Simulation in Information Systems: Potential of the vulnerability theory

Pedro Sá Silva[1], Jorge Pinto[2], João Varajão[2,3], António Trigo Ribeiro[1], Maria Manuela Cruz-Cunha[4, 7], Isabel Bentes[2], Humberto Varum[5], Jitendra Agarwal[6]

[1] Coimbra Institute of Accounting and Administration, Portugal
[2] University of Trás-os-Montes e Alto Douro, Portugal
[3] Centro ALGORITMI, Portugal
[5] Polytechnic Institute of Cávado e Ave, Portugal
[5] University of Aveiro, Portugal
[6] University of Bristol, U.K.
[7] CITEPE Research Centre, University of Minho, Portugal

Abstract. Systems simulation has been widely used in the last decades in order to analyze the impact of different scenarios in several areas, and its application to information systems in no exception. Analyzing information systems through simulation models is simultaneously much more affordable; it is required a smaller amount of resources and it is less disruptive with the real system. Since information systems are becoming a cornerstone for our society, a failure in these systems can have a huge impact. The theory of vulnerability identifies failures in which small damage can have disproportionate impact consequences in terms of the functionality of the whole system. This paper discusses the use of the theory of vulnerability in information system simulation.

Keywords: Simulation, modeling, vulnerability, information systems, failure scenarios.

1 Introduction

Our world is a wonderful, huge and complex system. It is a system because it has a set of entities interacting with each other in order to achieve some purpose [1-4]. It is complex because it has many entities interacting with each other at the same time and some of these interactions may be hard to represent through analytical models. It is huge because it incorporates many others subsystems such as health, business, education, transportation, political, among others, which may also include many others subsystems (ex: the transportation networks has the railway system, airway system, etc) and so on.

Simulation is used in many different contexts; its list of applications is wide because we can simulate any system in which it is possible to apply the concepts of simulation modeling [4]. Information systems (IS) are not an exception for applications of simulation. Di Domenica *et al.* [5] explained to the IS community how simulation models and their software realizations could be integrated with advanced IS and decision support systems tools [5].

A proper simulation can increase the performance quality of a process by rationalizing resources, reducing time consumption, decreasing costs [6-8] and reducing time-to-market [8, 9], fundamental aspects in the actual worldwide economic situation.

Our society is becoming totally dependent on information systems. For instance, today it is quite common that we entrust our banking information into the bank information system, however a breakdown or failure of these systems can have catastrophic consequences. IS reliability are more and more an area of interest on research and simulation about how a system can fail, and the identification of its impact consequences, contributes for a better understanding of that system [10, 11]. In this context, the theory of vulnerability can be extremely useful, as it is able to identify the vulnerable parts of a system, in which small damage can lead to disproportionate failure consequences [12]. The identification of the system's vulnerabilities enables system reliability [12].

This paper discusses how to apply the theory of vulnerability in the information systems context and highlights the inherent advantages. In section two, some important simulation concepts are presented, together with the presentation of simulation in information, followed by a brief description of the theory of vulnerability in section three. Then, the potential use of the theory of vulnerability in simulation is discussed and proposed in section four, and finally, section five draws some conclusions.

2 Simulation in information systems

There is still not a universal definition of simulation. Nevertheless, most of the existing definitions follow the same general concept that simulation is an imitation of a system [6, 13-16]. Systems imitation requires the construction of an artificial history based on the real system features [6, 14] that includes the system's dynamics and its behavior over time.

First of all, imitating a system requires a perfect understanding of it [7]. Putting "why" questions to comprehend how the system evolves and how the changes occur, allow predicting the impact of changes. By studying a system and constructing its simulation model will enable to explore new possibilities of achieving better performance without necessary committing resources acquisition [6, 7]. Simulation has revealed to be an excellent tool for the study of complex systems, whose analytical behavior modeling may be extremely complex.

Simulation has been used in many different contexts; practically, there are no boundaries, and it can be applied to any kind of system that fits modeling concepts. Manufacturing systems (optimization of production lines and logistics), public systems (emergency vehicle dispatch and weather forecast), military systems (warfare scenarios and training), transportations systems (railway network and air transportation), building industry systems (water pipe network, structures and electrical network), enterprise systems (financial and other business transaction processes) and computer systems (computer performance, computer networks and computer games) are some examples of possible applications [1, 2, 4, 14, 15].

2.1 Simulation basic concepts

The understanding of some based concepts like system, entity and resource is required in order to develop simulation models.

A system is a cluster of interrelated entities working together to achieve the same specific goal [2, 4, 14]. Systems are influenced by their environment. They receive inputs that cause systems changes and affect produce results (outputs). These changes are represented by state variables (in simulation vocabulary) and they define the system state in a certain period of time. In other words, system state variables contains the necessary data which together describe the system state in a particular moment on the simulation time [2, 6]. It is imperative for the analyst to know very well the system in order to identify correctly the system state variables.

An entity is an object or component that requires an explicit representation on the simulation model [6]. Clients and computers are examples of objects. Entities and their relationships define the system behavior Entities cause changes in the system state [13]. Each entity has its own characteristics or attributes. Attributes are identified characteristics (or qualities) from an entity that are very important to understand the entity role in the simulation [4, 13].

A resource is an object (or may be an entity) that has limited capacity [13]. Essentially, resources exist to serve entities and they can be many things such as machines, computers, workers and cars even entities. On the other hand, they are not always available to serve because they have states and limits.

2.2 Models

A model is a simplified representation of a system [4]. Simulation is a complex mathematical model that can be classified in: static or dynamic, deterministic or stochastic and continuous or discrete.

Static simulation models are used to represent systems only in a particular moment of time which means that time does not have an effect on the system [1, 2]. In contrast, in dynamic systems the time is fundamental because the system`s behavior is dependent of it [1, 2].

In deterministic or stochastic simulation models the main difference is related to the existence (or not) of probabilistic characteristics in the system [1]. When a system has probabilistic (i.e. random) components the model is stochastic, otherwise it is deterministic [2].

In a simulation model, it is analyzed how often the system`s state changes. In continuous simulation model, the system state changes continually over time, whereas in a discrete simulation model the system state only changes in some particular moments on time [2, 14].

2.3 Simulating information systems

Simulation applications areas are almost unlimited and the imagination of the analyst seems to be the only barrier [1]. Every system that fits into general simulation

concepts can be simulated. In IS, simulation has also an important role, like for instance, improving information workflow.

In general, an IS has entities and resources interacting to each other in order to manipulate information. By analyzing a new or an already existent IS through a model, the analyst can perform studies without changing the real IS itself. Figure 1 shows an example of a sales information system of a generic enterprise.

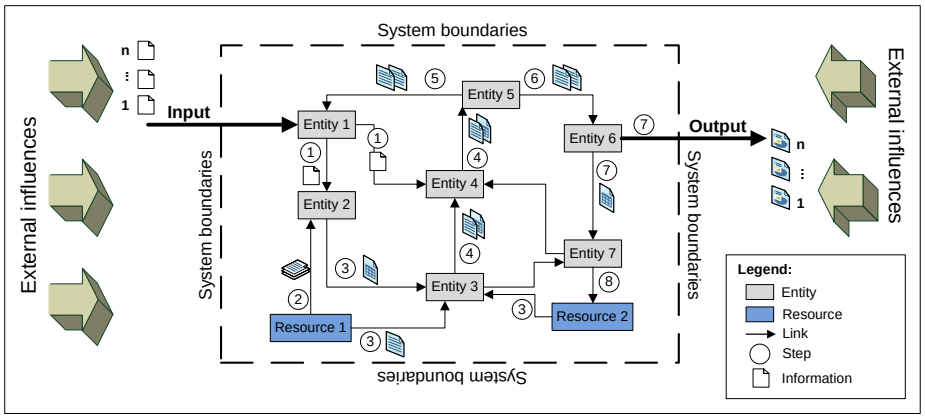


Fig. 1. Example of an enterprise information system

In the example in Figure 1, entities can be, for instance, workers, resources can be machines, and the arrows represent the communication links and information workflows (number near the arrow). Orders arrive into the enterprise information system by email and they are treated by different enterprise departments. Each department works based on the delivered information, adding eventually additional data to the initial order information. In terms of workflow, information may face several many different problems. Some of them may be related to entities (ex: missing person), to resources (ex: machine failure), to external environment (ex: international trade policies) or to communication channel (ex: without network). These influences may affect workflow and information in many aspects like quality, integrity, security, speed, among others. These aspects may be an excellent starting point of a simulation study.

Supposing that the study goal was to increase speed of order replies without adding new entities or resources, then some questions arise: could be simulation a good tool to answer this question? If yes, what would be the appropriated simulation model? If a system is too complex, then it is extremely difficult to model it through analytical methods and simulation may be a good alternative. In order to choose the appropriate model of a system, the analyst has to be aware of some relevant aspects such as the time influence, the probabilistic characteristics and the system behavior.

In this example, the system evolves over time (firstly a received order is processed, secondly that order is transferred to the correct department, as so on), thus the simulation model should be dynamic.

Information systems include human resources (entities) and this fact adds into the model an expressive degree of uncertainly. For instance, worker productivity varies

and changes over time. There are many other situations in which the only way of considering this uncertainty is by a statistical analysis. In general, when a system includes human decisions there is uncertainty.

The system's state changes over time. For instance, when the IS gets an order then the system is in a *busy* state. Otherwise, if there is no order the system is in an *idle* state. These characteristics are typical of a discrete simulation model.

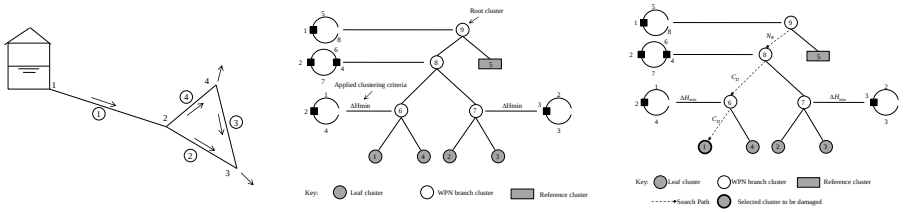
Based on the above analysis, we may propose that the type of simulation that is adequate to use in this example is the *discrete-event simulation* (DES). On DES, only when the system is in action it is important to the study, because it is assumed that nothing occurs outside these times [17]. The above example highlights that information systems can often be simulated using DES.

It should be possible to simulate IS aiming to answer one important question: what failures can cause major impact on the IS? The Theory of Vulnerability could help to answer to this question.

3 The Theory of Vulnerability

Traditionally, an analysis of demand and capacities has worked well for most of networked systems. However, with increasing complexity of systems and the changing nature of demands, that is no longer sufficient. There is a need to examine the impact of damage to a system. For this purpose, for structural systems a theory of vulnerability has been developed (see for example on [12, 18-21]). Meanwhile, recent research has lead to the application of the vulnerability concepts in several areas like for instance water pipe network systems (Figure 2) [22].

This is a theory of form and connectivity that is able to identify the vulnerable parts of a system. The concept of vulnerability is associated with the disproportionateness of the failure consequences in relation to the initial damage; thus a system is vulnerable when a small damage demand leads to a disproportionately large system failure. The action that may cause initial damage can be of any type including human error. These concepts are applicable to many systems [12].



a) Example of a WPN b) The hierarchical model c) The unzipping process

Fig. 2. Example of application of the vulnerability theory in the water pipe networks. Source: [22].

3.1 The basic theoretical concepts

A key concept in the proposed approach is to consider a system as a set of interacting objects. The objects are arranged in layers and connected together in an appropriate form. At the lowest level, a graph model represents the system in terms of nodes and links (Figure 2.b).

Clusters and rings. A cluster is a subset of the graph model in which the objects (links and joints) are in some sense more tightly connected to each other than to other objects outside of the cluster (Figure 2.b). A leaf cluster (or a primitive cluster) contains a single link and adjacent joints. A branch cluster is a cluster that contains more than one leaf clusters. A ring consists of two connected branch clusters or primitive clusters with the potential to allow the flow between two nodes. It can be an open ring or a closed ring depending upon whether the clusters are arranged in series or parallel, Figure 2.b.
A reference cluster is the source of the system. Total failure of the system occurs when there is a completely separation from all the reference clusters. The root cluster contains the entire system including the reference clusters.

Well formedness. The well formedness of a cluster is a measure of the quality of the form of the part of the system related to that cluster. Generally, it is related to (a) the properties of the links of the system, (b) the type of the joints of the system, (c) the configuration of the system gradients and (d) the connectivity of the network. Each type of system has a specific above factors.

Nodal connectivity. The nodal connectivity (η) of a branch cluster measures the connection of a branch cluster with the rest of the system. In other words, it captures the existing alternative flow paths between that branch cluster and the rest of the system. It also represents the likelihood of that branch cluster forming rings with the branch clusters of the rest of the system.

Deteriorating event. A deteriorating event causes an initial damage. It could be the result of any type of action which causes the loss of the capacity to flow to a node. Some of the possible actions are the collapse of the system either due to human error or design error and the degradation of flow quality, the latter being extremely important. An ordered sequence of deteriorating events forms a failure scenario of the system which decreases the performance of it.

Damage demand. Damage demand (E) is a measure of the effort required to cause a deteriorating event in the system.

Relative damage demand. Relative damage demand (E_r) of a system failure scenario is the ratio of the damage demand (E) of a failure scenario to the maximum possible damage demand (E_{max}) of a failure scenario in which deteriorating events occur in every system primitive clusters.

Separateness. Separateness (γ_r) is a measure of the failure consequence and it is calculated as the ratio of the loss in system well formedness of the deteriorated system to the well formedness of the intact system. Maximum separateness occurs when the system becomes disconnected from the reference cluster and that defines total failure. If the separateness of a failure scenario is equal to 1 then the system is unable to function. In contrast, if it is equal to 0 then the system is totally intact and it is able to work.

Vulnerability index. The system vulnerability index (φ) is a measure of the vulnerability of a system. It is calculated as the ratio of the separateness (γ_r) to the relative damage demand (E_r). It is a measure of the disproportionateness of the consequence (i.e. the separateness) to the damage. A large value of φ related to a certain failure scenario indicates that the system is highly vulnerable. The effort required to cause an initial damage and the resulting spread of damage may give guidance for the management of the system, for instance.

3.2 Application procedure of the theory

The application of the theory to a system consists of two main stages – a clustering process and an unzipping process. The clustering process results in a description of a hierarchical model of the system for use in the next stage. The unzipping process results in the identification of failure scenarios which are related to the vulnerable parts of the system.

Clustering process. The clustering process consists of a progressive formation of system branch clusters that are tightly connected. It starts at the lowest level by only using primitive clusters (i.e. the links and the adjacent nodes) and finishes, at the highest level, by having the whole system including the reference clusters. It is a selective process that requires clustering criteria to decide the next system branch cluster to be formed at each level of definition. These clustering criteria have to be defined for each system type.

Hierarchical model. A hierarchical model is an alternative representation of a system but one which is central to the vulnerability approach (Figure 2.b). However, the system elements (i.e. the joints and links) appear in this model according to the quality of the form of the system clusters resulting from the previously referred clustering process. The formation of a hierarchical model has to start from the bottom and then it moves up. New system branch clusters are formed during the clustering process and the respective primitive clusters used are clearly identified. Simultaneously, the system rings that represent these new system branch clusters and the clustering criteria used for the candidate selection are also shown. The part of the system that appears at the bottom of the hierarchical model has better form than the others parts appearing higher up in the hierarchy. This model is used during the next stage (i.e. the unzipping process) of the application of the theory.

The unzipping process. The unzipping process uses the hierarchical model of a system as the basis to search for the vulnerable failure scenarios in the system (Figure 2.c). The hierarchical model is unzipped from the top to the bottom focusing on all the existing system branch clusters. Each system branch is unzipped in turn by introducing deteriorating events until a system branch cluster or the whole system becomes totally inoperative. After every deteriorating event, the system branch cluster changes and, therefore, it becomes necessary to re-cluster and to define a corresponding new hierarchical model of the damaged system branch cluster. This indicates that the unzipping is an iterative process. An ordered sequence of deteriorating events resulting from this process defines a vulnerable failure scenario.
For the guided search of failure scenarios, the unzipping criteria have also to be defined for each type of system.

3.3 Failure scenarios

Through the unzipping process, several failure scenarios of a system are identified. Of these, the following are important. Total failure scenario is the one where least effort is required for the whole system to become inoperative. Among the identified failure scenarios with separateness equal to 1, the total failure scenario is the one that has highest value of vulnerability index (φ). Maximum failure scenario is the one that results in maximum damage from the least effort. Among the failure scenarios found, the maximum failure scenario is the one that has the highest value of φ. The maximum failure scenario is related to the most vulnerable part of a system. Minimum failure scenario is related to the least well formed part of a system and, in general, corresponds to the last leaf cluster to be clustered in the clustering process. Minimum demand failure scenario is related to the weakest part of a system to suffer damage. It corresponds to the leaf cluster that has the smallest value of damage demand. An interesting failure scenario is the one in which the designer is specifically interested for local reasons such as sensitivity to particular usage.

Knowing the vulnerable parts of a system is then possible to mitigate them and, consequently, to contribute to achieve a better robust system solution. The theory can be applied during the process of creating a new system or, alternatively, during the maintenance or management processes of existing systems.

4 Potential use of the theory of vulnerability in simulation

Simulation allows a better understanding of a system in terms of function and behavior over time. It also allows analyzing alternative actions in order to anticipate impact changes. The theory of vulnerability analyzes the impact of damage in a system focused on the disproportionateness failures consequences. Its main purpose is to help identifying weak links inherent of a system [12].

Simulation and theory of vulnerability have both the same main purpose: to study the system in order to improve its functionality. While simulation does not have a predefined study goal, vulnerability theory has a particular key point of study: to

identify actions that produce large disproportionate consequences to the system. By having only one particular goal of study does not mean that it is simple to achieve because it may be interrelated with other aspects (ex: security, performance, maintenance, among others). Currently, this theory has been especially applied in the water pipe networks. In Agarwal [12] there is a first step to extrapolate some of the main theoretical concepts of the theory to different types of systems. Table 1 includes some of results based on that research work; it compares water pipe networks and organizations type systems.

After the simulation concepts and the theory of vulnerability being introduced, using the example of Figure 1 and the information displayed in Table 1, it is evident that it is possible and useful to extrapolate the theory of vulnerability to the simulation of information system context.

Is it possible to build a simulation model to imitate damage events? Simulation main concept is to imitate any system (that fit on simulation concepts) and the theory of vulnerability gives a goal to the simulation (points of failure). Both techniques share the same first step and perhaps the most important: understand the system behavior. More the analyst knows about the system better will be the study conclusions. After understand the system behavior, comes the system representation. In theory of vulnerability the system is represented through a graph model, i.e. in terms of nodes and links [21], and in simulation there is not a pattern form. After the representation of the system through graph model comes the theory specifications: clustering and unzipping process. In those processes simulation may represent an interesting tool, especially on introduction of deteriorating events in the unzipping process. To achieve study goals the theory already gives the failure analysis process.

Table 1. Water pipe networks *versus* Information Systems

System	Water pipe networks	Information Sytems
Function (purpose)	Carry water without much loss of pressure	Manipulate information
Source	External supply, reservoir	Entities and Resources (need to exchange information)
References	Points of in-flow (out-flow not important)	Every node may be a reference
Damage event	Link cut	Communication failure between any two nodes
Partial failure	Some nodes do not get supply or sufficient pressure	Some links failed but mission can still be achieved
Total failure criteria	No nodes can get supply of water	Overall mission cannot be achieved

After building the simulation model according to this theory, simulation may be performed several times (those necessary to take valid conclusions) to identify the range of failure injection. Then the analyst can identify and study the failures that would create disproportioned failures in the system.

Figure 2 in section 3, briefly illustrates the application of the vulnerability theory in the water pipe networks (WPN) in which a water pipe network system made of four pipes (links) and four joints (nodes) is used as an example (Figure 2.a) [22]. The hierarchical model of the WPN resulted from the clustering process is shown in Figure 2.b. Meanwhile, the first step of the unzipping process is shown in Figure 2.c.

5 Conclusion

In this paper were presented the basic concepts of simulation as well as a brief description of the theory of vulnerability. The concept of vulnerability is associated with the disproportionateness of the failure consequences, in other words, a system is vulnerable when a small damage demand leads to a disproportionately large system failure. Based on graph model, this theory represents the system in terms of nodes and links. This theory can be very useful in the context of information systems simulation. As further work it is purposed to explore and extend this theory to IS context which can help to target its vulnerability.

References

1. Gogg, T.J., Mott, J.R.A.: Introduction to Simulation. Simulation Conference Proceedings, 1993. Winter (1993) 9-17
2. Law, A.M., Kelton, W.D.: Simulation Modeling and Analysis. McGraw-Hill Higher Education (1991)
3. Sanchez, P.J.: Fundamentals of simulation modeling. Simulation Conference, 2007 Winter (2007) 54-62
4. Seila, A.F.: Introduction to simulation. Simulation Conference Proceedings, 1995. Winter (1995) 7-15
5. Di Domenica, N., Mitra, G., Valente, P., Birbilis, G.: Stochastic programming and scenario generation within a simulation framework: An information systems perspective. Decision Support Systems **42** (2007) 2197-2218
6. Banks, J.: Introduction to simulation. Simulation Conference Proceedings, 2000. Winter, Vol. 1 (2000) 9-16 vol.11
7. Carson, J.S., II: Introduction to modeling and simulation. Simulation Conference, 2005 Proceedings of the Winter (2005) 8 pp.
8. Whicker, L., Bernon, M., Templar, S., Mena, C.: Understanding the relationships between time and cost to improve supply chain performance. International Journal of Production Economics **121** (2009) 641-650
9. Latorre, S., Pointet, J.-M.: The contributions and consequences of simulation tools and digital mock-ups on design and production as applied to the automobile and aeronautics industries. International Journal of Automotive Technology and Management **8** (2008) 350-368
10. Kosmidou, K., Zopounidis, C.: Predicting US commercial bank failures via a multicriteria approach. International Journal of Risk Assessment and Management **9** (2008) 26-43
11. Docherty, P., Wang, G.: Using synthetic data to evaluate the impact of RTGS on systemic risk in the Australian payments system. Journal of Financial Stability **6** (2010) 103-117
12. Agarwal, J., Blockley, D.I., Woodman, N.J.: Vulnerability of systems. Civil Engineering and Environmental Systems **18** (2001) 141 - 165

13. Ingalls, R.G.: Introduction to simulation. Simulation Conference, 2008. WSC 2008. Winter (2008) 17-26
14. Banks, J., Carson, J.S., Nelson, B.L.: Discrete-Event System Simulation. Prentice Hall (1996)
15. Robinson, S.: Simulation: The Practice of Model Development and Use. Wiley (2003)
16. Goldsman, D.: Introduction to simulation. Simulation Conference, 2007 Winter (2007) 26-37
17. Giaglis, G.M.: A Taxonomy of Business Process Modeling and Information Systems Modeling Techniques. International Journal of Flexible Manufacturing Systems **13** (2001) 209-228
18. Lu, Z., Yu, Y., Woodman, N.J., Blockley, D.I.: A theory of structural vulnerability. The Structural Engineer **77** (1999) 17-24
19. Pinto, J.T.: The risk of a vulnerable scenario. PhD thesis, University of Bristol, UK (2002)
20. Pinto, J.T., Blockley, D.I., Woodman, N.J.: The risk of vulnerable failure. Structural Safety **24** (2002) 107-122
21. Agarwal, J., Blockley, D., Woodman, N.: Vulnerability of structural systems. Structural Safety **25** (2003) 263-286
22. Pinto, J.T., Varum, H., Bentes, I., Agarwal, J.: A Theory of Vulnerability of Water Pipe Network (TVWPN). Water Resources Management (2010). (available online at http://www.springerlink.com/content/x0240l6077428716/)