sustainability

MDPI

Article

Holonic Crisis Handling Model for Corporate Sustainability

Levente Bakos [1,2,*] and Dănuț Dumitru Dumitrașcu [1]

[1] Management and Industrial Engineering Department, Lucian Blaga University of Sibiu, 550024 Sibiu, Romania; dan.dumitrascu@ulbsibiu.ro

[2] Mechanical Engineering, Sapientia Hungarian University of Transylvania, 400112 Cluj-Napoca, Romania

* Correspondence: bakos@ms.sapientia.ro; Tel.: +40-721-208-954

Received: 2 November 2017; Accepted: 4 December 2017; Published: 7 December 2017

Abstract: The new approaches of risk and crisis management of organizations point to corporate responsibility and corporate sustainability. In the 'Internet of Everything' era, when the new media and social networks create the possibility to ruin in a few seconds the reputation of a company built in decades, it is important to afford the maximum attention to risk management and crisis communication. Long-term sustainability requires a transparent, trustful communication in due time. In our study, we propose a crisis management model that leads to sustainable corporate behaviour. We consider organizations as complex systems, and we use the holonic multiagent modelling concept to depict the emergent behaviour of these systems. This theoretical paper has as its main result a crisis communication model, based on the adaptability feature of holons. In our non-linear approach for unpredictable situations we merged some findings of sustainability theory, corporate social responsibility (CSR) management, crisis communication, the holonic manufacturing concept and the latest security standards in computer communication.

Keywords: crisis communication; holonic concept; risk management; corporate sustainability

1. Introduction

Crisis situations at the firm level, regardless of the size of the organization, have a major impact on its future economic development. There is no crisis without economic damages and it is difficult to conceive a crisis situation without some social consequences. Unfortunately, many crisis cases in industry have environmental consequences, too. Definitely, during crises the organisations must deal with the three main sustainability spheres—economic development, social development, and environmental management (the so called triple bottom line of sustainability). Thus, risk assessment must consider the links between organization and society, and it has to account for their interdependence. As stated in the United Nations Global Compact Guide to Corporate Sustainability: "Assessing risks is a crucial step to implement corporate sustainability successfully, decrease the exposure to various risks and avoid costly damages" [1]. We will use Bergman's recent definition to corporate sustainability, considering it as a "systematic business approach and strategy that takes into consideration the long-term social and environmental impact of all economically motivated behaviours of a firm in the interest of consumers, employees, and owners or shareholders" [2]. In our approach, sustainability means also quick reactions during crises to all stakeholders' concerns. This is because crisis situations have significant influence on the relationship between the business and society. Risk and crisis management methods and models try to prepare an organization for unexpected events. It is in fact impossible to illustrate by computer software, or any other way, the complexity of an organization. Any model is simplification or reduction of real phenomena. Even so, researchers of different sciences developed different types of models in order to depict how an organization might work and prepare for the unexpected. Planning, designing, trend analysis, risks evaluation and many other scientific reasoning have as their ultimate

goal to prepare how an organization might behave in the future. This behaviour must be sustainable on a long-term basis in financial, environmental, social and ethical terms. The objective of our paper is to present a conceptual model based on a holonic concept. We will stress out the necessity of human-machine cooperation, the necessity to handle the human-machine and human-human communication under the same pattern. This communication must be transparent; transparency builds trust and trust is crucial for sustainability. We use a multidisciplinary approach taking and merging ideas from different sciences and theories, especially from software engineering, complexity theory, project management, multi-agent theory and public relations.

2. Origins and Characteristics of Corporate Sustainability

From an academic point of view the study of corporate sustainability over the last 50 years evolved from a few primary studies into an exponentially growing number of articles and researches after the 1990s [3]. Linnenluecke & Griffiths show that actually there are five conceptual genealogies: (1) corporate social performance theory, (2) stakeholder theory, (3) a corporate social performance versus financial performance debate, (4) a greening of management debate, and (5) marketing aspects (considered as an additional stream, not related to the triple bottom line of sustainability). From practical point of view the corporate sustainability is related to strategic management, social responsibility and public relations. Generally speaking, the idea of sustainability in the mind of the average manager is to balance goals and needs of the current activities with the long-term objectives. Today, corporate sustainability is a result of long evolution of ethical corporate practice. From this point of view is somehow the extent of the corporate social responsibility (CSR) concept and it is a market-oriented sustainability. Even if CSR and corporate sustainability are used many times as synonyms there are generally accepted fine distinctions between them. Usually, it is considered that sustainability targets a wider stakeholder range (from suppliers to end consumers) while CSR targets mostly the opinion leaders and media. The CSR is more related to Public Relations and is driven by the compliance to the (short term) expectations or to protect reputation. That is why CSR is managed usually by communications practitioners. Sustainability is slightly more related to strategic management, environment issues and (long term) operations. Sustainability issues are usually handled by the managers and by the marketing staff. We do not intend to put on opposite sides CSR and sustainability, because CSR can be considered one of the mechanisms for corporate sustainability and it is part of the social aspect of sustainability. We agree with Porter and Kramer [4] when they state that there is a strong link between competitive advantage and the CSR activities. There is an interrelation among the social influences and competitiveness of company. In other words, Porter and Kramer demonstrate that companies should operate in ways that secure long-term economic performance by avoiding short term behavior that is socially detrimental or environmentally wasteful. Corporate social responsibility means, among other things, a moral obligation for sustainability; it is a kind of license to operate given by the society. It influences the reputation and the goodwill of the organization. Sustainability emphasizes environmental and community stewardship.

Gandini et al. in [5] investigate the relationship between strategic and corporate complexity, global responsibility and risk management. In their findings, there is a relationship between the complexity of the organization, sustainability and risk control. In Figure 1 we show this relationship.

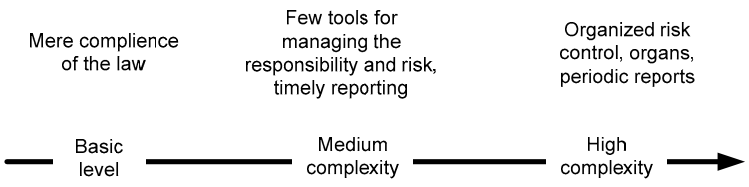

Figure 1. Company complexity and risk control (Source: [5]).

In [5] there is presented a conceptual framework in order to define the essential conditions for companies' global success and an effective and equitable management. Among their conclusions we find that it is not possible to predetermine a priority order among the dimensions of responsibility, because the relationship between the principle of profitability and sociality is mutual.

3. Complex Systems and Multiagent Models

In order to understand how an organization behaves in crisis situations we must understand its complexity. Traditionally, sciences like engineering, management, medicine and many of the social sciences have been trying to study the complexity of organizations. Recently, multiple simulation models were developed by computer sciences to depict the behaviour of complex systems.

Complex systems are somewhere in the middle among simple, ordered systems (for example a bicycle, the tax system, mathematics) and chaotic systems (for example the atmosphere, the movement of molecules, the stock market). In Figure 2 we briefly present how complexity evolves along different types of systems.

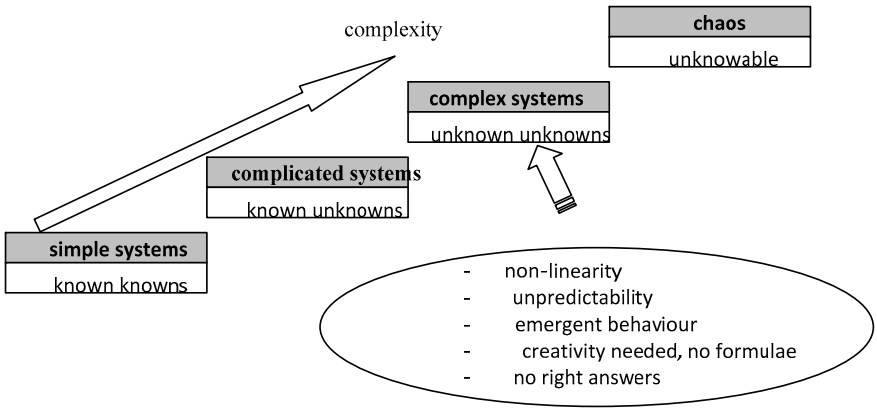

Figure 2. The evolution of complexity (Source: authors).

The simple and the complicated systems have a predictable behaviour, even during crisis situations. These systems can be handled by a deterministic approach: if there is a risk occurrence, then there is a readily prepared solution for it. In the case of complex systems, knowing the constituents of the system does not suffice it to describe how the system works or how it will behave in future. There will be unexpected collective behaviours of such systems, which are called "emergent". This emergent behaviouris crucial during crises, when we must deal with "known" and "unknown" unknowns.

We refer here to a now famous quote of the former American state secretary Donald Rumsfeld ("there are known knowns . . . , but there are also unknown unknowns—the ones we don't know we don't know" a phrase from a response of Donald Rumsfeld at a news briefing on 12 February 2002). The most difficult events are the totally unexpected "unknown unknowns". As Bar-Yam states: "Tounderstandthebehaviourofacomplexsystemwemustunderstandnotonlythebehaviour of the parts but how they act together to form the whole" [6]. This emergent, and unpredictable, behaviour must be handled during crisis situations when quick reaction time is needed and the wrong reactions would have major consequences to the negative. Public Relations practitioner experience and academic research set clear guidelines for the initial crisis response: (1) be quick, i.e., in the first hour after the crisis occurs, (2) be accurate, and (3) be consistent [7].

Computer sciences study complex adaptive systems by using the agent concept. There is no universally excepted definition of agents, but the most cited definition is related to Michel Wooldridge, one of the most known researchers of the multiagent theory: "An agent is a computer system that is situated in some environment, and that is capable of autonomous action in this environment in

order to meet its design objectives" [8]. Multiple and interacting agents form a computerized virtual structure called multiagent system (MAS). These intelligent agents act within an environment and can solve multiple technological, organizational and other problems. Multiagent systems show how software engineers and IT specialists see the world. Sometimes, their binary logic or the "If . . . then" based thinking simplify the real decisional situation and lead to acceptable solutions. But sometimes this approach is the reason why MAS cannot solve emergent problems. Among the large number of MAS concepts we pick up a special type, the Holonic Multi-Agent System concept, applying it to develop a sustainable risk management algorithm. This is connected to holonic philosophy. In holonic philosophy we can find two important figures: Arthur Koestler, a British-Hungarian author, and the Nobel Prize winner economist Herbert Simon. Based on some observations on social and biological systems, Koestler, in his book "*The Ghost in the Machine*" [9] proposes a concept with entities that are "wholes" and "parts" at the same time. The term *holon* coined by Koestler comes from the Greek *holos* (whole) and *-on* is a suffix, meaning "particle" (like in prot*on* neutr*on*, etc.).

The holons, being parts and wholes at the same time, are building blocks of a larger system, called *holarchy* (a notion also coined by Koestler; here the suffix '*archy*' means a rule or a government) that presents stability in changing environments. The secret of this stability relies on the observation that complex systems evolve better if their components are stable entities. The holons are autonomous self-reliant units and may act without the permission or instructions of higher authorities. For example, they act like soldiers do when they are lost behind the enemy lines in the battlefield. When the connection with headquarters is lost, the soldiers will do anything they can to return to their side and meanwhile to cause as much damage as they can to the enemy. They will do this without any permission and instruction from the higher authority. In warfare soldiers do what they previously are trained to do.

Koestler's holonic concept, in its initial form, had nothing in common with technical sciences. The Holonic Manufacturing System (HMS), based on Koestler's concept, arose two decades after his findings, in the early 1990s. These early achievements of the Holonic Manufacturing System concept were exhibited by James Christensen, of Rockwell Automation (one of the initiator partner companies of the HMS Consortium), in a state of art presentation [10], and more recently, in a similar review, by Babiceanu and Chen [11]. In other multiagent systems, the agents are totally autonomous and independent entities. Agents form so-called heterarchical systems, composed by unranked elements, characterized by extreme robustness against disturbances, but sometime with unpredictable behaviour. An HMS is expected to "combine the high and predictable behaviour of the classical hierarchical systems with the agility of the heterarchical systems" [12]. This way, holonic systems are more likely to emerge and survive in dynamic environments, but also they are more reliable than other artificial adaptive systems. Figure 3 shows the middle position of holonic systems between traditional organizations and the multi-agent concept.

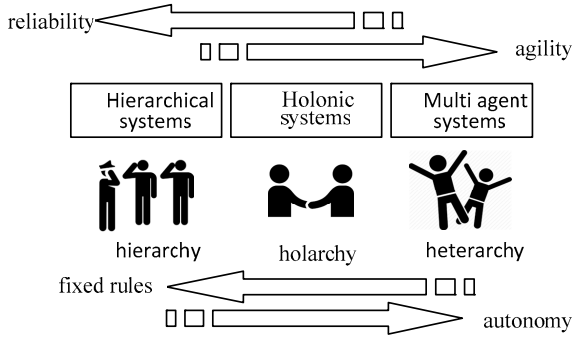

Figure 3. Comparison of the holonic, hierarchic and heterarchic systems (Source: authors).

Holarchy is a loose-coupled nested hierarchy, in which holons can enter and exit according to their will. Being able to negotiate, the holons find solutions for their problems by themselves and they are fault-tolerant. The autonomy gives the holon the capacity to cope with changes, uncertainty, and disturbances in its environment. This ability allows them to handle unpredictable situations.

In practice, the engineers and computer scientists translated Koestler's concepts into a set of appropriate concepts for manufacturing. Here the holons are building blocks of a manufacturing system for transforming, transporting, storing physical objects and/or validating information. The holons are not necessarily just simple software agents; they might consist of two parts, an information processing part and a physical processing part. They can include humans too.

The holonic concept has already exceeded the manufacturing environment. In the recent literature, the focus is not on HMS (holonic manufacturing) but on HMAS (holonic multiagent system) or on the basic holonic philosophy. Recently, several models have arisen from various scientific fields. For example, there are researches in evolutionary economics [13], smart city management [14], healthcare systems [15], logistics [16], vehicle routing, traffic control smart grids [17], energy management [18], services [19]. These totally different new approaches of the holonic concept have led us to propose a holonic application related to corporate sustainability and crisis management.

4. Crisis and Risk Management, Resilience and Corporate Sustainability

Organizations acting in today's faster than ever changing environment are exposed to a large number of risks. As Mehta has pointed out: "The risks associated with many industrial activities are often assessed in terms of morbidity and mortality statistics for populations exposed to a particular hazard. Rates of cancer, deaths from occupational accidents and genetic damage from chemical or radiation exposure are examples of how risk is used to evaluate the impact of different technologies" [20]. In a recent paper, Cioca et al. [21] presented several statistical data from the metallurgical industry, where in spite of the permanent concern for the development of healthy workplaces there are still several exposures to certain risks, and they show how healthier workplaces contribute to sustainable development.

The United Nation's Global Compact initiative, which is probably the most important corporate sustainability initiative, asks business to actively address environmental risks and opportunities, and have major efforts underway with business in the areas of climate, water and food. As a result, we are seeing businesses around the world preparing for a more sustainable future and becoming part of the solution (see: [1]). More recently, several policies and documents arose which create a concurrent framework for more sustainable enterprises. Let us mention the UN's "17 Sustainable Development Goals" adopted in 25 September 2015 [22], the "Better Policies 2030" Action Plan developed by the OECD (Organisation for Economic Co-operation and Development) [23] and the recently updated (March 2017) "Tripartite declaration of principles concerning multinational enterprises and social policy" of the International Labor Office from Geneva (usually referred as the 2017 ILO/MNE Declaration) [24]. All these documents contain sustainability guidelines that create new approaches, mechanisms (for example, alert mechanism treating with grievances) and targets to multinational enterprises, governments, and employers' and workers' organizations.

At this point we must mention the interrelation of sustainability with resilience. Commonly resilience is defined as the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events [25]. In [26] the relationship between sustainability and resilienceis analyzed in depth. The authors have found in the literature three different generalized management frameworks for organizing sustainability and resilience: (1) resilience as a component of sustainability, (2) sustainability as a component of resilience, or (3) sustainability and resilience as separate conceptual objectives. These results confirm once more that there is a huge diversity among the definitions of these concepts. Referring to resilience, in [27] there is a survey of resilience definitions for different categories of resilience (socio-ecological, economic, organizational and other categories of resilience), of which the majority can be related to sustainability. Our research topic is more related to resilience as a safety

management paradigm, and might be associated with the coupled ecological-engineered system resilience. In our simplified context resilience means to maintain operational capacity and certain goals during and after disturbances. In this context resilience is strongly related to risk management, even if there are some researches that show there is a significant difference between resilience analysis and risk assessment [27].

Risk management goes beyond the traditional approaches which very often are solely based on compliance and on narrowly defined risk assessments. A risk management strategy must contain a sustainability-reporting chapter for the internal and external stakeholders that demonstrates the organization's commitment to sustainable development. This approach increases stakeholder value as it shows awareness to social and environment concerns. It is a new paradigm that integrates the organization, as a man-made ecosystem, into the global ecosystem, maintaining the balance of the three sustainability components—social, environmental, and economic. This balance orientation is a risky, uncertain process and it must be treated cautiously. One of the most recommended practical ways to minimizing the directional risk of sustainability-oriented innovation is the Sustainability Innovation Cube (see Figure 4) presented in [28].

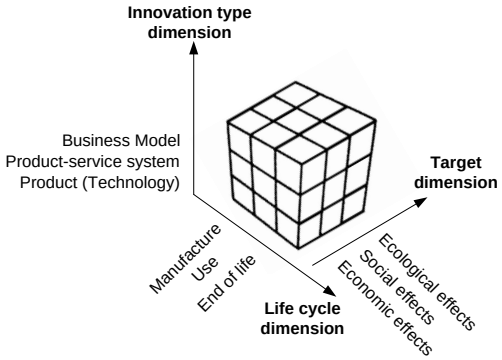

Figure 4. Sustainability Innovation Cube presented in [28].

In our own model, we have a larger perspective of risk management, acknowledging that the majority of threats have some sustainability concern. Usually, when managers/investors, engineers and experts design their risk analysis, they consider the organization to be a linear system, in which changes of the inputs result in proportional changes of the outputs. For example, they may incorrectly base the assumption on their previous experience that the increase/decrease of the number of employees causes a predictable change of productivity.

In Figure 5, we present a typical approach used by engineers where they apply the Gaussian (normal) distribution. In the case of a simple normal distribution, over 99% of the data can be found in a less than 3σ distance from the mean. Everything that is outside of this range is usually neglected. Crisis situations appear for that very reason: the linearization of the system misses a singularity or an extremely unexpected value.

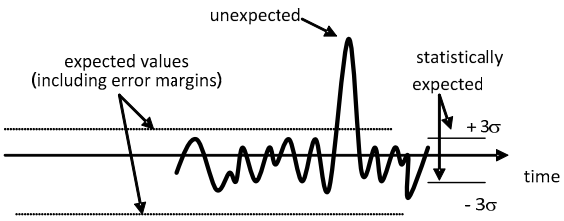

Figure 5. Unexpected situation in the case of single variable problem (Source: authors).

What we mean by crisis is a sudden emergency that causes serious damages and might have major consequences for the future of the organization. This is a simplified definition of "crisis" that only looks at those situations when the unexpected event has an impact at the level of individuals or a small group of people, and it ignores those situations that must be handled by authorities who have the power to govern. In our definition, the survival of the organization is at stake, regardless of its size and the cause of the crisis in which it might be involved.

Another example of linear thinking in risk management comes from the project management theory and practice. There is a risk evaluation technique, the Risk Assessment Matrix, in which the risks are evaluated on the matrix based on two criteria: *likelihood* (the probability of a risk) and *consequences* (the magnitude of the impact or the possible damage). In order to fill the matrix, practitioners employ there are some risk score formulae, like

$$Risk\ score = likelihood \times consequence, \tag{1}$$

or

$$Risk\ score = 2 \times likelihood + consequence, \tag{2}$$

Even if these risk assessment formulae are widely used in practice, they have some major shortcomings. First, the risk definition and analysis mostly focus on the previous experience of the managers or/and the team-members. The acceptance or rejection of a risk mostly hinges on the risk tolerance of some team-members and experts. This approach focuses on the most likely risk factors, ignoring that there might be others. The second weakness and simplification of this widely used method is that it ignores the context. Sometimes, when looking at a project, there is a noteworthy time-gap between the initiation and design phase of the project and the moment when the project is put into practice. The third weakness of this risk-assessment method is the possibility of indetermination. The first formula, in which the likelihood is multiplied by consequence, there is, from a mathematical point of view, an indetermination when one of the components (the likelihood) is almost zero and the other component (the magnitude of the consequence) is huge. In the same way, in the second formula, is pointless to completely ignore an important risk just because it is not probable.

Our last example of the linear approach of risk management, and our last argument for the necessity of a non-linear approach in crisis and risk management, comes from the risk management standard ISO 31000. As we can see in Figure 6, risk management is based mostly on a cyclic risk assessment and risk treatment. Risk treatment in the case of unacceptable risks consists mostly in risk mitigation, using a few strategies that are very static and linear at the same time.

In this paper, we seek solutions for situations in which risks

- are not accounted for in any risk mitigation programs.
- result of imperfect automation.
- can be related to bounded rationality.
- require a solution that focuses on internal communication.
- concern environmental and social issues.

The essence of our appeal is that corporate sustainability and risk management are not separable anymore. Evaluating sustainability involves risk assessment. There is a considerable literature including practical applications that shows the parallel evaluation of sustainability and risks. For example, in [29] Ivascu and etal present a software framework for sustainability evaluation where the solution involves risk assessment. The software creates a report with measures for prevention treatment regarding extremely serious or grave risks and risks with a high probability of occurrence. Our intention is to build on these existing results and to propose solutions for those cases when a company faces situations which are impossible to be included in the software-based prevention and treatment reports which already exist. We will now present our model from both a conceptual and a functional view.

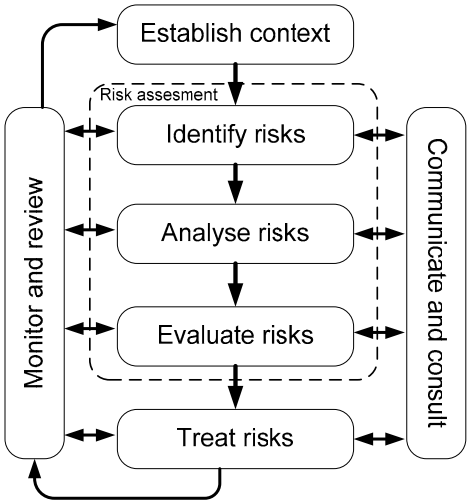

Figure 6. ISO 31000:2009 risk management process (Source: ISO 31000:2009).

5. Conceptual Presentation of the Developed Model

The purpose of our model is to develop a crisis management framework that is capable of reacting in due time to unknown and new kinds of risks. The normal case is that the organization has a corporate sustainability orientation and already has a risk database (RD). They will react according to the existing procedures and protocols in the case of the occurrence of known risk. These procedures are sustainability-tuned, thus a pure technical and economical risk handling approach is avoided, and there is a stakeholder value orientation. They are deployed irrespective of whether events occur on regular basis (for example machine breakdowns, electric power failures) or if they are uncommon. Being known risks, even those events with major consequences are handled well by organizations. A major earthquake or a tsunami at a nuclear power plant or an engine failure during a flight are extreme events, but they certainly do not find the organization/the flight pilot unprepared. These events have a pretty good chance to lead to a so-called "successful accident" due to the careful preparation of the human- and computer-based control system. There are several drills and simulations of such events, thus in the case of an emergency there is a known scenario, and the damages will be the less possible.

Our model focuses on those situations when the organization faces different types of unpredictable threats and proposes how to respond to those threats in critical time. The model is suitable for those organizations in which there are computer-assisted activities and the constituent entities communicate using an IT infrastructure. Step by step, we can include almost all types of organizations, because organizations are already digitalised down to worker's level, and they use computer assistance for most of the activities. The interaction of the computers creates, together with humans, an intelligent global net never experienced before.

In crisis management the due time is critical. That is why we focus on human–system integration. This assumes a human–machine, human–human and machine–machine integrated communication. Crisis handling requires intuition, quick reactions, brainstorming-like analysis and decision-making. We are interested in those communication situations in which the crisis handling entities, i.e., human and software agents, must communicate using a digital environment and/or they must use special communication protocols. That is why in our model we do not make much difference among the machine–machine, human–human and human–machine communication rules. Obviously, during crises situations human holons, if the crisis handling team is located at the same location, will communicate using the quickest way: by verbal communication and body language. As a result, in those situations where verbal communication based teamwork can be done (people are in same location) they all together are considered as a single holon.

The novelty of our approach consists of the existence of the human component of each holon, as opposed to the usual multiagent concepts, where there are only software agents. The proposed holonic framework is presented in Figure 7.

As we can see in Figure 7, in the midpoint of our model is the Crisis Management Holarchy (CMH) that interacts with several other holarchies. In this simplified figure we present, as an example, some constituent holons inside of the CMH (HRM, FA, PR, QAS holons). In practice, the CMH holon may contain many other types of holons depending on the company profile and its complexity. Each of these holons are part of the whole CMH, but at the same time they also belong to other different holarchies. This relationship with between CMH and other internal holarchies is marked by the dotted lines in Figure 7. The constituent holons inherit the knowledge of those holarchies they come from and bring it into the CMH. If we assume that these holarchies are some of the commonly found departments (financial, quality assurance, marketing and so on), we might have something similar in any other crisis handling team that we may find in practice. The main and first difference lies in the *nature* of the relationship among the constituent elements. Here the holons are entities that are in a loosely coupled hierarchy inside and outside of CMH (they are autonomous, self reliant, goal oriented) and there is a specially designed software agent related to each holon. This second characteristic shows a level of human–machine integration that is higher than what is found in majority of existing organizations. Figure 7 shows that the external environment (for example stakeholders, emergency services) and the internal environment (manager layer, risk monitoring department) have the same kind of relationship with the CMH. This equal treatment of all internal and external entities demonstrates the corporate sustainability orientation of our model. The entities connected with the CMH are assumed to also be holarchies, containing autonomous and independent holons, with own objectives and rules. The boldness of the arrows is meant to exhibit the importance and intensity of the communication among the holarchies.

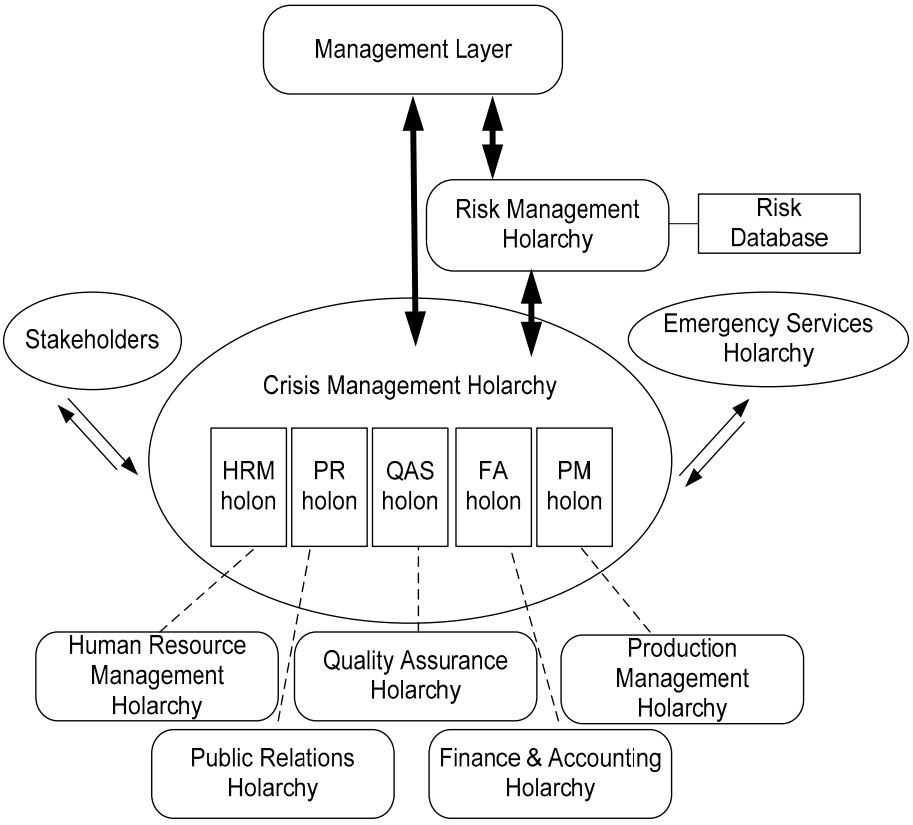

Figure 7. Crisis management holarchy (Source: authors).

The management layer (ML) holon represents the higher authority in the organization. The risk management holarchy (RMH) is a specially designed holarchy which is in charge of the risk management. The RMH manages the risk database (RD) and its permanent task is to detect and handle any threats. Under normal circumstances, and also under abnormal but known circumstances, the RMH is able to handle any disturbances that range from a major event occurring in the markets to, let ussay, a machine breakdown or an intruder in the courtyard. There is a complex relationship and strong interconnection between the RMH, ML and CMH. In Table 1 we present the main tasks of the most important constituents of our model.

Table 1. Major holarchies of the developed model.

Holarchy	Abr	Task
Management Layer	ML	design and supervising
Risk Management Holarchy	RMH	risk management
Crisis Management Holarchy	CMH	crisis management
Emergency Services Holarchy	ESH	professional help

The two upper levels of the Figure 7 present what we mostly find in the external environment of the organization. The arrows depict the obligation and intensity of external communication during crises. Here, what is meant by stakeholder, is any person, group, or company, i.e., institution that can affect or be affected by the crisis or the course of action during the crisis. This approach is narrower than the common concept of stakeholders used in strategic and project management or in the theory of CSR (corporate social responsibility). For example, the police or the fire department, as many other government authorities are stakeholders of the organization by common definition, but our model places them separately, incorporating them in the Emergency Services Holarchy. The reason for this special treatment lies with the corporate sustainability approach: In order to be functional, the CMH must have well-developed inter-holon communication procedures with these entities.

6. Functional Presentation of the Model

When the risk monitoring holarchy (RMH) identifies any kind of disturbance it compares the situation with the existing risk database (RD). If there is a match it starts the standardized risk handling procedure. For example, the RMH might send a message to the financial department concerning some new information regarding a supplier's possible bankruptcy. In the same way, the RMH might call the emergency number (for example, 112 in Europe) because there was an explosion in the warehouse or someone had a stroke. Under these "normal" conditions when known but unexpected events occur the RMH just initiates some already tested procedures. But it is far more challenging when the organization faces totally unknown and unexpected events. In such a situation, the RMH activates the Crisis Management Holarchy (CMH) that consists of multiple holons prepared for such situations. The constituent holons are software agents and human operators at the same time. To put the handling scenarios in action, the physical presence of each human holon is not required in the same location. Thus, the first handling scenarios can be configured in very short time. For example, the organization's website, its social media accounts and other communication interfaces can react in milliseconds, and start to work in one of the previously designed safe modes. As the members of the CMH are autonomous holons, they are self-reliant units and can make decisions without previously consulting their superiors. At the same time these holons are permanently subject to certain control activities, either from the CMH and the ML, or in some cases from holarchies they originally came from (as is shown in the lower part of the Figure 7). The CMH as a whole remains functional if some constituent holons are not operating, or if they are sending doubtful data. Even in the absence of communication with the ML or RMH, the CMH has the capability to operate. All holons and holarchies, regardless of their position in the organization, can act when some data are missing, and they can operate for the functionality of the bigger whole of which they are part. This way of acting creates a stable

holarchy that can cope with serious disturbances, as will be shown below in the description of the communication protocol.

After the first fast reaction and when it has put all the processes in safe mode, the CMH finishes its mission and will let the ML layer evaluate the damages and take the necessary steps for recovery. This crisis management cycle is then closed by the RMH, which updates the risk database with the solution provided by the CMH or by the ML, and sets up new risk handling procedures in order to avoid similar cases. In the following we present the main actors of the model.

6.1. The RMH

The RMH consist of a few (depending on the size and the type of the organization) specially trained holons. The RMH is a human–machine holarchy that entails software agents and human operators. In some situations, the human is not required (for example, the control system shuts down the main computer because the processor is overheated), and, in some cases, it is advisable that the human operator confirms the emergence of a risk. For example, it is likely that in the Internet of Things era the fire security systems alert the fire department, providing live images of a fire in the warehouse, but it is still the human operator who can give further and trustful data when calling the emergency number. The holonic design makes it possible that the fire department will detect the fire if at least one of the constituent elements of RMH is sending trustful data.

The number of holons strongly depends on the technology used, the size of the organization and the level of digitalization. It is common sense that in the case of an airport the RMH should be more complex than, let ussay, in a ... pub. It is out of the scope of this article to present how the RMH does the monitoring activity and how it collects the information about the ongoing processes inside the organization. The RMH has as a special job to update the risk management database with all the risks detected and to design the handling procedures of these risks. Even in the case of major, but already experienced, circumstances the RMH is able react by following previously designed routines. The RMH is a permanent structure inside the organization acting as a consulting staff for the management. In the case of large complex organizations, the RMH might look similar to a flight control room used in the case of spaceship launches. In other cases, it consists of a few computers and some operators that act like a call-centre, a surveillance office and a dispatching centre put together. The complex relationship and strong interconnection between the RMH, ML and CMH allows to the RMH to decide if they will act according to the procedures, inform the ML or trigger/create the CMH. If the information system of the organization detects malfunctions or an incoherent act of the RMH holarchy, the system activates the CMH instantly.

One major prerequisite in risk management is that the organization has identified and understood its risks. Risk judging, mitigation or actions to anticipate, monitor or review the progress, all depend on knowing to what kind of risks the organization is exposed. Only after that we can create policies, protocols and action plans. The role of the RMH is to keep an up-to-date risk register, with risk profile data, to measure some critical process parameters and to assure business continuity and disaster recovery plans. The RMH should make the emergency contact arrangements and deal with critical service suppliers (water, gas, electricity) and emergency services like fire department, hospitals, police and other authorities. At the same time, the RMH controls all the activities related to the security of the organization, from fire prevention, labour-safety, occupational health, response to cyber-attacks and many others. The risk database kept within the organization contains the metrics, the drivers and the profile for each category of risk. The RMH can search, detect and update identified risks on a risk database in a similar process like how virus signatures are added to the human immune system memory, as proposed by Ulieru and Worthington in [30]. As a result, the system can react more quickly to the recurring emergencies, or become immune like living organisms are becoming immune to known viruses.

Whenever a crisis situation appears, the Crisis Management Holarchy (CMH) is triggered or activated by the RMH or by the management layers. The triggering procedure shall be quick, robust

and trustful. Crisis situations seldom appear when known and predictable risks emerge. Usually crises emerge if there is a situation that has never been imagined, if there are totally new threats or if there is a simultaneous appearance of multiple risks in a previously not met combination.

6.2. The CMH

The Crisis Management Team Holarchy (CMH) represents the core holarchy of our model. As we already pointed out, the holarchies are loosely coupled hierarchical structures with autonomous holons. This is the main difference to the classical organizations, where we have strong connections among the hierarchical levels. In the case of holonic multiagent systems the holons can decide if they want to be part in a holarchy, and they can leave whenever they want. These decisions are made according to their—carefully designed—own goals. Whenever they consider that being part of a certain holarchy can help them to achieve their goals more easily, they will act inside the holarchy, in other case they will exit. In our case, the holons included in the CMH must be set (by assigning this as a goal) to stay in the holarchy as long the communication protocols perform well.

In order to understand how the concept works in Figure 8 we show the main communicational patterns among the CMH and the other constituent holons (the acronyms used in the figure will be explained in the passage that follows). Each of these holons are expert holons in a certain field, and they are set to contribute with their specific knowledge to solve a crisis situation. For example, the PR holon after receiving the trigger information will automatically set the on-line presence of the organization in a safe-mode; it can activate a backup-site or send a message to the social media about a possible technical problem. Under normal circumstances the constituent holons will never leave the CMH unless there are some inconsistencies in the messages they receive inside the CMH. The other way in which a constituent holon may exit CMH is when it receives a recall message from a (professional or functional) holarchy to which it belongs (marked with "RC" in Figure 8).

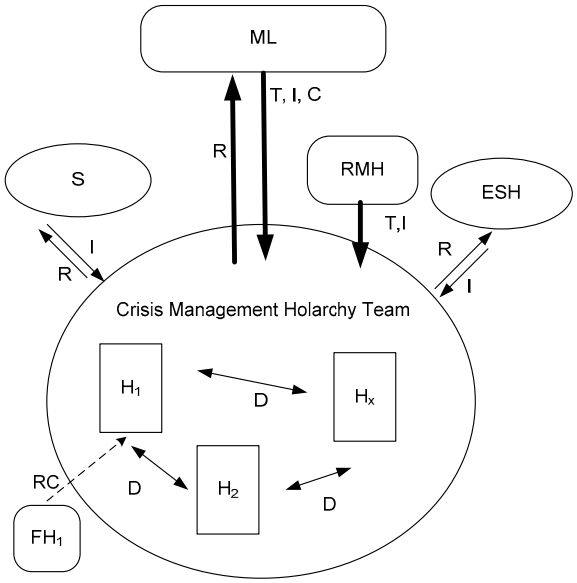

Figure 8. CMH communication patterns (Source: authors).

If the CMH holarchy is triggered, the constituent holons will be activated and they will constitute the CMH. The CMH will start to handle the situation about which the holons were informed in the triggering message. The triggering message (marked with "T" in Figure 8) usually comes from the RMH, but in the case of any malfunction, the message is sent by the management layer, as is presented in Figure 7. The CMH holarchy receives input information from all other holons fin its environment, and creates reports as output information for many other holons ("R" in Figure 8).

The constituent holons exchange data permanently (this data exchange is marked with "D" in Figure 8), using an artificial pheromone-based communication as suggested by Dorigo [31] or later Ulieru [32], or they use a cloud computing technology. The pheromone based-communication makes the holons communicate mostly with their environment and not among each other. Thus, all the information is available to each holon at the same time.

The job of the CMH ends with a final report that contains the conclusions and the solutions found during the crisis. This information will be inserted by the RMH in the risk database, in order to have a procedure for solution and for handling all similar situations in the future. The activity of the CMH can stop in the case of a cancelling message sent by the ML ("C" in Figure 8). The cancelling message (C), in the same way as the recall message (RC), will be ignored by the CMH and the constituent holons, if there are suspicions that the received message is a result of a decision that was made on the grounds of untrustful data. This is one of the features of the model that assures sustainability, stability and trustful communication.

One of the novelties of our model consists of the reporting ability to the stakeholders and the emergency services without the approval of a higher authority. This unorthodox proposal is based mostly on two considerations. The first is related to the quick reaction time needed during crisis situations. Here the due time is critical; sometimes a minute delay may double the damages. The second consideration is that in the short time frame the ML will never have time to get a second opinion, and anyway it is pointless to overrule a report made by a carefully selected professional team.

Crisis situations need teamwork, creativity, cooperation and professional approach. We agree with Guy Boy, who said that it is time to (re-)learn how to deal with the unexpected using a non-linear approach, where experience and expertise are key assets. Dealing with the unexpected requires accurate and effective situation awareness, synthetic mind, decision-making capability, self-control, multi-tasking, stress management and cooperation (team spirit) [33].

The CMH must be designed in that way because it must be able to make decisions even if some of the constituent holons are not available. Obviously, the more malfunctioning holons we have the less useful outcome we might have. But, a less optimal decision usually is far better than a passive perspective. In a limited time frame the CMH has full authority to overrule any prior decision of any authority, to reschedule all resources and to assign tasks, define interconnections and reroute crews.

6.3. The ML

The management layer (ML) in Figure 8 represents the higher authority on the system. Its structure may vary on a large scale in function of the size and the type of the organization. In our model, the ML has a supervising role during the crises. This layer creates the holonic structure of the organization; it can state whether there is a crisis situation, and it can decide when the crisis is over and the CMH should cease its activity. The ML is responsible for the design of the interconnections not only inside the CMH, but also with the RMH and the other holarchies. We propose that during the crisis, there is a full delegation of responsibilities to the CMH, in a similar manner like in the case of many projects where the project manager has full authority. Another example might be the way in which some multinational holdings are organized. The full responsibility lies with the management board of the affiliated company and not with the board of the holding. Of course, the holding has the necessary tools to control the activity of the affiliated company, but in the short term it is impossible to tightly control any branch or member of the group.

7. The Communication Protocol

Communication protocol, as we define it here, is a human–machine, human–human or machine–machine conversation policy. These policies, a suite of well-defined rules and procedures, must be set carefully in order to assure the operability of the model. The efficiency of the entire system during crises is given by the efficiency of the communication. In fact, crisis management is firstly communication, and just secondly is about management activity.

The organizations are nowadays usually digitalised down to the worker's level. During crises, we can assume that each entity is in a position to make use of a "thing" to communicate. Relatively few situations can be conceived when the *majority* of the crisis handling holons are not able (or are put) to abort IT based communication. We might think of only very few situations: either all of the staff is in the same room (and the crisis is so small that it can be solved by oral discussion), either there was a fatal cyber-attack, or the whole organisation has ceased to exist for some reason.

The design-process of the communication protocols that was outlined above calls for teamwork among multiple specialists and for proper team management. The ICT specialists can create artefacts only after the information system is carefully designed. We assume that readership of this journal is unlikely to be interested in the applicable technical standards and of specific software, and thus we decided not to present the wide range of technologies available to carry out the communication network required by our model. The definition of the holons usually is made using the JADE development environment (http//jade.tilab.com).In practice, the solutions are up to the best knowledge of the IT experts involved.

In Figure 9 we just suggest a TCP/IP-like linking among the holons, using a three-way handshake method for establishing the connection, and a four-way handshake closing procedure. SYN denominates the request for the synchronisation, ACK is the acknowledgement, and FIN is finish. This way of establishing and closing communication can be augmented, sometimes replaced, with the CNP task-sharing protocol that is specially designed for multiagent systems. CNP (Contract Net Protocol) was originally developed many decades ago by Smith [34].This protocol simulates a negotiation taking place in a virtual marketplace among holons for certain tasks. Usually there are five stages: Recognition, Announcement, Bidding, Awarding, and Expediting. Apart from the inter-holon communication algorithm, Figure 9 also depicts some security issues of this communication. Among the security measures we propose AES (Advanced Encryption Standard) scripting during the communication; the exchanged messages may contain a secure checksum value to verify the integrity of the data. The current hash technology in industry uses the Secure Hash Algorithm (SHA).

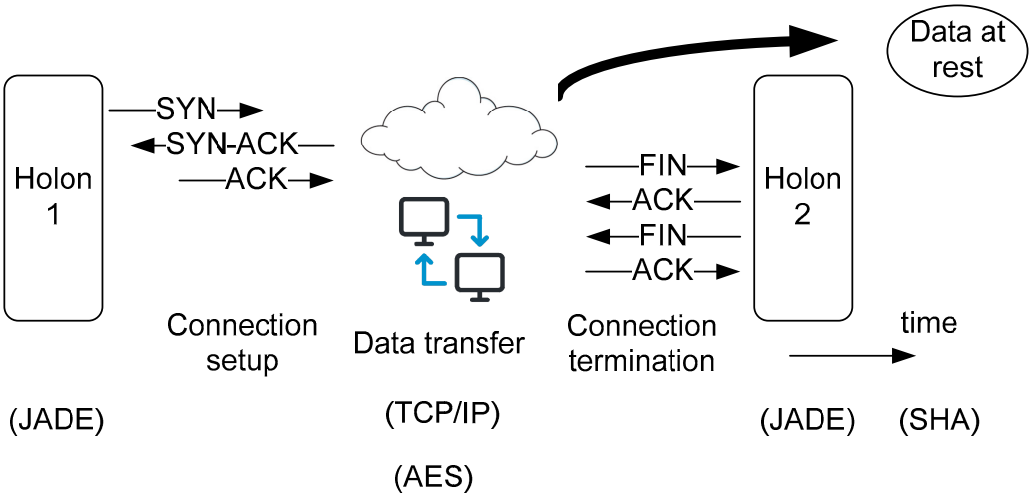

Figure 9. Communication platform (Source: authors).

In inter-holon communication it might be necessary to use simple usual communication methods parallel to sophisticated solutions, for example a spreadsheet technology (such as Google Docs). This would help to find remote solutions for a certain problem, because in crisis management we have to focus on the problem rather than on the software technology. Even the simplest technologies available for the average organizations are already designed for an acceptable security with regard to data management. On the other end, even the most developed security systems used by military

or intelligence purposes are not bulletproof against certain types of attacks, for example against "insider threats".

In addition to what the rich literature of IT security offers, and endorsing the use of specific standards (for example the ISO/IEC 27001 family providing requirements for an information security management system—ISMS), we recommend that robust holonic structures be conceived along the "laws of the artificial" created recently by Valckenaers and Van Brussel for holonic developers [17].

Another "holon-friendly" communication solution has already been mentioned above where we presented the constituent elements. This is the artificial pheromone-based communication. Similar concepts are stigmergy-based communication as suggested by Dorigo [31], the holonic Cybersecurity model proposed by Ulieru et al. [35] or the artificial immune system concepts. They are still up-to-date solutions. Here, the holarchies and the holons communicate as some simple biological organisms do, like ants in food foraging or antibodies in fighting viruses. Next to the effective communication we must mention both methods' agilityin learning, their ability to produce a quicker response in the case of repetitive threats and the robust behaviour when some constituent holons behave inconsistently, are performing ill or when the communication is interrupted.

8. Final Remarks

The holonic-based communication protocol presented in this paper proposes solutions for those unpredictable situations that are not covered by the traditional risk assessment and mitigation processes. The main characteristics—agility, resilience and stakeholder orientation—contribute to sustainable corporate behaviour. We lean on Bergman's sustainability typology (three conceptual types and nine subtypes of corporate sustainability) [1], and from there our model contributes to those conceptual works that consider corporate sustainability strongly bounded with corporate social responsibility (the first conceptual type), complemented with possibilities given by the holonic multiagent concept. The proposed communication protocol is based on a pattern that has its roots in machine–machine communication, and can perform under circumstances when some of the constituent elements are under-performing or are missing. The loosely coupled networks, i.e., the holarchies, can be customized in practical applications, and thus they can cope with the permanently changing market conditions and/or customer demands and lead to sustainable corporate behaviour.

The presented model emphasizes a market-oriented sustainability even during crises, when sometimes in only a few minutes there is a need to balance goals and needs of the current activities with the long-term objectives. We supply here arguments for the validity of the theory presented by Porter and Kramer [4]. Here in the case of extremely short span of time companies should operate in ways that secure long-term economic performance by avoiding short term behaviour that is socially detrimental or environmentally wasteful. Even during crises, it is not possible to predetermine a priority order among the dimensions of responsibility, because the relationship between the principle of profitability and sociality is mutual, as Gandini et al. stated in [5]. The essence of our appeal is that corporate sustainability, crisis management and resilience are not separable.

The resilience of the model consists of ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events, as it was defined in [25]. From the theoretical point of view, the loose-coupled nested hierarchy depicted above can be already considered as an example for a holonic system that follows the principles and laws presented by Valckenaers and VanBrussel in [17].

As future work, the authors wish to develop some applications to test in situthe presented model. At the same time, there is an ongoing research to create metrics of the resilience and adaptability of the developed model.

Author Contributions: All authors contributed equally to the writing of this paper and read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. United Nations Global Compact (UNGC). Guide to Corporate Sustainability. 2015. Available online: https://www.unglobalcompact.org/library/1151 (accessed on 13 October 2017).
2. Bergman, M.M.; Bergman, Z.; Berger, L. An Empirical Exploration, Typology, and Definition of Corporate Sustainability. *Sustainability* **2017**, *9*, 753. [CrossRef]
3. Linnenluecke, M.K.; Griffiths, A. Firms and sustainability: Mapping the intellectual origins and structure of the corporate sustainability field. *Glob. Environ. Chang.* **2013**, *23*, 382–391. [CrossRef]
4. Porter, M.E.; Kramer, M.R. *Strategy and Society: The Link between Competitive Advantage and Corporate Social Responsibility*; Harward Business Review: Boston, MA, USA, 2006.
5. Gandini, G.; Gennari, F.; Cassano, R. Global Responsibility and Strategic Risk Management. *J. Bus. Manag. Appl. Econ.* **2014**, *III*, 1–15.
6. Bar-Yam, Y. *Dynamics of Complex Systems*; Addison-Wesley: Boston, MA, USA; Perseus Books: Cambridge, MA, USA, 1997; ISBN 978-020155748.
7. Coombs, W.T.; Holladay, S.J. *The Handbook of Crisis Communication*; Wiley-Blackwell: Malden, MA, USA, 2010; ISBN 978-1444361902.
8. Wooldridge, M. *An Introduction to MultiAgent Systems*; John Wiley & Sons, Ltd.: Chichester, UK, 2002; ISBN 0-471-49691-X.
9. Koestler, A. *The Ghost in the Machine*; The Macmillan Company: Hutchinson, UK, 1967.
10. Christensen, J.H. Holonic Manufacturing Systems: Initial Architecture and Standards Directions. In Proceedings of the First European Conference on Holonic Manufacturing Systems, Hannover, Germany, 1 December 1994.
11. Babiceanu, R.F.; Chen, F.F. Development and applications of holonic manufacturing systems: A survey. *J. Intell. Manuf.* **2006**, *17*, 111–131. [CrossRef]
12. McFarlane, D.C.; Bussmann, S. Developments in holonic production planning and control. *Prod. Plan. Control* **2000**, *11*, 522–536. [CrossRef]
13. Madureira, A.; Hartog, F.; Baken, N. A holonic framework to understand and apply information processes in evolutionary economics: Survey and proposal. *Netnomics* **2016**, *7*, 157–190. [CrossRef]
14. Bakos, L. Smart City Management and Holonic Manufacturing Concept. In Proceedings of the Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Vienna, Austria, 23–26 November 2011; pp. 1623–1624.
15. Valckenaers, P.; De Mazière, P. Innovative ICT Systems for Integrated Care. In Proceedings of the International eHealth, Telemedicine and Health ICT Forum for Educational, Networking and Business, Luxembourg, 9–11 April 2014.
16. Van Belle, J.; Saint Germain, B.; Philips, J.; Valckenaers, P.; Cattrysse, D. Cooperation between a holonic logistics execution system and a vehicle routing scheduling system. *IFAC Proc. Vol.* **2013**, *46*, 41–46. [CrossRef]
17. Valckenaers, P.; Van Brussel, H. *Design for the Unexpected: From Holonic Manufacturing Systems towards a Humane Mechatronics Society*; Butterworth-Heinemann: Oxford, UK, 2015; ISBN 978-0-12-803662-4. [CrossRef]
18. Fähnrich, K. P.; Kühne, S.; Hummel, A. Multi-Agent-Based Simulation of Decentralized Energy Systems. In *Proceedings of the 2nd International Conference on Green Materials and Environmental Engineering*; Advances in Engineering Research; Atlantis Press: Paris, France, 2015.
19. Borangiu, T.; Trentesaux, D.; Thomas, A.; McFarlane, D. (Eds.) *Service Orientation in Holonic and Multi-Agent Manufacturing*; Springer International Publishing: Cham, Switzerland, 2012; pp. 103–113. [CrossRef]
20. Mehta, D.M. Risk Assessment and Sustainable Development: Towards a Concept of Sustainable Risk. *RISK Health Saf. Environ.* **1997**, *8*, 137–154.
21. Cioca, M.; Ivascu, L.; Cioca, L.I. Safety Performance Indicators in the Metallurgical Industry Using Web Programming. *Metalurgija* **2017**, *56*, 272–274.
22. UN's 17 Sustainable Development Goals. Available online: www.un.org/sustainabledevelopment/sustainable-development-goals/ (accessed on 6 December 2017).
23. Better Policies for 2030. An OECD Action Plan on the Sustainable Development Goals. Available online: www.oecd.org/dac/Better%20Policies%20for%202030.pdf (accessed on 6 December 2017).

24. Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy. Available online: http://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/---multi/documents/publication/wcms_094386.pdf (accessed on 6 December 2017).
25. National Research Council. *Disaster Resilience: A National Imperative*; The National Academies Press: Washington, DC, USA, 2012. [CrossRef]
26. Marchese, D.; Reynolds, E.; Bates, M.E.; Morgan, H.; Clark, C.C.; Linkov, I. Resilience and sustainability: Similarities and differences in environmental management applications. *Sci. Total Environ.* **2018**, *613–614*, 1275–1283. [CrossRef] [PubMed]
27. Francis, R.; Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 90–103. [CrossRef]
28. Hansen, E.; Grosse-Dunker, F.; Reichwald, R. Sustainability Innovation Cube—A Framework to Evaluate Sustainability-Oriented Innovations. *Int. J. Innov. Manag.* **2009**, *13*, 683. [CrossRef]
29. Ivascu, L.; Cioca, L.I.; Rus, S. Sustainable Development Influence on the Competitive Advantage of Companies. In Proceedings of the 27th IBIMA Conference, Milan, Italy, 4–5 May 2016.
30. Ulieru, M.; Worthington, P. Autonomic risk management for critical infrastructure protection. *Integr. Comput. Aided Eng.* **2006**, *13*, 63–80.
31. Dorigo, M.; Bonabeau, E.; Theraulaz, G. Ant algorithms and Stigmergy. *Future Gen. Comput. Syst.* **2000**, *16*, 851–871. [CrossRef]
32. Ulieru, M. Adaptive Information Infrastructures for the e-Society. In *Engineering Self-Organising Systems*; Brueckner, S.A., Di MarzoSerugendo, G., Karageorgos, A., Nagpal, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3464.
33. Boy, G.A. Dealing with the Unexpected in our Complex Socio-Technical World. In Proceedings of the 12th IFAC Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, Las Vegas, NV, USA, 11–15 August 2013.
34. Smith, G.R. The Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver. *IEEE Trans. Comput.* **1980**, *C-29*, 1104–1113. [CrossRef]
35. Ulieru, M.; Grobbelaar, S.; Sohail, M.; Bu, S. *eNetworks Cyber Engineering: Infrastructures for Cyber-Physical Ecosystems*; IEEE: Montreal, QC, Canada, 2007. [CrossRef]