2011 Eighth IEEE International Conference and Workshops on Engineering of Autonomic and Autonomous Systems

Apoptotic Robotics
Programmed Death by Default

Roy Sterritt
School of Computing and Mathematics & Computer Science Research Institute,
University of Ulster, Jordanstown Campus, Northern Ireland.
r.sterritt@ulster.ac.uk

Abstract

Apoptotic Computing and Apoptotic Communications are inspired by the apoptosis mechanism in biological systems. This mechanism provides security for the overall system by having a preprogrammed death and indeed a death by default at, for instance, the cellular level. It has been argued that this approach should be included in our modern ubiquitous/pervasive computer-based systems. This paper specifically makes that case for Robotic systems.

Keywords: Emerging Technologies, Biological Inspired, Autonomic, Apoptotic, Self-managing, Autonomy

1. Introduction

Credit: 20TH CENTURY FOX

"Scientists fear a revolt by killer robots" was a headline in the UK's *Sunday Times [1]* reporting on scientists who presented their findings at the International Joint Conference for Artificial Intelligence in Pasadena, California, in July 2009, feared that nightmare scenarios, which have until now been limited to science fiction films, such as the Terminator series, The Matrix, 2001: A Space Odyssey, Minority Report and I Robot, could come true. They warned that mankind might lose control over computer-based systems that carry out a growing share of society's workload, from waging war to chatting on the phone, and have already reached a level of indestructibility comparable with a cockroach. For instance, robotic unmanned predator drones, which can seek out and kill human targets, have already moved out of the movie theatres and into the theatre of war in Afghanistan and Iraq. While at present controlled by human operators, they are moving towards more autonomous control. They may also soon be found on the streets. Samsung, the South Korean electronics company, has developed autonomous sentry robots to serve as armed border guards. They have "shoot-to-kill" capability [1].

This news report in fact sensationalized the interim report from the AAAI Presidential Panel on Long Term AI Futures (August 2009)[2] which had met in February 2009 as well as at IJCAI 2009. The sub-panel on Pace, Concerns, Control had in reality dismissed much of the hype around *Singularity* and actually raised concerns of the non-AI community perception that this was forthcoming. Nevertheless, there was a shared sense that additional research would be valuable on methods for understanding and verifying the range of behaviours of complex computational systems and to minimize unexpected outcomes.

As it happens, co-located that week with IJCAI in Pasadena was the IEEE Computer Society's and NASA linked "System Mission Challenges for IT (SMC-IT) conference" where in one of the workshops on *Autonomous and Autonomic Space Exploration Systems (AA-SES)* the author presented the latest developments on work [3] in Autonomic Computing and Apoptotic

978-0-7695-4380-2/11 $26.00 © 2011 IEEE
DOI 10.1109/EASe.2011.21

Computing in which NASA were being granted several US Patents.

The Apoptotic Computing project, first started back in 2002 [4][5][6][7][3] involves working towards the long-term goal of developing Programmed Death by Default for Computer-Based Systems to provide for this foreseen future. It is essentially biologically-inspired by the Apoptosis mechanisms in multicellular organisms. It may be considered as a sub-area of Bio-Inspired Computing, Natural Computing or Autonomic Systems (providing the self-destruct property).

In this article we focus on the case for having a death by default built into Robotic systems.

2. Biological Apoptosis

If one cuts oneself and starts bleeding, one treats it and carrying on with one's tasks without any further conscious thought (although pain receptors will induce self-protection and self-configuration to use the other hand!). Yet, often, the cut will have caused skin cells to be displaced down into muscle tissue [9]. If they survive and divide, they have the potential to grow into a tumour. The body's solution to dealing with this situation is cell self-destruction (with mounting evidence that some forms of cancer are the result of cells not dying fast enough, rather than multiplying out of control, as previously thought and considered by the general public).

It is believed that a cell knows when to commit suicide because cells are programmed to do so – self-destruct (sD) is an intrinsic property. This sD is delayed due to the continuous receipt of biochemical retrieves. This process is referred to as apoptosis[27], pronounced either as APE-oh-TOE-sls or uh-POP-tuh-sis and means for 'to fall off' or 'drop out', used by the Greeks to refer to the Fall/Autumn dropping of leaves from trees; i.e., loss of cells that ought to die in the midst of the living structure. The process has also been nicknamed 'death by default'[9], where cells are prevented from putting an end to themselves due to constant receipt of biochemical 'stay alive' signals (*Figure* ***1***). The key aspect of apoptosis is that the cell's self-destruction takes place in a programmed and controlled way (*Figure* ***2***); the suicidal cell starts to shrink, decomposes internal structures and degrades all internal proteins. Thereafter, the cell breaks into small membrane-wrapped fragments (drop-off) that will be engulfed by phagocytic cells for recycling. Necrosis, is the un-programmed death of a cell, involving inflammation and toxic substances leaking to the environment [10].

Further investigations into the apoptosis process [27] have discovered more details about the self-destruct program. Whenever a cell divides, it simultaneously receives orders to kill itself. Without a reprieve signal, the cell does indeed self-destruct. It is believed that the reason for this is self-protection, as the most dangerous time for the body is when a cell divides, since if just one of the billions of cells locks into division the result is a tumour, while simultaneously a cell must divide to build and maintain a body.

The suicide and reprieve controls have been compared to the dual-key on a nuclear missile [8]. The key (chemical signal) turns on cell growth but at the same time switches on a sequence that leads to self-destruction. The second key overrides the self-destruct [8].

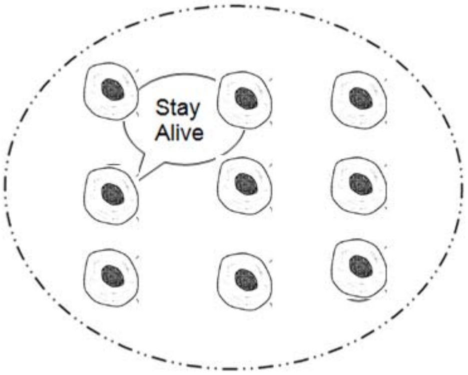

Figure 1 Turning off the self-destruct sequence - cell receives 'stay alive' signal [4].

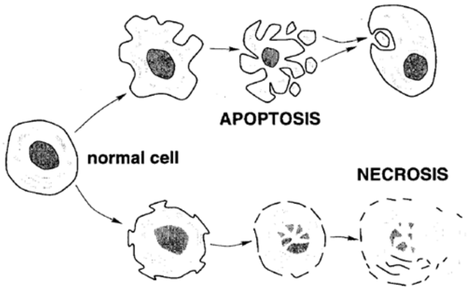

Figure 2 Programmed death by default (apoptosis) and necrosis due to injury [10]

3. Computer-Based System's Apoptosis

The case has been made for introducing apoptotic measures into Agent-Based Systems, Autonomic (Self-managing and adaptive) Systems and Swarm Based Space Exploration Systems [3]-[7] and is recapped in this section.

3.1 Agent-Based Apoptotic Systems

Agent destruction has been proposed for mobile agents, in order to facilitate security measures [12]. Greenberg et al. highlighted the scenario simply by recalling the situation where the server omega.univ.edu was decommissioned, its work moving to other machines. When a few years later a new computer was assigned the old name, to the surprise of everyone, email arrived, much of it 3 years old[12]. The mail had survived 'pending' on Internet relays waiting for omega.univ.edu to come back up.

Greenberg encourages consideration of the same situation for mobile agents; these would not be rogue mobile agents – they would be carrying proper authenticated credentials. This work would be done totally out-of-context due to neither abnormal procedure nor system failure. In this circumstance, the mobile agent could cause substantial damage, e.g., deliver an archaic upgrade to part of the network operating system, resulting in bringing down the entire network.

Misuse involving mobile agents comes in the form of: misuse of hosts by agents, misuse of agents by hosts, and misuse of agents by other agents.

From an agent perspective, the first is through accidental or unintentional situations caused by that agent (race conditions and unexpected emergent behavior), the latter two through deliberate or accidental situations caused by external bodies acting upon the agent. The range of these situations and attacks have been categorized as: damage, denial-of-service, breach-of-privacy, harassment, social engineering, event-triggered attacks, and compound attacks.

In the situation where portions of an agent's binary image (e.g., monetary certificates, keys, information, etc.) are vulnerable to being copied when visiting a host, this can be prevented by encryption. Yet there has to be decryption in order to execute, which provides a window of vulnerability [12]. This situation has similar overtones to our previous discussion on biological apoptosis, where the body is at its most vulnerable during cell division [4]. As such an agent should have an inherent pre-programmed self-destruct mechanism inbuilt for safety of the information or code it carries, either that can be self-activated if detects interference or if it has not received its stay-alive signal as it is no longer in the correct context or arrived with an non-authorized host.

3.2 Autonomic Apoptotic Systems

Autonomic Computing and Communications is inspired by the biological nervous system and properties of homeostasis and responsiveness The general properties of an autonomic, or self-managing, system can be summarized by four objectives—self-configuration, self-healing, self-optimization and self-protection—and four attributes— self-awareness, self-situation, self-monitoring and self-adjusting [11][24][25].

Essentially, the objectives represent broad system requirements, while the attributes identify basic implementation mechanisms.

The autonomic paradigm assigns an "autonomic manager" to a component utilizing a sensors and effectors and a closed control feedback loop to provide the self-management. Autonomic Mangers communicate and cooperate to provide system wide self-management.

AMs may communicate and cooperate through a combination of various means; self-managing event messages, heart-beats, pulse signals, RPCs, and mobile agents. The apoptosis (stay alive / self-destruct mechanism) may be utilized in this scenario as self-protection, to withdraw authorization to continue operation, for example, if the policies become out-of-date when they arrive at the autonomic manager their "stay alive" reprieve has not been received thus preventing the system changes from being enacted.

3.3 Swarm-Based Space Exploration Systems

Space Exploration Missions, through necessity, have been incorporating more and more autonomy and adaptability. Autonomy may be considered as self-governance of one's own tasks/goals. NASA is investigating the use of swarm technologies for the development of sustainable exploration missions that will be autonomous and exhibit autonomic properties. The idea is that biologically-inspired swarms of smaller spacecraft offer greater redundancy (and, consequently, greater protection of assets), reduced costs and risks, and the ability to explore regions of space where a single large spacecraft would be impractical.

ANTS (Autonomous Nano-Technology Swarm) is a NASA concept mission, a collaboration between NASA Goddard Space Flight Center and NASA Langley Research Center, which aims at the development of revolutionary mission architectures and the exploitation of artificial intelligence techniques and the paradigm of biological inspiration in future space exploration[15]. The mission concept includes the use of swarm technologies for both spacecraft and surface-based rovers, and consists of several submissions such as SARA (The Saturn Autonomous Ring Array), PAM (Prospecting Asteroid Mission) and LARA (ANTS Application Lunar Base Activities).

In terms of ANTS missions' Autonomy, for instance, results in a worker having responsibility for its goals. To achieve these goals many self-* properties such as self-configuration will be necessary, as well as utilization of heart-beats, pulse signals and reflex reactions within AMs. NASA missions, such as ANTS, have Mission control and operations in a trusted private environment. This eliminates many of the wide range of agent and autonomic security issues briefly highlighted earlier, just leaving the particular concern is the agent operating in the correct context and exhibiting emergent behavior within acceptable parameters, whereupon apoptosis can make a contribution.

The ANTS architecture is itself inspired by biological low level social insect colonies with their success in the division of labor. Within their specialties, individual specialists generally outperform generalists, and with sufficiently efficient social interaction and coordination, the group of specialists generally outperforms the group of generalists. Thus systems designed as ANTS are built from potentially very large numbers of highly autonomous, yet socially interactive, elements. The architecture is self-similar in that elements and sub-elements of the system may also be recursively structured as ANTS [13], and as such the self-management architecture with at least an AM per ANT craft can abstractly fit with that portrayed for the Autonomic Systems paradigm.

The revolutionary ANTS paradigm makes the achievement of such goals possible through the use of many small, autonomous, reconfigurable, redundant element craft acting as independent or collective agents[14].

Let us consider the role of the self-destruct property, inspired by apoptosis, in the ANTS mission: suppose one of the worker agents was indicating incorrect operation, or when co-existing with other workers was the cause of undesirable emergent behavior, and was failing to self-heal correctly. That emergent behavior (depending on what it was) may put the scientific mission in danger. Ultimately the stay-alive signal from the ruler agent would be withdrawn[4].

Also, if a worker, or its instrument, were damaged, either by collision with another worker, or (more likely) with an asteroid, or during a solar storm, a ruler could withdraw the stay-alive signal and request a replacement worker. Another worker could self-configure to take on the role of the lost worker; i.e., the ANTS adapt to ensure an optimal and balanced coverage of tasks to meet the scientific goals.

If a ruler or messenger were similarly damaged, its stay-alive signal would also be withdrawn, and a worker would be promoted to play its role.

4. Strong vs Weak Apoptotic Computing

In our opinion Apoptotic Computing and the use of Apoptosis is "Death by Default" requiring periodic "Stay Alive" signals to prevent self-destruction/suicide. Although this may seem at first a subtle difference from sending a self-destruct signal/trigger to induce self-destruction it is fundamental. Only an inherent built in default death can guarantee safety for the scenarios touched on here. For instance, relying on sending a self-destruct signal/trigger to an agent containing system password updates that is now in a hostile environment – that signal will never get through. Likewise a Robot with adaptive capabilities may learn behaviour to ignore such a trigger. To boot, consider garbage collection first used in Lisp and many languages since or the destructor method on OO, is a death trigger for programmed death in principle any different? The true apoptosis is death by default with stay alive signals. That said we recognise not all circumstances will require the extreme death by default mechanism and as such we have utilized (also the biologically cell inspired) Quiescence (self-sleep) as a less drastic measure. As such programmed death triggered by a death signal may also be appropriate in some circumstances, although we believe many using it under the Apoptosis descriptor should really be using death by default. To distinguish the difference we refer to Death by Default with Stay Alive signs as Strong Apoptotic Computing and Programmed Death with death trigger as Weak Apoptotic Computing.

5. Robotic Apoptosis

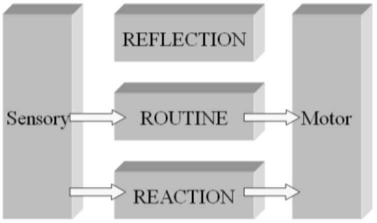

Figure 3 Intelligent machine architecture

Figure 3 recalls a high level architecture for an Intelligent Machine or Robot (adapted from [34], [26]). It describes three levels for the design of intelligent systems:

1. Reaction—lowest level, where no learning occurs but there is immediate response to state information coming from sensory systems.
2. Routine—middle level, where largely routine evaluation and planning behaviours take place. Input is received from sensors as well as from the reaction level and reflection level.
3. Reflection—top level, receives no sensory input or has no motor output; input is received from below. Reflection is a meta-process,

whereby the mind deliberates about itself. Essentially, operations at this level look at the system's representations of its experiences, its current behaviour, its current environment, etc.

Input from, and output to, the environment only takes place within the reflex and routine layers. One may consider that reaction level essentially sits within the "hard" engineering domain, monitoring the current state of both the machine and its environment, with rapid reaction to changing circumstances; and, that the reflection level may reside within the AI domain utilizing its techniques to consider the behavior of the system and learn new strategies. The routine level may be a cooperative mixture of both (*Figure 3*).

Rouff et.al. reflected on using Autonomic Computing for Robotics based on things that could go wrong as highlighted by Carlson and Murphy's work [30]-[32]. In this study they examined the results from 10 different robotic projects that used 15 different robot models, from small models that were 1 foot by 6 includes by 2 inches long to a modified M1 tank that was converted to tele-operation for experimental purposes. From this study they developed a taxonomy of how robots fail, which were categorized as either physical or human failures. The projects studied consisted of eight projects from the Test and Evaluation Office (TECO) at Fort Lenard Wood, robotic failures from two weeks during the World Trade Center rescue response that searched for survivors, and from the day to day use of robots over a two year period of time [29]. This work [30]-[32] mostly focused on tele-operated robotics, yet the self-configuring, healing, optimization and self-protecting autonomic properities were presented as a way forward [29].

If we consider the increasing amount of autonomy and adaptively planned for such systems the reflection (self-examination) on how well it is following its policies, scientific goals, mission level objectives and so on, is increasingly critical.

Ultimately self-monitoring/examination may not work due to conditions in the environment or individual sensors cannot sense (beyond its programmed and learnt scope) or learnt adaptive behavior, as is often the case in the biological environment, has self-denial that we are in the wrong or unhealthy, to the science fiction utopia or catastrophe coming singularity and intelligence explosion creating a new self-* property self*ish* and non desirable behavior means that there should be pre-programmed default mechanisms that are controlled/triggered beyond the 'self', that is, by having built in mechanism that will happen unless appropriate credentials are received from the environment. These environmental/societal controls are there to protect the overall system function and success and may be comparable to the Sci-Fi Asimov three laws of robotics [33]. The ultimate control is the apoptotic state.

6. Related Work

The Apoptotic Computing paradigm and Apoptosis concept has also been investigated by other researchers. Tschudin proposed utilizing apoptosis (programmed death) in highly distributed systems [16], "once triggered by some external event, a termination signal will propagate". Riordan and Alessandri proposed apoptosis (programmed death) as a means to automatically counter the increasing amount of security vulnerabilities published and which hackers make use of before systems administrators can close of the published vulnerability [17]. They propose an Apoptosis Service Provider that "should a vulnerability be found in name, secret is released into the environment to trigger various preconfigured responses (presumably to shut down name or to warn a responsible party). Lilien and Bhargava [18] utilize apoptosis as a means to protect the security of data, where it is activated when detectors determine a credible threat of a successful attack on the bundle (atomic bundle of private data as an agent or object) by any host, including the destination guardian of a bundle being transmitted. Burbeck [19] essentially presents a tutorial on parallels between biology and computing, and evolves four interconnected principles for Multicellular Computing; one being Apoptosis (programmed death), mentioning that a familiar example in computing is the Blue Screen of Death which is a programmed response to an unrecoverable error. A civilized metazoan (comparing with biological metazoan cell) computer should sense its own rogue behavior, e.g., download of uncertified code, and disconnect itself from the network. Olsen et al have developed a multi-agent system (named HADES) that is capable to control and protect itself via life protocols and a rescue protocol. Its life protocols control the replication, repair, movement, and self-induced death that govern each agent in the system [20]. Saudi et al [21] essentially discuss Apoptosis for security systems, specifically focusing on network problems, recovering ground highlighted in Burbeck[19] and go on to apply that to addressing worms [22]. Jones [23], in his master's dissertation, implemented apoptotic self-destruct and stay-alive signalling specifically investigating memory requirements of inheritance vs an abstract oriented approach (AOP). The majority of these works may be considered to fall into the weak Apoptotic Computing (programmed death & termination signals) area yet could benefit from utilizing strong Apoptitic Computing (programmed death by default & stay alive signals).

7. Conclusion

We have made the case previously that all computer-based systems should be Apoptotic [28], especially as we increasingly move into a vast pervasive and ubiquitous environment. This should cover all levels of interaction with technology from data, to services, to agents, to robotics. With recent headline incidents of credit card and personal data loses by organizations and governments to the Sci-Fi nightmare scenarios now being discussed as possible future, programmed death by default becomes a necessity.

We're rapidly approaching the time when new autonomous computer-based systems and robots should undergo tests, similar to ethical and clinical trials for new drugs, before they can be introduced, the emerging research from Apoptotic Computing and Apoptotic Communications may offer that safe-guard.

Acknowledgements

The author is supported by the University of Ulster's Computer Science Research Institute and School of Computing and Mathematics. Some of the research described in this paper is patented and patent-pending by Roy Sterritt (University of Ulster) and Mike Hinchey (Lero—the Irish Software Engineering Research Centre) through NASA and assigned to the US government.

References

[1] John Arlidge, "Scientists fear a revolt by killer robots" The Sunday Times, August 2, 2009.

[2] Eric Horvitz, Bart Selman, "Interim Report from Panel Chairs", AAAI Presidential Panel on Long Term AI Futures, August 2009. http://www.aaai.org/Organization/presidential-panel.php.

[3] R Sterritt, MG Hinchey, (Mar 2010) "SPAACE IV: Self-Properties for an Autonomous & Autonomic Computing Environment – Part IV A Newish Hope", Proceedings of AA-SES-IV: 4th IEEE International Workshop on Autonomic and Autonomous Space Exploration Systems (at SMC-IT), Pasadena, CA, USA, June 2009, in "Proceedings of the Seventh IEEE International Conference and Workshops on Engineering of Autonomic and Autonomous Systems (EASe 2010)", IEEE CS Press, Pages 119-125

[4] R Sterritt, MG Hinchey, (Dec 2004) "Apoptosis and Self-Destruct: A Contribution to Autonomic Agents?", Proceedings of Third NASA-Goddard/IEEE Workshop on Formal Approaches to Agent-Based Systems (FAABS III), Washington DC, April 26-27, 2004, in "LNAI 3228", Springer-Verlag, Pages 262-270, doi: 10.1007/978-3-540-30960-4_18

[5] R Sterritt, MG Hinchey, (Apr 2005) "Engineering Ultimate Self-Protection in Autonomic Agents for Space Exploration Missions", Proceedings of IEEE Workshop on the Engineering of Autonomic Systems (EASe 2005) at 12th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS 2005), Greenbelt, MD, USA, , 3-8 April, 2005, Pages 506-511

[6] R Sterritt, MG Hinchey, (Jun 2005) "From Here to Autonomicity: Self-Managing Agents and the Biological Metaphors that Inspire Them", Proceedings of Integrated Design & Process Technology Symposium (IDPT 2005), Beijing, China, 13-17 June, Pages 143-150

[7] R Sterritt, MG Hinchey, (May 2006) "Biologically-Inspired Concepts for Autonomic Self-Protection in Multiagent Systems", Proceedings of 3rd International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2006) at AAMAS 2006, Hakodate, Japan, 8 Ma

[8] J. Newell, "Dying to live: why our cells self-destruct," Focus, Dec. 1994.

[9] Y. Ishizaki, L. Cheng, A.W. Mudge, M.C. Raff, "Programmed cell death by default in embryonic cells, fibroblasts, and cancer cells," Mol. Biol. Cell, 6(11):1443-1458, 1995.

[10] M Sluyser, (ed) "Apoptosis in Normal Development and Cancer". Taylor & Francis, London, 1996

[11] R Sterritt, DW Bustard DW, "Towards an Autonomic Computing Environment", Proceedings of IEEE DEXA 2003 Workshops - 1st International Workshop on Autonomic Computing Systems, Prague, Czech Republic, September 1-5, 2003, Pages 694-698

[12] M.S. Greenberg, J.C. Byington, T. Holding, D.G. Harper, Mobile Agents and Security, IEEE Communications, July 1998.

[13] S. A., J. Mica, J. Nuth, G. Marr, M. Rilee, M. Bhat, ANTS (Autonomous Nano-Technology Swarm): An Artificial Intelligence Approach to Asteroid Belt Resource Exploration, Curtis, International Astronautical Federation, 51st Congress, October 2000.

[14] P.E. Clark, S. Curtis, M. Rilee, W. Truszkowski, J. Iyengar, H. Crawford, "ANTS: A New Concept for Very Remote Exploration with Intelligent Software Agents", Presented at 2001 Spring Meeting of the American Geophysical Union, San Francisco, 10-14 December 2001; EOS Trans. AGU, 82 (47), 2001.

[15] NASA ANTS Online, http://ants.gsfc.nasa.gov/

[16] C. Tschudin. Apoptosis - the programmed death of distributed services. In J. Vitek and C. Jensen, editors, Secure Internet Programming - Security Issues for Mobile and Distributed Objects, pp 253–260. Springer, 1999

[17] Riordan J, Alessandri D, "Target Naming and Service Apoptosis", in Debar H, Mé L, and Wu S, Recent Advances in Intrusion Detection (LNCS 1907), Springer, pp 217-225, 2000

[18] Lilien, L.; Bhargava, B.; , "A scheme for privacy-preserving data dissemination," Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on , vol.36, no.3, pp.503-506, May 2006
doi: 10.1109/TSMCA.2006.871655

[19] Burbeck, S., "Complexity and the Evolution of Computing: Biological Principles for Managing Evolving Systems". Whitepaper (V2.2), 2007.

[20] Olsen, M.M., Siegelmann-Danieli, N. & Siegelmann, H.T., "Robust artificial life via artificial programmed death", Artif. Intell., 172, pp.884-98, 2008.

[21] Saudi, M.M., Woodward, M., Cullen, A.J. & Noor, H.M., 2008. An overview of apoptosis for computer security. In Proc. International Symposium on Information Technology ITSim 2008., 2008.

[22] Saudi, M.M.; Cullen, A.J.; Woodward, M.E.; Hamid, H.A.; Abhalim, A.H.; , "An overview of STAKCERT framework in confronting worms attack," Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on , vol., no., pp.104-108, 8-11 Aug. 2009
doi: 10.1109/ICCSIT.2009.5234764

[23] Jones D, "Implementing biologically-inspired Apoptotic behaviour in digital objects: An Aspect-Oriented Approach", MSc Dissertation, Open University UK, March 2010

[24] Sterritt, R., Towards Autonomic Computing: Effective Event Management*, Proceedings of 27th Annual IEEE/NASA Software Engineering Workshop (SEW)*, Maryland, USA, December 3-5, IEEE Computer Society, pp 40-47.

[25] Sterritt, R. and Bustard, D.W., Autonomic Computing: a Means of Achieving Dependability? *Proceedings of 10th IEEE International Conference on the Engineering of Computer Based Systems (ECBS '03)*, Huntsville, Alabama, USA, April 7-11, IEEE CS Press, pp 247-251.

[26] Sterritt, R., Pulse Monitoring: Extending the Health-check for the Autonomic GRID. *Proceedings of IEEE Workshop on Autonomic Computing Principles and Architectures (AUCOPA 2003) at INDIN 2003*, Banff, Alberta, Canada, 22–23 August, pp 433–440.

[27] J. Klefstrom, E.W. Verschuren, G.I. Evan, c-Myc Augments the Apoptotic Activity of Cytosolic Death Receptor Signaling Proteins by Engaging the Mitochondrial Apoptotic Pathway, *J. Biol Chem*,. **277**:43224-43232, 2002.

[28] Sterritt R, "Apoptotic Computing", IEEE Computer, January 2011 . pp. 37-43

[29] Christopher Rouff, James Rash, Walter Truszkowski, "Overcoming Robotic Failures through Autonomicity," ease, pp.154-162, Fourth IEEE International Workshop on Engineering of Autonomic and Autonomous Systems (EASe'07), 2007

[30] J. Carlson and R. R. Murphy. Reliability analysis of mobile robots. In Proceedings of the 2003 IEEE International Conference on Robotics and Automation (ICRA 2003), pages 274–281, Taipei, Taiwan, 14–19 September 2003. IEEE.

[31] J. Carlson and R. R. Murphy. How ugvs physically fail in the field. IEEE Transactions on Robotics, 21(3):423–437, June 2005.

[32] J. Carlson, R. R. Murphy, and A. Nelson. Follow-up analysis of mobile robot failures. In Proceedings of the 2004 IEEE International Conference on Robotics and Automation (ICRA 2004), Barcelona, Spain, 18–22 April 2004. IEEE.

[33] Issac Asimov, "Runaround" March 1942 Astounding Science Fiction, March 1942.

[34] Norman, D.A., Ortony, A. and Russell, D.M., Affect and Machine Design: Lessons for the Development of Autonomous Machines, *IBM Systems Journal*, 42(1):38–44.