a result, we have developed the following levels:
    - "Non-admissible" with $ES_r = h_{ESr} \cdot P_{accr}$ level equals or higher than \$ 250,000.
    - Urgent with $ES_r = h_{ESr} \cdot P_{accr}$ level between \$ 50,000 and \$ 250,000.
    - Possible with $ES_r = h_{ESr} \cdot P_{accr}$ level between \$ 5,000 and \$ 50,000.
    - N/A with $ES_r = h_{ESr} \cdot P_{accr}$ level equals or minor than \$ 5,000.
- Social Importance Criterion (SI): Accordingly our four types of customers, the classification level in this effect criterion are the following:
    - More than three social sites or large enterprises, failure impact estimated over \$250,000, valuing the impact as *"non-admissible"*.
    - High impact with less than three social sites or large enterprises with failure impact between \$50,000 to \$250,000.
    - Medium impact with more than 10 Medium and Small enterprises with failure impact between \$5,000 to \$50,000.

  - Low impact with less than 10 Medium and Small enterprises or regular customers with failure impact less than $5,000.
- Network Security Criterion (NS): By virtue of translate the impact to term of cost, and once the Pareto analysis has been utilized searching the distribution on 4 costs categories with their averages costs following the corresponding developed levels for the Loss Exposure Criterion (LE).
  - Very High (10%),
  - High (20%),
  - Medium (20%) and
  - Low (50%).

Thus, consistency in the Severity calculation of one element with respect to another is ensured, but also remarking non admissible situation such us the determined by Marketing and H&S departments in SI and ES respectively, searching consensus among conflicting worries about business value or costs. In our model we have used 100 as maximum value for overall severity to the network assets. The relative values for the different effects for each criteria are presented in a matrix, see Table 1, where units for these relative values are based on cost.

Criteria to measure Severity			
LE	ES	NS	SI
Category of effects per criteria and functional loss			
50,000	**Non admissible**	50,000	**Non admissible**
20,000	50,000	20,000	50,000
5,000	5,000	5,000	5,000
0	0	0	0

Table 1. Effects matrix per functional loss

3.5 WEIGHTING SEVERITY FACTORS

At this point, it is addressed the definition of the criteria weights and levels. Four levels of severity have been used for the evaluation of each of the four established criteria. In our case, in order to assign criteria weights that represent their relative importance within the model, it is recommended to employ a formalized method as AHP (Analytical Hierarchy Process) to obtain the subjective judgments about criteria importance from the experts involved in the meetings. In AHP, thanks to hierarchical structuring of decision-making, pairwise comparisons, redundant judgments and the eigenvector method for deriving weights and consistency considerations, the criteria weights combine both objective measures and subjective preferences, quantifying relative priorities for a given set of alternatives on a ratio scale[35,36]. The recommendation is to employ this method in few number of criteria, because the major drawback in the use of AHP is the effort required to make all pair-wise comparisons. In the example of this paper, w_i , weight given to the severity criteria i by experts, resulting from the AHP analysis are assume to be equal to:

$$[w_i]= 25, 20, 25, 30, \text{ where } [i]=LE, ES, NS, SI \tag{9}$$

In the mathematical model proposed, the effects severity matrix has been pre-defined previously, for any element included in the analysis (r), as follows:

$$S_{ij} = \begin{cases} MS, & for \quad M_i < j \leq m, \quad \forall i \\ \\ w_i v_{ij}, & for \quad 1 \leq j \leq M_i, \quad \forall i \end{cases} \tag{10}$$

Where

MS: Maximum value for overall severity.

M_i: Maximum level of admissible effect for criteria i, with $M_i \leq m$, $\forall i$ where $[i]=LE, ES, NS, SI$ *criterion* and $[M_i]$=4,3,4,3 as maximum levels of admissible effects for each criteria.

$v_{ij} = \dfrac{e_{ij}}{e_{ik}}$, with $k= M_i$ and $j \leq M_i$, and with $v_{ij} = 1$ for $j = M_i$ and $\forall i$, with e_{ij} as the effect j of the severity criteria i, *and* v_{ij} is the fractional value of effect j for the severity criteria i.

Thus, the corresponding effects severity matrix (according to Equation 10, and for MS=100) is included in Table 2. Notice how a non-admissible effect of SI will count for 100 (maximum value) regardless of the effect in any other criteria. Let's see the interpretation of Tables 1 and 2 as example:

- If its functional loss happens, node A, with effects on LE criterion with potential cost of 3,238.92 \$, on ES criterion with potential impact of 5,000 \$, on NS criterion with potential cost of 20,181 \$, and on SI criterion with less than three social sites or large enterprises (SLE); so the severity effect levels respectively are 1 in LE, 2 in ES, 3 in NS and 3 in SI.
- The correspondent points of severity effects are 0 in LE, 10 in ES, 10 in NS and 30 in SI, then the total severity criteria are 50.

Criteria to measure Severity			
LE (w_1=25%)	ES (w_2=20%)	NS (w_3=25%)	SI (w_4=30%)
Category of effects per criteria and functional loss			
25	**Non**	**20**	**Non**

	admissible:100		admissible:100
15	20	10	30
5	10	5	15
0	0	0	0

Table 2. Effects severity matrix per functional loss, S_{ij}

3.6 FREQUENCY FACTOR AND SCALE DEFINITION

Based on the unreliability, centered on the probability of functional failure occurrence, the frequency levels are determined, and using Pareto analysis (percentage of elements inside each level by the meetings of experts) according to 4 ($z=1..l$) frequency categories depending on the functional loss frequency: very high (10%), high (25%), medium (25%) and low functional loss frequency (40%), see Table 3. In the mathematical model, af_z is the average frequency of functional loss for frequency level z, and the frequency factor vector is ff_z.

Asset	f/y
A	7
B	1
C	4
D	3
E	1
F	1
G	8
H	6

Asset	f/y	Category (z)	% (z)	af_z	ff_z
G	8	Very high	10%	8	8
A	7	High	25%	6.5	6.5
H	6				
C	4	Medium	25%	3.5	3.5
D	3				
E	1	Low	40%	1	1
B	1				
F	1				

Table 3. Calculation of frequency factors per selected functional levels

The mathematical representation of the frequency of functional losses for an asset (r) is expressed in a vector fe_{rz} of (z) Boolean variables according to the levels of functional loss frequency:

$$fe_{rz} = \begin{cases} 1, \text{ when z is the observed frequency category } ff_z \text{ of element r functional loss} \\ 0, \text{ otherwise.} \end{cases} \qquad (11)$$

The frequency factor to apply to one element would be the result of the following scalar product:

$$f_r = \sum_{z=1}^{z=l} ff_z \ fe_{rz} \tag{12}$$

In our example for the asset *A*, the functional loss frequency vector is $[fe_{Az}]$=0,0,1,0, and the frequency factor to consider finally in order to calculate its criticality is: f_A=1x0+3.5x0+6.5x1+8x0=6.5.

3.7 CONSISTENCY ANALYSIS AND CRITICALITY LEVELS

In order to capture data concerning maximum potential effects, a matrix of n x m Boolean elements (pe_{rij}) are used for each asset (r), where i: 1…n are different severity criterion and and j: 1…m are levels of possible effects of a functional loss for any criterion. See the resultant matrix for A asset.

$$pe_{rij,} = \begin{cases} 1, & \text{When } j \text{ is the level of maximum potential effect of the functional loss of an element } r \text{ and for the severity criterion } i \\ 0, & \text{Otherwise.} \end{cases} \tag{13}$$

$$[pe_{Aij}] = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \tag{14}$$

Therefore, the total Severity of the functional loss of element r is as follows:

$$S_r = Min(MS, \sum_{i=1}^{i=n} \sum_{j=1}^{j=m} pe_{rij} S_{ij}) \tag{15}$$

And therefore the severity of the asset A would result in:

$$S_A = Min(100, 0+10+10+30) = 50 \tag{16}$$

Finally, according to the retrieved frequency factor (vector) and the severity factor (matrix) for a functional loss of an asset, concreted potential criticality is calculated as (see example for A asset):

$$C_r = f_r \times S_r \tag{17}$$

$$C_A=6.5x50=325 \tag{18}$$

As a result, we could generate automatically the criticality asset ranking per hierarchical level of the network, classifying them quantitatively in three criticality categories: low, mid, or high criticality, see Table 4. Then, these categories reflect the priorization for activity assignation from a strategic and cost point of view (business point of view). For this purpose, the amount of assets classified in each category has to be decided according to the budget segmentation of the department, in our example 15% for critical, 35% for semicritical and 50% for not critical.

Criticality level	% of assets	Criticality value interval	Area color in Figure 6 & Table 5
Critical	10	400–800	Dark grey
Semicritical	35	175-400	Grey
Not critical	55	0–175	White

Table 4. Criticality Categories for activities prioritation

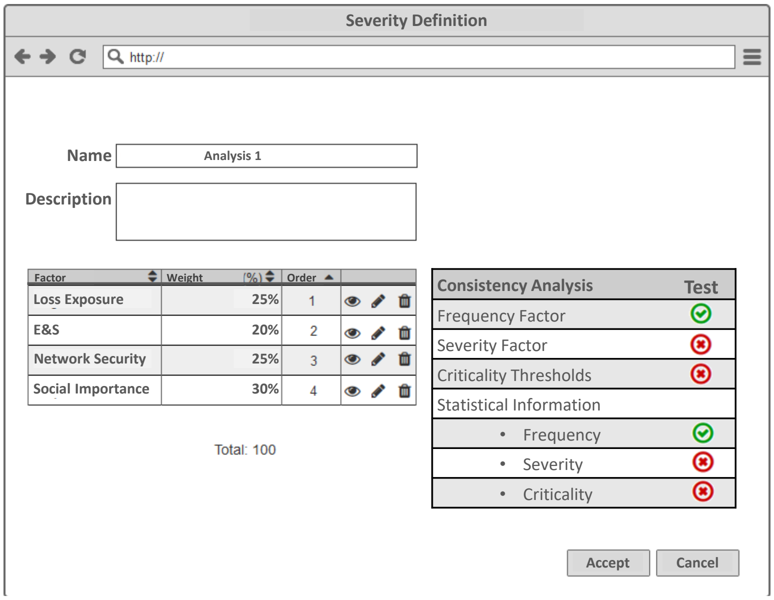
Once frequency and severity factors have been defined, they have to be reviewed, avoiding:

- Their levels cannot overlap;
- There are possible values that do not fit in some of the levels;
- There are levels of these factors empty of assets;
- The sum of the weighting of the different levels are consistent with the data;
- The sum of the weighting of the different factors adds up to 100;
- There are possible technical locations of asset without frequency and severity factors defined;
- There are assets of the same family in different levels without consistency;
- The criticality thresholds are correctly defined and congruent.

In order to control these issues, the criticality methodology has been developed in a software to test automatically them, and so several warning icons are included in the software indicating each one, see Figure 5. Besides, some graphs are incorporated in the consistency analysis:

- Ones showing the number and percentage of assets that have already defined a level of frequency and severity factors;
- Another graph indicating the number and percentage of all asset with assigned criticality and;
- Other group of graphs illustrating the percentage of assets in each level of frequency and severity factors;

- Another graph showing also the number and percentage of assets in each one of the criticality levels and;
- Advanced graphs and tables support the analysis with statistical information as a summary including density distribution functions and their parameters (including normal, exponential, Weibull, gamma, Poisson, and binomial) that best fit to distributions of assets in severity, frequency and criticality levels.



Name: Analysis 1

Description:

Factor	Weight (%)	Order
Loss Exposure	25%	1
E&S	20%	2
Network Security	25%	3
Social Importance	30%	4

Total: 100

Consistency Analysis	Test
Frequency Factor	✓
Severity Factor	✗
Criticality Thresholds	✗
Statistical Information	
• Frequency	✓
• Severity	✗
• Criticality	✗

Figure 5. Consistency Analysis in the software.

3.8 CRITICALITY PROCUREMENT

After the consistency analysis, it could re-adjust the levels and weights, the criticality matrix is realized, although the analysis methodology encompasses two additional studies of sustainable evolution of criticality: comparison of assets in the same or similar families/types/zones, and comparison of the asset over time.

- Family/Type/Zone Asset Comparison: Assessing the criticality occurrences by families/types/zones of assets, distinguishing extreme values in severity and frequency factors. I.e., in network utilities, some special geographical or environmental circumstances could increment the normal asset degradation (such us mudslides, steep vegetation, etc.), and from risk assessment point of view, the influence of this zone factor may obey, searching simplifying for a practical application, proportional contributions to the risk and without time dependency. Then, we would employ a component of proportionality with the failure frequency, modifying the frequency factor of an asset, from other of the similar family, with a proportional factor of probability γ_{xy}, being the multiplier factor in y number of times failure frequency of functional loss. With this proportional factor in frequency, we could model dynamic adaptation to real conditions, such us mudslides or steep vegetation. In case of proportional contribution, the frequency value of element r has to be obtained, multiplying by the proportionality factor γ_{xy} the frequency of the nodes in the same family with normal degradation. Then, the obtained frequency by proportionality will be set in the respective frequency category and obtaining the final f_r^y value for the frequency of the functional loss of element r. In case of proportionality factor γ_{x2} for node A, the frequency vector will be $[fe_{Az}{}^2]$=0,0,0,1 and the new correspondent frequency factor $f_A{}^2$=1x0+3.5x0+6.5x0+8x1=8.

- Dynamic Comparison: Orientated to sustainable evolution with the time, it is important to compare potential criticality versus new criticality for each asset. We have previously calculated the first, and in order to so, now we have to calculate the last one, retrieved from new data for observed functional loss effects. Then, we can model the new Severity and Frequency Factors of element r as follows with new effects, and the retrieved new criticality is formulated as C'_r (see example in node A with a change in frequency of failure to 4 and so the correspondent level is 2 with a value of 3,5). Due to frequency change of asset A, its criticality has been modified as semicritical instead of critical, showing this criticality reduction and improvement in the risk.

$$C'_r = f'_r \times S'_r \quad \rightarrow \quad C_{A'}=3{,}5\text{x}50=175 \tag{19}$$

The details for severity and criticality calculation of each node are described hereafter, in our case about a telecom company with the following average values for all the elements:

$$LE_r = CNPV \cdot n_{cr} \cdot \left[\left(q_a + \frac{t_r}{T} \right) + \left(P_a(t_r) + \rho(t_r) \cdot (20 - 10 \cdot n_{pr}) \cdot q_p \right) \right]$$

- CNPV=1,415€ with T=2 years or 17,520 hours of life time cycle,
- n_{cr}=50 concerned customers per failure of the 2,000 total possible customers of capacity per node,
- The corrective cost per failure is 5,640 €, then q_a= 8%,
- $t_{contract}$=12h and for all of them t_r> $t_{contract}$ then ρ=1,
- n_{pr}=25% market coverage ratio of customers in the area,
- The publicity cost per influenced potential customer q_p=20 €, then q_p =1.41%,
- $P_a(t)$ obtained by Weibull analysis with parameters β=1.67, α=96 as abandon probability per customer related to the offered reestablishment time by the contract,
- x_r=250 customers in terms of average remaining capacity of the element for all nodes.

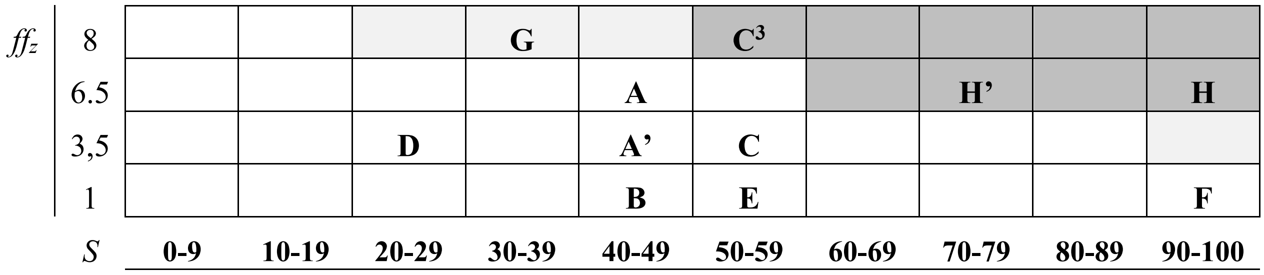
In Table 5, the reader can find the calculus in which are based each severity criterion and its correspondent severity level. The sum of all is multiplied by the frequency level to obtain the criticality per element.

Node Element	**Frequency**	Criteria to measure Severity															**Criticality**
		Loss Exposure (weight: 25%)			Legal Importance (weight: 20%)				Network Security (weight: 25%)			Strategic Importance (weight: 30%)			Severity		
	FE	tr	Total Risk	PE1	hES	Pacc	Total Risk	PE2	b	Total Risk	PE3	Strategic Customers	Total Risk	PE4	Total		
A	**6.5**	12	7,850.40	5	100,000	0.05	5,000	10	0.35	3,091	0	<3SLE	50,000	30	**45**		**292.5**
B	**1**	12	7,850.40	5	100,000	0.50	50,000	20	0.44	3,864	0	>10SME	5,000	15	**40**		**40**
C	**3.5**	15	26,317.03	15	50,000	0.10	5,000	10	0.00	0	0	<3SLE	50,000	30	**55**		**192.5**
D	**3.5**	12	7,850.40	5	5,000	0.01	50	0	0.13	1,159	0	>10SME	5,000	15	**20**		**70**
E	**1**	16	26,666.91	15	5,000	0.50	2,500	0	0.97	8,500	5	<3SLE	50,000	30	**50**		**50**
F	**1**	18	27,404.89	15	50,000	0.05	2,500	0	1.00	8,763	5	>3SLE	250,000	100	**100**		**100**
G	**8**	13	25,658.19	15	5,000	0.01	50	0	0.06	515	0	>10SME	5,000	15	**30**		**240**
H	**6.5**	14	25,980.60	15	250,000	0.10	25,000	10	0.22	1,932	0	>3SLE	250,000	100	**100**		**650**

Table 5. Criticality and Severity details per asset

The criticality analysis of the example, is summarized in Figure 6, where criticality categories are shown in boxes of grey colours. Besides, after two years the criticality analysis has been reviewed, changing for some nodes past criticality to new criticality values, that is, as a result of any improvement on reliability terms of the asset, the frequency over time was reduced, and in the opposite way, overstepped operating conditions increased the frequency over time.

In order to facilitate analysing the difference among past and new criticality as sample of the asset management performance, both calculations could be represented in a matrix, see in Figure 6, past and new criticality for all the assets. Thanks to the this results representation, we can audit current maintenance management, showing how good the applied activities are for an asset, either reducing frequency or minoring the consequences. A asset as example of the first case, and H asset for the last case. In addition, if node C has changed its locational environment, as example with more radiation can increase temperature, a proportional factor x3 has been obtained to model this circumstance, and so C^3 is introduced in the matrix.



ff$_z$	8				**G**		**C^3**				
	6.5					**A**			**H'**		**H**
	3,5			**D**		**A'**	**C**				
	1					**B**	**E**				**F**
	S	**0-9**	**10-19**	**20-29**	**30-39**	**40-49**	**50-59**	**60-69**	**70-79**	**80-89**	**90-100**

Figure 6. Past and New criticality matrices representation

4 CONCLUSIONS

The purpose of this methodology is to align assets management to business value, prioritizing any activity in the infrastructure, not only from a hierarchical point of view, but also evaluating the network topology implications (considering the network graph). Network utilities are companies that provide essential services or products to customers were reputational impacts are higher than operational impacts. Consequently, infrastructure has to be analysed with a risk-based methodology that considered these kind of impacts in the risk assessment. Our methodology employs also graph coefficients in order to include survivability perspective, and it has been applied in several network utilities (electricity, gas, and telecom) of national importance in Spain. Software tools have been developed to manage criticality of their networks which have about 25,000 nodes.

This methodology allows maintenance managers guiding the evolution of the life cycle of their infrastructure according to the business value conception, and at the same time to adapt their actions according to on-line data of in-service complex engineering assets. This makes this methodology specially suitable for supporting new challenging scenarios of maintenance management characterized for a high technological level, great interaction between assets and system and high rate of changing of demand and requirements of services. In addition, it will generate a great amount of data and information for the decision making. A practical approach to the strategical maintenance management, like is presented in this paper, will not be an option any more but a critical requirement.

This managerial tool allows structuring the maintenance department scorecard according to criticality levels. This facilitates graphic representations in different areas by level of criticality, delimiting the rank of assets encompassed by specific maintenance policies. For example, Condition-Based Maintenance (CBM), Root-Cause analysis (RCA) and RCM (Reliability Centered Maintenance) analysis can be suggested for critical assets; detailed Risk-Cost-Benefit analysis can be derived for semi-critical assets; and Run to Fail policies for non-critical. This relocates the maintenance efforts into more critical assets.

This methodology has been fully implemented in the telecom company that has provided the data used in this paper. As a result, improving network availability in 0,73% (from 98,5% to 99,23%), in a planning horizon of two years, and 10% reduction of the maintenance overall budget in the same period.

REFERENCES

1. EN 13306:2010, (2010) Maintenance Terminology. European Standard. CEN (European Committee for Standardization), Brussels.
2. ISO 9001, (2008) Quality management systems—requirements. *International Standards for Business, Government and Society*. http://www.iso.org.
3. Murthy DNP, Atrens A, Eccleston JA, (2002) Strategic maintenance management. *Journal of Quality Maintenance Engineering* 8(4):287–305.
4. EN 13269, (2006) Maintenance—guideline on preparation of maintenance contracts. *European Standard, CEN (European Committee for Standardization)*, Brussels.
5. Guillén AJ, Crespo A, Macchi M., & Gómez JF (2016). On the role of Prognostics and Health Management in advanced maintenance systems. *Production Planning & Control*, 27(12), 991-1004.
6. Kamoun F (2005). Toward best maintenance practices in communications network management. *International Journal of Network Management*, *15*(5), 321–334.
7. Crespo A, Sola A, (2016) *Principles and framework of Asset Management.* AENOR
8. Crespo Márquez A, (2007) The Maintenance Management Framework. Models and Methods for Complex Systems Maintenance. London: Springer Verlag UK.

9. Campbell JD, Jardine A, (2001) Maintenance excellence. New York: Marcel Dekker.
10. Newbery DMG, (2002) Privatization, restructuring, and regulation of network utilities. MIT Press, Cambridge.
11. Saleh JH, Marais KB, (2006) Reliability: How much is it worth? Beyond its estimation or prediction, the (net) present value of reliability. Reliability Engineering and System Safety 91, 665–673.
12. Crespo A, Moreu de León P, Sola A, Gómez JF, (2016). Criticality Analysis for Maintenance Purposes: A Study for Complex In-service Engineering Assets. *Quality Reliability Engineering International*, 32 519–533 in Wiley Online Library.
13. Woodhouse J, (1994) Criticality Analysis Revisited. The Woodhouse Partnership Limited, Newbury, England 1994.
14. Duffuaa SO, Raouf A, Campbell JD, (2000) Planning and control of maintenance systems. Indianapolis: John Wiley and Sons.
15. Khan FI, Haddara M, (2003) Risk-based maintenance (RBM): a new approach for process plant inspecton and maintenance. *Process Saf. Prog*. 23 (4): 252–265.
16. Brown SJ, May IL, (2000) Risk-based hazardous protection and prevention by inspection and maintenance, Trans. *ASME J. Press. Ves. Technol.* 122: 362–367.
17. ISO 55000:2013, Asset Management - Overview, principles and terminology
18. Rubio-Loyola J, Toscano-Pulido G, Charalambides M., Magaña-Aguilar M, Serrat-Fernández J, Pavlou G & Galeana-Zapién H. (2015). Business-driven policy optimization for service management. International Journal of Network Management, 25(2), 113-140.
19. Gómez JF, Crespo A, (2012) Maintenance Management in Network Utilities: framework and practical implementation. London: Springer-Verlag.
20. Gómez JF, Crespo A, López-Campos M, (2016) Customer-oriented risk assessment in network utilities. Reliability Engineering and System Safety 147, 72–83.
21. Woodhouse J, (1996) Course of Reliability Centered Maintenance (RCM) – Section two: Failure Modes and Effects Analysis. The Woodhouse Partnership, England.
22. Zio (2016) Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering and System Safety 152: 137-150.
23. COUNCIL DIRECTIVE 2008/114/EC (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.
24. Jones R, (1985) Risk-Based Management: A Reliability-Centered Approach, Gulf Publishing Company, First Edition, Houston, Texas.
25. Arunraj NS, Maiti J, (2007) Risk-based maintenance -Techniques and applications. *Journal of Hazardous Materials* 142: 653–661.
26. UNE 66178, (2004) *Quality Management System. Guide for the management of process for improvement.*
27. Dale BG, Plunkett JJ (1991) *Quality costing*. Chapman Hall, London.

28. Goodman J, (1986) Technical assistance research program (TARP). USA: US Office of consumer affairs study on complaint handling in America.
29. Keaveney S, (1995) Customer switching behaviour in service industries: an exploratory study. J Mark 59:71–82.
30. Wireman T, (1998) Developing performance indicators for managing maintenance. New York: Industrial Press.
31. MIL-STD-882C (1993) Military Standard System Safety Program Requirements. Department of Defense, United States of America.
32. Rohrer JP, Naidu R, Sterbenz JPG (2009) Multipath at the Transport Layer: An End-to-End Resilience Mechanism. 9781-4244-3941-6/. IEEE.
33. Rohrer JP, Sterbenz JPG (2011) Predicting topology survivability using path diversity. Published in: Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on Conference. Page(s): 1 – 7. ISSN: 2157-0221. ISBN: 978-1-4577-0682-0. IEEE.
34. Knight RF, Pretty DJ, (1997) The impact of catastrophes on shareholder value. Oxford Executive Research Briefings, Templeton College, University of Oxford.
35. Bevilacqua M, Braglia M, (2000) The analytic hierarchy process applied to maintenance strategy selection. *Reliability Engineering and System Safety* 70: 71–83.
36. Molenaers A, Baets H, Pintelon L, Waeyenbergh G, (2012) Criticality classification of spare parts: A case study. Int. J. Production Economics 140: 570–578
37. El-Akruti K, Dwight R, Zhang T, (2013) The strategic role of Engineering Asset Management. Int. J. Production Economics 146: 227-239
38. Rodney Howes, (2000) Improving the performance of Earned Value Analysis as a construction project management tool. Engineering, Construction and Architectural Management, Vol. 7 Issue: 4, 399-411
39. Zhou J, Huang N, Sun X, Wang K, Yang H, (2015) A new model of network cascading failures with dependent nodes. Annual Reliability and Maintainability Symposium (RAMS)
40. Heegaard P, Trivedi K, (2009) Network survivability modelling. Computer Networks, vol. 53, no. 8, pp. 1215-1234, 2009
41. [21]J. Sterbenz, D. Hutchison, E. Çetinkaya, A. Jabbar, J. Rohrer, M. Schöller and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines", Computer Networks, vol. 54, no. 8, pp. 1245-1265, 2010

TABLES

Table 1. Effects matrix per functional loss

Criteria to measure Severity			
LE	ES	NS	SI
Category of effects per criteria and functional loss			
50,000	**Non admissible**	50,000	**Non admissible**
20,000	50,000	20,000	50,000
5,000	5,000	5,000	5,000
0	0	0	0

Table 2. Effects severity matrix per functional loss, S_{ij}

Criteria to measure Severity			
LE (w_1=25%)	ES (w_2=20%)	NS (w_3=25%)	SI (w_4=30%)
Category of effects per criteria and functional loss			
25	**Non admissible:100**	**20**	**Non admissible:100**
15	20	10	30
5	10	5	15
0	0	0	0

Table 3. Calculation of frequency factors per selected functional levels

Asset	**f/y**
A	7
B	1
C	4
D	3
E	1
F	1
G	8
H	6

Asset	**f/y**	**Category (z)**	**% (z)**	af_z	ff_z
G	8	Very high	10%	8	8
A	7	High	25%	6.5	6.5
H	6				
C	4	Medium	25%	3.5	3.5
D	3				
E	1	Low	40%	1	1
B	1				
F	1				

Table 4. Criticality Categories for activities prioritation

Criticality level	% of assets	Criticality value interval	Area color in Figure 6 & Table 5
Critical	10	400–800	Dark grey
Semicritical	35	175-400	Grey
Not critical	55	0–175	White

Table 5. Criticality and Severity details per asset

Node Element	**Frequency**	Criteria to measure Severity														**Criticality**
		Loss Exposure (weight: 25%)			Legal Importance (weight: 20%)				Network Security (weight: 25%)			Strategic Importance (weight: 30%)			Severity	
	FE	tr	Total Risk	PE1	hES	Pacc	Total Risk	PE2	b	Total Risk	PE3	Strategic Customers	Total Risk	PE4	Total	
A	**6.5**	12	7,850.40	5	100,000	0.05	5,000	10	0.35	3,091	0	<3SLE	50,000	30	**45**	**292.5**
B	**1**	12	7,850.40	5	100,000	0.50	50,000	20	0.44	3,864	0	>10SME	5,000	15	**40**	**40**
C	**3.5**	15	26,317.03	15	50,000	0.10	5,000	10	0.00	0	0	<3SLE	50,000	30	**55**	**192.5**
D	**3.5**	12	7,850.40	5	5,000	0.01	50	0	0.13	1,159	0	>10SME	5,000	15	**20**	**70**
E	**1**	16	26,666.91	15	5,000	0.50	2,500	0	0.97	8,500	5	<3SLE	50,000	30	**50**	**50**
F	**1**	18	27,404.89	15	50,000	0.05	2,500	0	1.00	8,763	5	>3SLE	250,000	100	**100**	**100**
G	**8**	13	25,658.19	15	5,000	0.01	50	0	0.06	515	0	>10SME	5,000	15	**30**	**240**
H	**6.5**	14	25,980.60	15	250,000	0.10	25,000	10	0.22	1,932	0	>3SLE	250,000	100	**100**	**650**

FIGURE LEGENDS

AUTHOR BIOGRAPHIES (See also http://taylor.us.es/sim/)

JUAN FRANCISCO GÓMEZ FERNÁNDEZ is currently part of the Spanish Research & Development Group in Industrial Management of the University of Seville. He has obtained his PhD in Industrial Management from this University and awarded with the Best Master Thesis in Maintenance in Europe by the EFNMS. He has authored publications in journals such us Computers in Industry, Reliability Engineering and System Safety, International Journal of Simulation and Process Modeling, Journal of Quality in Maintenance Engineering, Journal of Management Mathematics, among others. Juan is the author of one book with Springer-Verlag in 2012 about maintenance management in network utilities. In relation to the practical application and experience, he has managed network maintenance and deployment departments in various national distribution network companies, both from private and public sector. He has conducted and participated in engineering and consulting projects for different companies, related to Information and Communications Technologies, Maintenance Management, and Outsourcing services in distribution network companies.

ANTONIO JESÚS GUILLÉN LÓPEZ is Industrial Engineering, University of Seville (USE), from 2004 and Master in Industrial Organization & Business Management (USE) from 2012. From 2003 to 2004 working for the Elasticity and Strength of Materials Group (GESM) of the USE as student-researcher in aeronautical materials tests. During 2005 and 2006 is Technical Manager of PHQ Company, concrete prefabrication SME. From 2006 to 2009 member of the Department of Electronic Engineering of USE, working in numerous public-private international R&D project, developing new thermo-mechanical design applications for improving the performance and the life cycle of power electronics system. From 2009 to 2010 is Project Manager of “Solarkit” project, representing Andalucia’s Government and USE in the international competition Solar Decathlon 2010. Is foundational partner of Win Inertia Tech., technological based company specializing in electronic R&D for Smart Grids and Energy Store fields, where he has carried out different roles, from R&D engineer to General Manager until September 2012. Nowadays is PhD student and contracted researcher in Intelligent Maintenance

System research group (SIM) of the USE, focusing his studies in Prognosis Health Management (PHM) and Condition Based Maintenance applications.

PABLO MARTÍNEZ-GALÁN FERNÁNDEZ is currently part of the Spanish Research & Development Group in Industrial Management of the University of Seville. He has been working in one of the main national electrical network companies and he is participating in consulting projects related to Maintenance Management with a leading company in the sector of Oil & Gas.

ADOLFO CRESPO MARQUEZ is currently Full Professor at the School of Engineering of the University of Seville, in the Department of Industrial Management. He holds a PhD in Industrial Engineering from this same University. His research works have been published in journals such as the International Journal of Production Research, International Journal of Production Economics, European Journal of Operations Research, Omega, Decision Support Systems, Computers in Industry, Reliability Engineering and System Safety or Quality and Reliability Engineering, among others. Prof. Crespo is the author of 5 books, the last three with Springer-Verlag in 2007, 2010 and 2012, about maintenance and supply chain management. Prof. Crespo leads the Spanish Research Network on Dependability Management and the Spanish Committee for Maintenance Standardization (1995-2003). He also leads a research team related to maintenance and dependability management currently with 5 PhD students and 4 researchers. He has extensively participated in many engineering and consulting projects for different companies, for the Spanish Departments of Defense, Science and Education as well as for the European Commission (IPTS). He is the President of INGEMAN (a National Association for the Development of Maintenance Engineering in Spain) since 2002.