Engineering Ultimate Self-Protection in Autonomic Agents for Space Exploration Missions

Roy Sterritt
School of Computing and Mathematics,
Faculty of Engineering
University of Ulster
Northern Ireland
r.sterritt@ulster.ac.uk

Mike Hinchey
NASA Goddard Space Flight Center
Software Engineering Laboratory
Greenbelt, MD 20771
USA
michael.g.hinchey@nasa.gov

Abstract

NASA's Exploration Initiative (EI) will push space exploration missions to the limit. Future missions will be required to be self-managing as well as self-directed, in order to meet the challenges of human and robotic space exploration. We discuss security and self-protection in autonomic agent based-systems, and propose the ultimate self-protection mechanism for such systems—self-destruction. Like other metaphors in Autonomic Computing, this is inspired by biological systems, and is the analog of biological apoptosis. Finally, we discuss the role it might play in future NASA space exploration missions.

Keywords: Autonomic Computing, Autonomic Agents, Exploration, Self-Protection, Self-Destruction, Pulse Monitoring, Apoptosis.

1. Introduction

It's been almost four decades since any human has ventured beyond the confines of Earth and set foot on another heavenly body. Twice in the last decade, Shuttle tragedies, resulting in the loss of the entire crew, have meant significant set-backs for the space program, and in particular human exploration.

Yet man's fascination, almost obsession, with space and the other planets in our solar system has remained undaunted. The very idea that there may be some form of life somewhere "out there" continues to fuel our imagination and our desire for exploration. At the time of writing, Cassini has reached Titan, the most important of Saturn's moons, we have been thrilled by the progress on the Mars rovers on the Martian surface, and the DAWN mission will explore Ceres and Vesta, at the extreme outposts of our solar system.

The Exploration Initiative (EI), which will include both human and robotic exploration of space, aims to put man back on the moon, and, ultimately, to put the first human on Mars. The protection of valuable resources (the most precious of which is human life), while achieving the complex goals of the initiative, poses significant challenges.

In the remainder of this paper, we will describe some NASA experiences with autonomous and autonomic systems, and propose the ultimate self-protection mechanism for space exploration missions (and other systems): the use of biological *apoptosis* as a metaphor within autonomic agents to provide a dynamic health indicator signal, and a self-destruction mechanism.

2. Exploration Challenges

The EI poses some of the most significant challenges that NASA, or anyone, has had to address.

Exploration will involve complex tasks and procedures that must be fully automated, even though we have not yet fully formulated all of the requirements.

New paradigms in spacecraft design are leading to radical changes in the way NASA designs spacecraft operations [1]. Increasing constraints on resources, and greater focus on the cost of operations, has led NASA to utilize adaptive operations and move towards almost total onboard autonomy in certain classes of mission operations [2],[3].

Almost entirely autonomous decision-making will be necessary to overcome the unacceptable time lag between a craft encountering new situations and the round-trip delay (of upwards of 40 (Earth) minutes) in obtaining responses and guidance from mission control.

More and more NASA missions will, and *must*, incorporate autonomicity as well as autonomy [4],[5]. In short: as missions increasingly incorporate autonomy

– being self-governing of their own goals – there is a strong case to be made that this needs to be extended to include autonomicity – that is, that there is self-management of the mission.

2.1 Autonomy in NASA Missions

Two of the first notable NASA missions to incorporate autonomy were DS1 (Deep Space 1) and the Mars Pathfinder [6].

In the DS1 mission [7] the responsibility of health monitoring was transferred from ground to spacecraft [8]. This marked a paradigm shift for NASA from its traditional routine telemetry downlink and ground analysis, to onboard health determination [7].

Some longer-term drawbacks of the approach were discovered. As one of the primary goals was to reduce the amount of data sent to the ground (achieved by eliminating the download of telemetry data), operators lost the ability to gain an intuitive feel for the performance and characteristics of the craft and its components, as well as losing the ability to run the data through simulations [1].

To resolve this, engineering data summarization was introduced to facilitate ground study of the long-term behavior of the spacecraft [9]. This now represented a *fast loop* of real-time health assessment, supplemented by a *slow loop* to study the long-term behavior of the spacecraft. Specifically the *engineering data summarization* is a set of abstractions regarding the sensor telemetry, which is then sent back to ground to provide the missing context for operators. This dual approach has conceptually much in common with the biological reflex and healing approach [8],[10].

2.2 Future NASA Autonomic Systems

The Autonomic Computing initiative has been identified by NASA as having potential to contribute to their goals of autonomy and cost reduction in future space exploration missions [3]-[5],[10].

Autonomic Computing is a metaphor based on the biological Autonomic Nervous System (ANS) [11], taking the ANS as inspiration to achieve self-managing computer-based systems without "conscious effort" from the user. The initiative's initial set of self-properties (self-configuration, self-healing, self-optimization and self-protection through self-awareness, self-monitoring and self-adjusting) have been expanded to include many self-* properties leading to the adoption of the term *selfware*.

Certain missions will *require* autonomic properties if they are to succeed. ANTS (Autonomous Nano-Technology Swarm), for example, is a mission that will launch sometime between 2020 and 2030—"any day now" in terms of NASA missions. The mission is viewed as an exemplar for how many future unmanned missions will be developed and how future space exploration will exploit autonomous and autonomic behavior.

One such mission (ANTS) will involve the launch of a 1000 pico-class spacecraft swarm from a stationary factory ship, on which the spacecraft will be assembled. The spacecraft will explore the asteroid belt from close-up, something that cannot be done with conventionally-sized spacecraft.

As much as 60% to 70% of the spacecraft will be lost on first launch as they enter the asteroid belt. The surviving craft will work as a swarm, forming smaller groupings of *worker* craft (each containing a unique instrument for data gathering), a coordinating *ruler*, that will use the data it receives from workers to determine which asteroids are of interest and to issue instructions to the workers and act as a coordinator, and *messenger* craft which will coordinate communications between members of the swarm and between the swarm and ground control. Communications with Earth will be limited to the download of science data and status information, and requests for additional craft to be launched from Earth as necessary.

3. Autonomic Computing and Agents

Autonomic Computing is dependent on many disciplines for its success; not least of these is research in agent technologies. At this stage, there are no assumptions that agents have to be used in an autonomic architecture, but as in complex systems there are arguments for designing the system with agents [12], as well as providing inbuilt redundancy and greater robustness [13], through to retrofitting legacy systems with autonomic capabilities that may benefit from an agent approach [14].

Emerging research suggests that the autonomic manager may be an agent itself, for instance, an agent termed a *self-managing cell* (SMC) [15], containing functionality for measurement and event correlation and support for policy-based control.

Essentially, the aim of autonomic computing is to create robust dependable self-managing systems [16]. To facilitate this aim, fault-tolerant mechanisms such as a heart-beat monitor ('I am alive' signals) and pulse monitor (urgency/reflex signals) may be included within the autonomic element [8],[10]. The notion behind the pulse monitor (PBM) is to provide an early warning of a condition so that preparations can be made to handle the processing load of diagnosis and planning a response,

including diversion of load. Together with other forms of communications it creates dynamics of autonomic responses [17] – the introduction of multiple loops of control, some slow and precise, others fast and possibly imprecise, fitting with the biological metaphor of reflex and healing [10].

4. Biological Apoptosis

The biological analogy of autonomic systems has been well discussed in the literature. While reading this the reader is not consciously concerned with their breathing rate or how fast their heart is beating. Achieving the development of a computer system that can self-manage without the conscious effort of the user is the overarching vision of the Autonomic Computing initiative [18]. Another typical biological example is that the touching of a sharp knife results in a reflex reaction to reconfigure the area in danger to a state that is no longer in danger (self-protection, self-configuration, and, if damage has occurred, self-healing) [19].

If you cut yourself and it starts bleeding, you will treat it and carry on with your tasks without any further conscious thought. Yet, often, the cut will have caused skin cells to be displaced down into muscle tissue [20]. If they survive and divide, they have the potential to grow into a tumor. The body's solution to dealing with this situation is cell self-destruction. There is mounting evidence that cancer is the result of cells not dying fast enough, rather than multiplying out of control, as previously thought.

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 self-destruction is delayed due to the continuous receipt of biochemical reprieves. This process is referred to as *apoptosis* [21], meaning "drop out", and was used by the Greeks to refer to the 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" [22], where cells are prevented from putting an end to themselves due to constant receipt of biochemical "stay alive" signals.

Further investigations into the apoptosis process [23] have discovered more details about the self-destruct predisposition. 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 tumor, while simultaneously a cell *must* divide in order to build and maintain a body.

The suicide and reprieve controls have been compared to the dual-key on a nuclear missile [20]. 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 [20].

5. The Role of Apoptosis within Agents

Agent destruction has been proposed for mobile agents to facilitate security measures [24]. Greenberg *et al.* highlighted the situation 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 [25]. 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 [25]. This situation has similar overtones to our previous discussion on biological apoptosis, where the body is at its most vulnerable during cell division.

We have established the concepts of the HBM and PBM: Heart-Beat Monitor (*I am alive*) a fault-tolerant

mechanism which may be used to safeguard the autonomic manager to ensure that it is still functioning by periodically sending 'I am alive' signals. Pulse Monitor (*I am healthy*) extends the HBM to incorporate reflex/urgency/health indicators from the autonomic manager, representing its view of the current self-management state. The analogy is with measuring the pulse rate instead of merely detecting its existence.

Apoptosis (*Stay alive*) a proposed additional construct used to safeguard the system and agent; a signal indicates that the agent is still operating within the correct context and behavior, and should not self-destruct.

Is there a role for the apoptosis metaphor in the development of autonomic agents? [26]

With many security issues, the lack of an agreed standard approach to agent-based systems prohibits, for now, further practical development of the use of apoptosis for agent security in a generic fashion within autonomic systems. We will now, however look at the role of apoptosis in NASA missions.

6. Apoptosis in NASA Missions

Of course, with NASA missions, such as ANTS, we are not considering a generic situation. Mission control and operations is a trusted private environment. This eliminates many of the wide range of agent security issues discussed earlier, just leaving the particular concerns; namely, is the agent operating in the correct context and showing 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 [27].

Targets for ANTS-like missions include surveys of extreme environments on the Earth, Moon, or Mars, as well as asteroid, comet, or dust populations. 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 [28].

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.

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.

All of the spacecraft are powered by batteries that are recharged by the sun using solar sails [3],[5]. Although battery technology has greatly advanced, there is still a "memory loss" situation, whereby batteries that are continuously recharged eventually lose some of their power and cannot be recharged to full power. After several months of continual operation, each of the ANTS will no longer be able to recharge sufficiently, at which point their stay-alive signals will be withdrawn, and new craft will need to be assembled or launched from Earth.

7. Conclusions

Space Exploration Missions, through necessity, have been incorporating more and more Autonomy. Autonomy may be considered as self-governance of ones own tasks/goals. In terms of ANTS missions this for instance results in a *worker* having responsibility for its goals. To achieve these goals many self-* properties such as self-configuration may be necessary.

The overarching vision of Autonomicity may be considered self-management through utilizing self-* properties. As such Autonomy and Autonomicity may share common ground, while Autonomicity adds additional responsibility to achieving one's goals – the shared responsibility of managing the mission.

This paper presented an analogy from biological systems, *Apoptosis,* and its value in future autonomic systems lies in providing an ultimate protection mechanism— *self-destruct.*

Agents are well-accepted as a means of implementing autonomy. In terms of the Autonomic initiatives, agent

technologies also have the potential to become an intrinsic approach [29]-[31].

A major concern with Autonomy is the emergence of undesirable behaviors and race conditions. Formal approaches to agent-based systems [32],[33] has a primary focus of identifying these race conditions, highlighting undesirable emergent behavior, and verifying the correctness of systems. However, under certain circumstances race conditions and undesirable behavior may still occur and it may not be possible to self-correct. In this situation, the self-destruction of the agent may be viewed as a last resort scenario to prevent further damage and endangerment of the mission.

Acknowledgements

The development of this paper was supported at University of Ulster by the Centre for Software Process Technologies (CSPT), funded by Invest NI through the Centres of Excellence Programme, under the EU Peace II initiative. Acknowledgement is also due to Gerry Clarke, an M.Sc. Informatics student at the University of Ulster.

Part of this work has been supported by the NASA Office of Systems and Mission Assurance (OSMA) through its Software Assurance Research Program (SARP) project, Formal Approaches to Swarm Technologies (FAST), and by NASA Goddard Space Flight Center, Software Engineering Laboratory (Code 581).

References

[1] M.A. Swartwout, *Engineering Data Summaries for Space Missions*, SSDL, 1998.

[2] J. Wyatt, R. Sherwood, M. Sue, J. Szijjarto, Flight Validation of On-Demand Operations: The Deep Space One Beacon Monitor Operations Experiment, In *Proceedings 5th International Symposium on Artificial Intelligence, Robotics and Automation in Space (i-SAIRAS '99)*, ESTEC, Noordwijk, The Netherlands, 1-3 June, 1999.

[3] W. Truszkowski, M. Hinchey, J. Rash and C. Rouff, NASA's Swarm Missions: The Challenge of Building Autonomous Software, *IEEE IT Professional*, September/October 2004, pp 51-56.

[4] W. Truszkowski, M. Hinchey, C. Rouff and J. Rash, Autonomous and Autonomic Systems: A Paradigm for Future Space Exploration Missions, *IEEE Trans. on Systems, Man and Cybernetics, Part C*, to appear.

[5] W. Truszkowski, J. Rash, C. Rouff and M. Hinchey, Asteroid Exploration with Autonomic Systems, In Proceedings *of IEEE Workshop on the Engineering of Autonomic Systems (EASe 2004) at the 11th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS 2004)*, Brno, Czech Republic, 24-27 May 2004, pp 484-490.

[6] N. Muscettola,cP. P. Nayak, B. Pell, and B. Williams, Remote Agent: To Boldly Go Where No AI System Has Gone Before, *Artificial Intelligence* **103**(1-2):5-48, 1998.

[7] J.Wyatt, H. Hotz, R. Sherwood, J. Szijjaro, M. Sue, Beacon Monitor Operations on the Deep Space One Mission, In *Proceedings 5th Int. Sym. AI, Robotics and Automation in Space*, Tokyo, Japan, 1998.

[8] R. Sterritt, Towards Autonomic Computing: Effective Event Management, In *Proceedings of 27th Annual IEEE/NASA Software Engineering Workshop (SEW-27)*, Greenbelt, MD, USA, December 3-5 2002, IEEE Computer Society Press, pp 40-47.

[9] R. Sherwood, J. Wyatt, H. Hotz, A. Schlutsmeyer, M. Sue, Lessons Learned During Implementation and Early Operations of the DS1 Beacon Monitor Experiment, In *Proceedings of the Third International Symposium on Reducing the Cost of Ground Systems and Spacecraft Operations*, Tainan, Taiwan, 1999.

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

[11] P. Horn, Autonomic Computing: IBM Perspective on the State of Information Technology," IBM T.J. Watson Labs, NY, 15th October 2001. Presented at AGENDA 2001, Scottsdale, AZ (available at http://www.research.ibm.com/autonomic/), 2001.

[12] N.R. Jennings, M. Wooldridge, Agent-oriented Software Engineering, In J. Bradshaw (ed.), *Handbook of Agent Technology*, AAAI/MIT Press, Cambridge, 2000.

[13] M.N. Huhns, V.T. Holderfield, R.L.Z. Gutierrez, Robust Software via Agent-Based Redundancy, In *Proceedings Second International Joint Conference on Autonomous Agents & Multiagent Systems, AAMAS 2003*, July 14-18, 2003, Melbourne, Victoria, Australia, pp 1018-1019.

[14] G. Kaiser, J. Parekh, P. Gross, G. Valetto, Kinesthetics eXtreme: An External Infrastructure for Monitoring Distributed Legacy Systems, In *Proceedings Autonomic Computing Workshop – IEEE Fifth Annual International Active Middleware Workshop*, Seattle, USA, June 2003.

[15] E. Lupu, et al., EPSRC AMUSE: Autonomic Management of Ubiquitous Systems for e-Health, 2003.

[16] R. Sterritt, D.W. Bustard, Autonomic Computing: a Means of Achieving Dependability?, In *Proceedings of IEEE International Conference on the Engineering of Computer Based Systems (ECBS 2003)*, Huntsville, Alabama, USA, April 7-11 2003, IEEE Computer Society Press, pp 247-251.

[17] R. Sterritt, D.F. Bantz, PAC-MEN: Personal Autonomic Computing Monitoring Environments, In *Proceedings of IEEE DEXA 2004 Workshops - 2nd International Workshop on Self-Adaptive and Autonomic Computing Systems (SAACS '04)*, Zaragoza, Spain, August 30 – 3 September, 2003.

[18] J. O. Kephart and D. M. Chess. The Vision of Autonomic Computing, *Computer*, **36**(1):41–52, 2003.

[19] R. Sterritt, D.W. Bustard, Towards an Autonomic Computing Environment, In *Proceedings of IEEE DEXA 2003 Workshops - 1st International Workshop on Autonomic Computing Systems*, Prague, Czech Republic, September 1-5, 2003, IEEE Computer Society Press, pp 694-698.

[20] J. Newell, Dying to Live: Why our Cells Self-Destruct, *Focus*, December 1994.

[21] R. Lockshin, Z. Zakeri, Programmed Cell Death and Apoptosis: Origins of the Theory, *Nature Reviews Molecular Cell Biology*, **2**:542-550, 2001.

[22] 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.

[23] 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.

[24] J.D. Hartline, *Mobile Agents: A Survey of Fault Tolerance and Security*, University of Washington, 1998.

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

[26] R. Sterritt, M. G. Hinchey, Apoptosis and Self-Destruct: A Contribution to Autonomic Agents? In *Proceedings FAABS-III, 3rd NASA/IEEE Workshop on Formal Approaches to Agent-Based Systems (April 2004)*, Greenbelt, MD, Springer Verlag LNCS **3228**, 2005.

[27] 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.

[28] 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.

[29] J. McCann, M. Huebscher, *Evaluation Issues in Autonomic Computing*, Proceedings of the International Workshop on Agents and Autonomic Computing and Grid Enabled Virtual Organizations (AAC-GEVO'04), 3rd International Conference on Grid and Cooperative Computing Wuhan, China, 21-24 October, Springer-Verlag .LNCS **3252**, 2004, pp 597-608.

[30] J.P. Bigus, D.A. Schlosnagle, JR. Pilgrim, W.N. Mills III, Y. Diao, ABLE: a Toolkit for Building Multiagent Autonomic Systems, *IBM Systems J.*, **41**(3):350-371, 2002.

[31] G. Tesauro, D.M. Chess, W.E. Walsh, R. Das, "A Multi-Agent Systems Approach to Autonomic Computing", *AAMAS'04*, July 19-23, 2004, New York, USA.

[32] C.A. Rouff, M. G. Hinchey, W. Truszkowski, J.L. Rash and D. Spears, editors, *Agent Technology from a Formal Perspective*, NASA Monographs in Systems and Software Engineering, Springer Verlag, London, 2005.

[33] W. Truszkowski, C.A. Rouff, H.L. Hallock, J. Karlin, J.L. Rash, M.G. Hinchey and R. Sterritt, *Autonomous and Autonomic Systems: With Applications to NASA Intelligent Spacecraft Operations and Exploration Systems*, NASA Monographs in Systems and Software Engineering, Springer Verlag, London, 2005.