Annals of the Academy of Romanian Scientists
Series on Science and Technology and Information
Online ISSN **2066- 8562** Volume **13**, Number 1/**2020**

ANTIFRAGILE DESIGN OF SELF-IMPROVING SYSTEMS

Radu DOBRESCU[1]

Abstract. *The purpose of this paper is to highlight how the concept of antifragility can be introduced in the design stage of self-improving systems, considered as complex adaptive systems capable of maintaining the functionality at optimal parameters under adverse conditions caused by unforeseen changes in context. Assuming that an antifragile system not only maintains its robust behavior when faced with stressful and harmful events, but even benefits to optimize its performance, the paper offers a detailed description of the features that must be ensured when designing a self-improving system.*

Keywords: antifragile, resilience, robustness, self-improvement, complexity, self-adaptive, context-aware, uncertainties, decision-making.

2. Introduction

Antifragility is a concept introduced and developed by Nassim Nicholas Taleb in his book “Antifragile: Things That Gain from Disorder” [1]. The term “antifragility” appears about 5 years after Taleb made a "revolution" in the way of referring to rare, unlikely events, which he calls "black swans" and which he defines through three essential characteristics: 1) they are difficult to predict, almost impossible; 2) they are easy to explain in retrospect, that is, after they have been reported; 3) they have a very pronounced impact in different environments of high complexity. Taleb points out that "black swans" cannot be characterized stochastically by Gaussian distributions, because they are far from average. Although these events can have a positive impact on the evolution of processes, usually by contributing to the stabilization of feedback loops, and thus leading to increased robustness of the process, there are situations where the effect is opposite and may lead to systems "weakening" due to unwarranted trust leading to the neglect of safety policies. To use only positively the impact of black swans, Taleb introduces the concept of antifragility as an alternative design criterion for a system with a high degree of robustness. In short, antifragility refers to systems that improve their behavior when subjected to exaggerated and slightly plausible parameter changes. Another important difference is that an antifragile system acts preventively, before the critical event occurs, while a robust system focuses on

[1]Prof., Faculty of Automatic Control and Computers., Univ. “Politehnica” Bucharest, Romania
Correspondent member of the Academy of Romanian Scientists

adapting "a posteriori", which often becomes late. According to Taleb, antifragility is more than robustness (the ability to withstand or overcome adverse conditions and therefore to recover from failure) and more than resilience (the ability to resist failure). In other words, the concept of antifragility is that certain things can improve and even grow stronger when subjected to stress.
Two years after the appearance of Taleb's book, Vincenzo De Florio publishes a work that somewhat systematizes the means by which an antifragile system can be designed, formulating an equation that has won its celebrity: "Antifragility = Elasticity + Resilience + Machine Learning" [2]. This paper proposes a scheme capable of self-optimizing system processing using a machine learning step which succeed to enhance the ability of the system to adjust to adverse environmental conditions, so arguing that an antifragile system may correspond to systems able to learn while running resilient strategies. What is important in this approach is the idea of self-optimization of the process in hostile environmental conditions, an idea resumed in another paper [3]. After this first step, several researchers offered various implementation solutions for antifragile systems. Most of the time these solutions have been associated with the technological progress achieved through techniques borrowed from Artificial Intelligence area, in particular Multi-Agent Systems, Machine Learning and Neural Networks. The essential property of these systems is the capability of self-organization, which favors emergent behaviors that face the unexpected changes in the context in which the system works.

This paper proposes a methodology for designing a context-aware adaptive control system capable of improving its performance under adverse and stressful conditions, that is, having the property of self-improvement and therefore called Antifragile Self-Improving System (ASIS).

2. Conceptual definition of antifragile self-improving systems

Although we have stated that an antifragile system is more than robust and resilient, it must be primarily robust (to maintain its normal operating parameters in the presence of disturbances) and resilient (to be able to return to its original state when its operation mode is altered). But he must be even more than that - to improve his performance in stressful conditions. An antifragile system is based on the fragility of its components, meaning that it must be able to get rid of those components that can fail quickly and to resort to alternative components that are better adapted to the impact of uncertainties due to unforeseeable context changes. Therefore, an antifragile system must be a complex adaptive system that is capable of limiting the impact of surprising incidents.
Conceptually, a self-adaptive system has two main components - one that ensures functionality (for which the system was developed, including control procedures

for normal condition) and another that ensures adaptive management (for achieving the goals under changing conditions). Most approaches reported in the literature focus on the first component, proposing solutions for realizing key *self-functionalities*. Thus, the paper [4] focuses on *self-configuration*, proposing a framework for selecting and configuring network parameters based on the requirements of the application quality service quality (QoS), which subsequently adapts the configuration during running to constantly satisfy changes. dynamics of these requirements. The paper [5] presents an executable model for testing *self-healing* behaviors under uncertain conditions, as well as a methodology for specifying test models that capture both expected functioning behaviors and the response to the negative effect of environmental uncertainties. The paper [6] proposes a monitor of analysis, learning, planning and execution for the exercise of the *self-protection* function in cyber-attacks and at the same time a knowledge base that assures the assistance of a self-adapting module of cyber-physical type, which activates in an industrial environment and generates alarms and warnings regarding any kind of anomalies or threats. In [7] the authors discuss a *self-optimization* control solution that ensures minimizing the deviations from the nominal operating parameters due to the disturbances, by maintaining the selected controlled variables at constant set values. The optimization is carried out in two stages, because after selecting the optimal parameters, a combination of the measured values in the feedback loops generates a control strategy that ensures the further reduction of losses.

However, many authors tend to ignore the need for self-management adaptation mechanisms. There are two reasons to build adaptation mechanisms: 1) The basic resilience addresses the dynamics of how a system absorbs the impacts of stress or shocks, so focusing on system reactions to randomness. 2) Fragility must be excluded from the generic system types as they break from randomness and, hence, do not provide the desired robustness. The manner in which a resilient system returns to its original state after randomness is doubled by the manner in which an antifragile systems deals with disturbances, absorbs the impacts of stress or shocks, and how it reorganizes afterwards. Its recovery process is based on self-organization, a mean to learn from different circumstances and to adapt its capacity towards future stressors. This means that the design of a resilient system (named in the following resilience engineering) builds up redundancy, which allows the system to survive future similar stressors.

Differently from the common resilience engineering which creates knowledge based on what events to expect and the prevention of the unexpected events, antifragility engineering considers mechanisms able to learn and adapt to the real unexpected circumstances. In summary, in Table 1 are presented properties and definitions of resilience and antifragility, in order to demonstrate their similarities

and differences, proving that antifragility is a superior type of resilience, in the most advanced form.

Table 1

Resilience	Antifragility
Characterized by low vulnerability to perturbations. Is the "ability of the systems to absorb changes of state variables, driving variables, and parameters, and persist"	It not only resists the ravages of time but become able to cope with an unpredictable future, through the creation and recombination of novel components.
Positive end of the distribution of developmental outcomes among individuals at high risk	Presents emergence properties related to the self-organized behavior of Self-adapted Complex Systems
Dynamic process encompassing positive adaptation within the context of significant adversity	Provides sufficient response to uncertainty together with a process of learning for building a knowledge repository from tough experiences
Resilience requires a constant sense of unease that prevents complacency	While resilient is neither harmed nor helped by volatility and disorder, the antifragile benefits from them.
Resilience enables the system to cushion the effects of unforeseen disturbances by absorbing the shock and adapting to changing conditions	Being antifragile means being able to grow despite the crises that might arise. It represents a mix of adaptative and absorptive capacity, fostered by innovation and learning capabilities
Capability of organization related to adaptive practices that lead the system to higher levels of efficiency	Stronger through learn fostered by resilient strategies, is rewarded with good results and protected from adverse events

We can therefore consider antifragile engineering as a superior form of robust and resilience engineering, related to the idea of dynamic balance, in which the systems change and evolve when disturbed by changing the state after stress. In this direction, mechanisms of adaptation, self-organization and self-improvement are responsible for enabling systems to learn and improve on past situations, in order to take better advantage in future ones.

3. Knowledge acquisition in ASISs.

Learning becomes essential to offer the knowledge necessary for decision making under uncertainty. In [8] is described a model of the repartition of knowledge, in a four-quadrants representation as shown in Fig. 1.

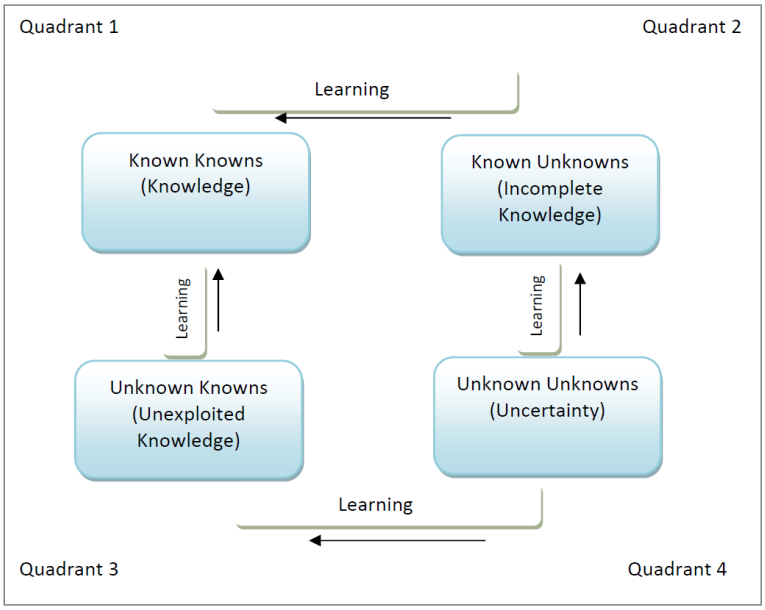

Figure 1. Four-quadrants knowledge model (after [8])

It should also be mentioned that the mere classification of information according to the specificity of each quadrant is not sufficient. As the information changes due to the changes that appear in the context, the ones that are used in the decision process are no longer information (in the position of interpreted data), but knowledge (in the position of information with meaning). Because "information" and "knowledge" may have different meanings depending on the context in which they are used, the learning process through which the decision-maker's expertise is to be improved must be doubled by an informative process, which requires a prior understanding along with the interpretation of the results of which is structured knowledge. However, we cannot really speak of knowledge as an object independent of any subjective holder, because the meaning is still determined by the subjectivity of the decision maker. Complete automation of the decision (for example on the basis of consensus) reduces this subjective side until the annulment, but it still remains questionable whether the significance should always be considered by the receiver to meet the transmitter's constraints.

4. Self-Awareness in ASISs

ASISs are complex systems that must adapt during running, as a response to external (context) changes, with the goal of improving performance. At the same time, an ASIS is pursuing another important goal, self-awareness. We have shown in the previous section the essential role of learning in a process of acquiring knowledge, and the importance of using comprehensive models that contain both their own functioning process and the interaction process with the environment. This approach takes into account both the dynamic nature of the objectives and the continual nature of the learning processes needed. It is precisely the characteristic of self-awareness that allows the detection of gaps in the knowledge bases and the completion with preemption of these gaps before the occurrence of the situations in which the respective knowledge is necessary for making appropriate decisions. This situation is much complicated when several context-aware systems (through specific means of interaction: cooperation, competition, synergy) are linked together with several operating systems with different architectural structures (hierarchy, peer-to-peer, heterarchy, stigmergy). In this situation the priority in completing knowledge must belong to the cooperative systems of self-awareness, which are in the first line of the changes of measured values, and which must ensure self-integration dynamically into learning processes. By formalizing each knowledge space with highlighting both acquired knowledge and existing gaps, particular rationing mechanisms can share both individual knowledge bases and those of other context-aware systems.

Fig.2 shows an architecture for a context-aware system able to be associated with any ASIS, regardless of the nature of the industrial process (production, manufacturing, transport, etc.) for which it is desired to obtain an antifragile behavior.

The structure of the system is a hierarchy distributed vertically on three levels. At the lower level it is placed the Context Sensing Module, which collects data provided by both application sensors (User sensors) and context sensors (Environment sensors). In addition, a mechanism for analyzing User requirements is included at the same level, which in this way can provide a set of preferential scenarios.

The medium level contains a Context Information Management (CIM) module. CIM has two associated subsystems, namely the subsystem of the context database, which stores the data provided by the module at the lower level, and a subsystem of contextual reasoning, which offers a decision-making mechanism, which uses a classical inference technique. based on rules of artificial intelligence.

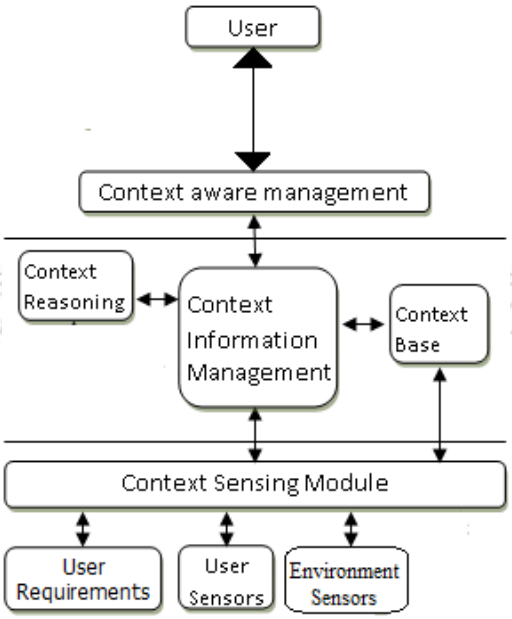

Fig.2. Block scheme of the Context-aware system

In the database we find three categories of contextual information: static, transient and persistent. Static information is invariant and is kept unchanged - it corresponds to the KK module of the knowledge model in fig.1. The content of the transient data is updated in real time, as the application runs. Persistent information is historical data, which can be replaced when they become outdated or are considered irrelevant. In the current application, adaptations are made both on the basis of transient data, and on historical data grouped over time series that are processed by predictive algorithms capable of identifying hidden patterns in the controlled technological parameters or self-similarity indicators in the informational flow which corresponds to the technological process. The contextual reasoning module periodically interrogates the contextual database to generate a set of relevant information, which are interpreted by an inference engine to produce appropriate setting values.

At the top of the hierarchy is placed the Context-aware Services Management module, which corresponds to the user's requirements. This module processes information from the data and knowledge bases of the middle level in order to model, generate and validate context-aware adaptive behavior.

Conclusions

In this paper, we presented our opinion on how to achieve antifragility in complex adaptive systems with self-improvement. In particular, we have argued that the property of self-improvement can be achieved by simultaneously achieving two other objectives: the realization of a learning subsystem that will allow the structuring of knowledge and its classification into categories, so as to ensure the necessary expertise for real-time decision making. For each of the designed subsystems, functional models with multilevel hierarchical structure have been presented, which allow for a multi-objective optimization, with the mention that at each level of information processing we must on the one hand to optimize the production process itself, by providing robust control procedures, and on the other hand optimizes the management process (more precisely self-management) through which antifragility is achieved. These characteristics represent a challenge and also an incentive for the research community to find advanced processing procedures compatible with the ASIS design framework proposed in the paper that will enhance the operating mode with the uncertainties.

R E F E R E N C E S

[1] Taleb, N. Antifragile: Things That Gain from Disorder. Random House, 2012

[2] De Florio, V. Antifragility=elasticity+resilience+machine learning models and algorithms for open system fidelity, Procedia Computer Science, vol.32, pp. 834-841, 2014

[3] De Florio, V. On resilient behaviors in computational systems and environments. Journal of Reliable Intelligent Environments, Vol. 1, Iss. 1, pp. 33-46, 2015

[4] Shi, J. and Sha, M. Parameter Self-Configuration and Self-Adaptation in Industrial Wireless Sensor-Actuator Networks, Proceedings of IEEE Conf. on Computer Communications, pp. 658-666, 2019

[5] Tao, M., Shaukat, A., and Tao, Y. Modeling foundations for executable model-based testing of self-healing cyber-physical systems, Software and Systems Modeling, Vol. 18, Iss. 5, pp. 2843-2873, 2019

[6] Elgendi, I., Hossain, F., Jamalipour, A., and Munasinghe, K. Protecting Cyber Physical Systems Using a Learned MAPE-K Model, IEEE Access, Vol. 7, pp. 90954-90963, 2019

[7] Klemets, J. R. and Hovd, M. Accounting for dynamics in self-optimizing control, Journal of Process Control, Vol. 76, pp. 15-26, 2019

[8] Baruwal Chhetri, M., Uzunov, A., Nepal, S. and Kowalczyk, R. Self-Improving Autonomic Systems for Antifragile Cyber Defence: Challenges and Opportunities, Proceedings of the IEEE Int. Conf. on Autonomic Computing, pp. 18-23, 2019.