Autonomic computing meets SCADA security

Nazir, Sajid; Patel, Shushma; Patel, Dilip

Published in:
IEEE 16th International Conference on Cognitive Informatics and Cognitive Computing

DOI:
10.1109/ICCI-CC.2017.8109795

Publication date:
2017

Document Version
Peer reviewed version

Link to publication in ResearchOnline

Citation for published version (Harvard):
Nazir, S, Patel, S & Patel, D 2017, Autonomic computing meets SCADA security. in *IEEE 16th International Conference on Cognitive Informatics and Cognitive Computing.* IEEE. https://doi.org/10.1109/ICCI-CC.2017.8109795

Autonomic Computing Meets SCADA Security

Sajid Nazir
Firstco Ltd.
London, W2 6EU
United Kingdom
sajid.nazir@firstco.uk.com

Shushma Patel, Dilip Patel
School Of Engineering
London South Bank University
London, SE1 0AA, UK
{shushma, dilip}@lsbu.ac.uk

***Abstract*— National assets such as transportation networks, large manufacturing, business and health facilities, power generation, and distribution networks are critical infrastructures. The cyber threats to these infrastructures have increasingly become more sophisticated, extensive and numerous. Cyber security conventional measures have proved useful in the past but increasing sophistication of attacks dictates the need for newer measures. The autonomic computing paradigm mimics the autonomic nervous system and is promising to meet the latest challenges in the cyber threat landscape. This paper provides a brief review of autonomic computing applications for SCADA systems and proposes architecture for cyber security.**

Keywords—Critical infrastructures; Machine learning; Cyber attacks; Architecture; Autonomic computing; SCADA security.

I. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control complex infrastructures of national importance such as transportation networks, power generation and manufacturing plants. Even the smallest intrusions on the critical infrastructure controls, can result in malfunctions which have devastating ripple effects on the system as a whole.

Traditionally, SCADA systems have been developed as closed systems [1] with security being the overriding factor, with no Internet connectivity. However, to leverage efficiency and gain a competitive advantage, the systems are increasingly becoming connected to the Internet and cloud technologies [2]. SCADA system security vulnerabilities were first highlighted by the Stuxnet [3] attack. Subsequently, there has been an increase in the frequency and sophistication as evidenced by the recent attacks [4].

Isolation and obscurity [5] as a mechanism for protection is no longer an option for critical infrastructures. At the same time systems are getting so complex that it is difficult to develop effective defence strategies, as there is a lesser understanding of the complex interactions between the many system entities. The systems complexity and interactions as a result of interconnectivity goes beyond the capability of system developers and integrators [6]. Thus increasingly there is a lack of full understanding of the system which makes it very difficult to tune a system and to make decisions in case of changed requirements.

This has led to a realization that conventional and rigid techniques will not help. What is needed is a new way of looking at the problem of cyber security that is robust, manageable and self-realising with a minimum requirement to monitor systems to make decisions. What is proposed is an entirely new way of thinking about the problem where the system itself is intelligent and helps to maintain and extend its behaviour, with the use of autonomic computing [6].

The term ‘Autonomic Computing’ was first used by IBM in 2001 to combat the looming complexity crisis [7]. The concept has been inspired by human biological autonomic system. An autonomic system is self-healing, self-regulating, self-optimising and self-protecting [7]. Therefore, the system should be able to protect itself against both malicious attacks and unintended mistakes by the operator. We propose to generally use the autonomic computing paradigm features to SCADA system security, in particular focussing on self-protecting SCADA systems.

The basic principles of autonomic computing are very much applicable to increasingly complex SCADA system protection because: (i) The boundaries between physical and virtual systems have been blurred through virtualisation. It is possible to host a cluster of machines in a virtual environment; (ii) Even with hardware there are sufficient advances in other domains with self-healing materials; (iii) Advances in machine learning and artificial intelligence, for protection, and the knowledge base needs to be capitalised; (iv) The systems are highly interconnected and the distributed nature of systems poses an exponential complexity.

There has been some research on autonomic computing application to complex SCADA systems. The application of autonomic computing for smart grids has been discussed [8] as a solution to manage system complexities. Key components of a self-protecting SCADA system have been proposed and a survey of techniques provided for the realisation of such systems [9]. Also, there are few dedicated research groups [10], [11] focusing research on the applicability. JADE [12] provides a framework for building autonomic management systems. A test bed was developed [10][13] for modelling critical infrastructures for testing autonomic technologies. However, there is a lot of work required before the full potential of autonomic computing for SCADA security can be realised.

This paper reviews the literature relating to the application of autonomic computing to SCADA system protection and proposes an architecture that can support cyber security against emerging threats providing support at various stages or layers.

The rest of this paper is organized as follows: Section II outlines the relevant background on SCADA security aspects.

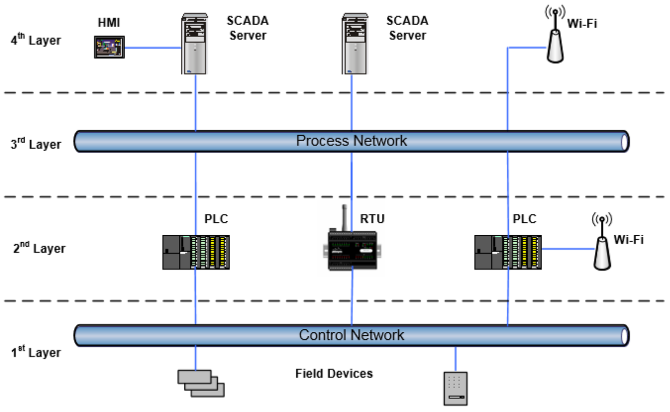

Fig. 1. Simplified Layered Architecture of a SCADA system.

Threat landscape and the need for better protective techniques are described in Section III and IV. Section V provides the relevant information on autonomic computing. The proposed architecture is presented in Section VI and finally Section VII concludes the paper.

II. SCADA AS SYSTEMS OF SYSTEMS

SCADA systems have been adopting the latest trends and innovations, such as virtualisation, analytics and databases, and wireless communications, which must work together in close collaboration to achieve the system mission. SCADA databases contain big data [14] and need sophisticated techniques for timely and meaningful inferences to detect outliers. The integrated framework can rightly be called systems of systems as the complexity has increased beyond simple control and monitoring tasks, the fundamental basis of SCADA. This complexity implies that developing and maintaining such systems are reaching the limits of human cognition [6][15].

A. *System Architecture*

A SCADA system can be visualised as a layered architecture, as shown in Figure 1. The field devices (sensors etc.) at the lowest layer interact with the physical processes. At layer 2, The Programmable Logic Controllers (PLC), and Remote Terminal Units (RTUs) aggregate data values from the lower layer and communicate the commands and their responses through the communications network to the SCADA server and Human Machine Interface (HMI). It is through the generation of commands at the top layer and collection of responses from the lowest layer that result in monitoring and control of the process.

B. *SCADA System Characteristics*

- SCADA applications are hosted on generic operating systems and tend to have a long operational lifetime.
- With lots of added features the systems complexities have increased and are thus difficult to maintain [1].
- The systems remain in continuous operation and have a range of redundancies incorporated to protect stalling the system for foreseeable problems.
- The command and response relies on tight timing constraints.
- The system is susceptible to attacks with minor effects, which can alter the system behaviour in a negative manner, leading to a ripple effect that compromises the whole system.

III. THREAT LANDSCAPE

The threat landscape is rapidly evolving and has gained momentum where the state and non-state agents are trying to exploit the system's vulnerabilities. For detailed threat ontologies please refer to [13]. There are many paths to exploitation but the threats can be categorised into the following main categories:

A. *Internet Connectivity*

The protection offered through an unconnected SCADA system is not there anymore. The benefits are too lucrative to be ignored by vendors and industry. Unfortunately it comes at an increased threat exposure.

B. *Cloud Computing*

The increasing reliance of moving the computing and networking assets to the cloud could create a hurdle for a SCADA system. Although this depends upon the amount of data moved to the cloud it definitely imposes certain system constraints to be violated, in case of disconnection from data stored in remote cloud infrastructure.

C. *Wireless Communications*

There are many publicly available tools that can capture network traffic wirelessly. Also the wireless devices that feed data to the SCADA system provide easy entry points for the intruder into the system because the end devices do not have adequate protection, due to very low power requirements.

D. *System Composition*

There are many complex technologies underpinning a modern SCADA system. The system interactions are complex and open new threat entry points as there are many third party libraries and hardware assembled with components from around the world, with exploitable threats such as backdoors, often unknown to the SCADA system vendor.

E. *Social Engineering Attacks*

Sophisticated attacks where the passwords and other details are stolen posing as an authorised agent or person. Threats could also emanate from an innocent or deliberate mistake from an insider. In the current threat scenario, ransomware may be a motivation to exploit a system. Although WannaCry [16] did not specifically target a SCADA system but raises a lot of questions about SCADA systems vulnerabilities that could make them lucrative target for ransomware.

IV. Need for better Protective Measures

System protection can be ensured through many techniques. The majority depend on the judgement of a human to provide safeguards for the system.

The cyber attack paradigms have progressed much beyond the simple attack methodologies such as man-in-the-middle (MITM), Denial of Service (DOS) attacks [9] and are waged with increasing sophistication to hide detection. The traditional defence approaches such as firewalls are unable to cope with the latest attack methodologies where for example, the system parameters are altered, and are individually legitimate, but on the whole result in system collapse. Firewall configuration is a complicated task that requires automated setting as proposed in [17].

Machine learning and other such techniques can effectively analyse a system to detect anomalous activity in a system. Such unsupervised anomaly detection schemes are more appropriate and efficient compared to human analysts [18] and other signature based approaches [9]. The system can thus learn new approaches and provide defence against as yet unseen scenarios, as in case of supervised learning approaches. The other techniques of interest could be based on agent based, artificial intelligence, and adaptive systems [8]. The future of cyber security lies with exploiting such techniques that can not only autonomously assess the threats to the system security, but also contain and mitigate the threat from spreading resulting in more damage. The operator alert can notify the human operator to initiate disaster recovery operations.

A recent breakthrough in this direction is that of the Autonomic Computing paradigm. With Autonomic Computing, the ultimate control still rests with a human but the drudgery of data manipulation and threat assessment can be taken out of the loop. Autonomic computing has been applied for resource optimisation for cloud [19] arguing that the traditional management techniques cannot handle availability and security, these being complex problems for traditional approaches.

Autonomic computing systems have four main features: self-configuring; self-healing; self-optimising; and self-protecting [7].

V. Autonomic Computing Paradigm

The core of the Autonomic Computing paradigm is that the system should be intelligent to enable it to develop and maintain itself in an optimised state.

A. Basis in Human Nervous System

The human body's feedback and control mechanisms [6][20] have formed the basis of general systems theory and holism for the development and management of computer based systems. The autonomic computing paradigm mimics the autonomic human nervous system. The ability to self-manage SCADA system security threats by developing learning systems that recognise vulnerabilities will be hugely advantageous. The agents and software services will form a part of the systems, gathering data and monitoring systems continuously [21].

B. Basic Functions

Autonomic computing can result from the use of different technologies; however an autonomic system must demonstrate the following features [7]:

1) Self-configuring: The system must be able to reconfigure its behaviour based on the changing system requirements. For example, to acquire more system resources, such as memory, in case the system is overburdened.

2) *Self-healing:* In response to detecting a compromised element in its configurtion, or lack of resources, an autonomic system can respond by repairing itself to a good state. Based on this assessment the system should be able to, for example, isolate the system components that have been compromised and continue operation with the remaining elements and at the same time attemping to restore the compromised system elements.

3) Self-optimising: The system must be able to assess the current state of the system variables and be abe to tune them to result in an optimised tuned behaviour. This is crucial as in the case of complex systems there are thousands of system parameters that can affect the system performance. Knowing or applying them all for best results is beyond the grasp of human mind, in a resonable amount of time.

4) Self-protecting: The system should be aware of the normal system operation and be able to continuously monitor the current system state to determine when deviations occur. It can then take measures to contain the threat and take measures to handle it

C. Application for SCADA Security

Autonomic computing facilitates identifying factors that relate to a specific state – homeostasis. The development of a knowledge network will help to identify what 'homeostasis' is and when there is an imbalance, to understand the structure of the network, the defences, the threats and the attacks. The threats can be classified into two categories: 1) process-related: when valid credentials are used to make legitimate changes that can impact on industrial processes. These can also be due to an error in the input of incorrect values or an actual attack [22] by, for example, disgruntled employees; and 2) system-related: which are exploited via software or configuration vulnerabilities. For example, flaws in communication protocols, which are low level (layers 1 and 2) attacks on the SCADA architecture [23]. Developing a mechanism to mine logged data on process-related incidents is a potential solution to developing an autonomic computing approach for SCADA security. Identifying user activities and classifying the actions into signed-on or known user actions allows the analysis of threats as legitimate system commands by legitimate users, or by illegitimate users, to distinguish the threats into attacks or errors by developing a knowledge base. [24].

The work to date for securing SCADA security focuses on discrete approaches. However, we propose an integrated approach that combines, the discrete knowledge based approaches with cognitive approaches. The memory

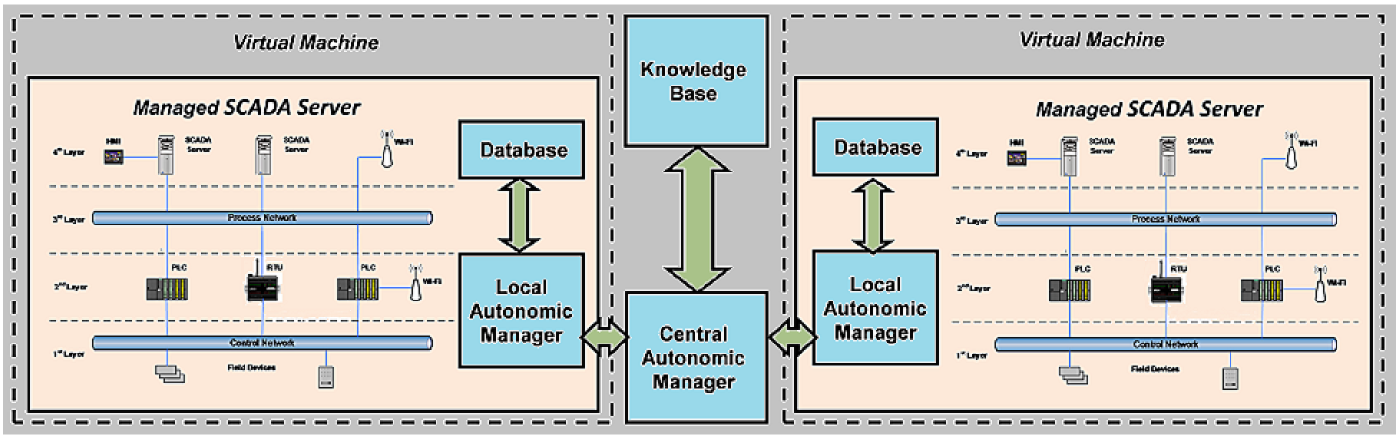

Fig 2. Proposed Architecture for an autonomic SCADA system.

layer of the Layered Reference Model of the Brain (LRMB) (layer 2), reflects the knowledge base that captures the short term, long term and transient memories. This can be utilised to capture process- and systems-related threats. Memory can be defined as a set of subconscious cognitive processes that retains the external or internal information about various SCADA security events. The subconscious knowledge base is inherited from the range of events and threats identified, and the conscious subsystem, however, is acquired and flexible, based on the autonomic computing paradigm [25][26].

Thus the autonomic paradigm holds great promise to address the general security problems associated with the SCADA systems.

VI. Autonomic Architecture for SCADA Security

A. *SCADA Features*

Some recent technology adoptions and improvements in the SCADA systems are promising to aid developing systems that can result in an autonomic SCADA system.

1) Databases: Most SCADA vendors allow integration with relational databases in addition to the built-in Historian databases that have some advantages [27]. Relational databases such as Oracle have their own integrated analytics and data mining services that can make it easier to uncover any anomalous activity.

2) Machine Learning: The machine learning and data analytics techniques have revolutionised many application domains and and have recently been introduced in SCADA applications software. Such native integration makes it easier for the SCADA developers to analyse the system operation and identify impending attacks [28][29].

3) Virtualisation: Virtualisation techniques provide many benefits that can advantageously be applied to support the autonomic computing paradigm. Virtualisation enables easy containment of an attack, restoring and disaster recovery, change and optimisation of system resources etc. in a truly elastic manner.

B. *Proposed Architecture*

An autonomic system should enable a SCADA system to optimise, configure and protect itself in case of changing system state. The SCADA system entities are generally spread over a large geographical area, thus necessitating synchronisation of information at each location. This necessitates an autonomic manager at each location that can monitor the security in the local areas and coordinate the efforts through the overall system manager.

A simplified architecture is shown in Figure 2. We propose hosting the SCADA system on a virtual platform. The advantages are that it can provide high availability through protection against hardware and software failures. At the heart of the system is a central autonomic manager that can enforce the broad hardware and software policies in the managed system as dictated by the system administrator. The knowledge base provides the various system models that can be analysed to check conformance. The local autonomic managers continually observe the system state and act promptly in case of identified security threats to the local system.

Some autonomic architectures have been proposed in the research literature. The IBM autonomic computing system comprises, monitoring, analysing, planning, executing and knowledge base component [30]. An architecture for an autonomic element as a smallest functional unit is proposed by Parashar and Hariri [20]. Chen and Abdelwahed [9] present an autonomic security model comprising of risk assessment, early warning and prevention, intrusion detection, and intrusion response. A detailed survey of autonomic computing models and applications is provided in [15]. A multi-tiered architecture [14] for QoS-aware autonomic cloud computing was suggested by Singh *et al*. The OPC (Open Platform Communications) forensics and analytics platform has been proposed by Amrein *et al.* which can be used with autonomic computing. HAMIDS system that can automatically detect threats from the network traffic has been proposed by Ghaeini et al. [31]. In contrast our proposed architecture provides a broad generalised structure based on virtualisation wherein appropriate technologies can be selected to best suit an application within the given framework. The identification of anomalies at an area level helps to counter the threats locally, relieving the central autonomic manager to take more holistic actions to counter system wide threats.

It is also pertinent to point out here that the autonomic manager itself can be the target of a cyber attack. Such exploitation can be avoided through redundant deployments of managers and an integrated approach as proposed.

VII. Conclusion

The evolving cyber threat landscape dictates changes to defence approaches. Unlike the traditional defence approaches where the response is governed by tailoring and monitoring according to threat, the concept of autonomic computing provides an advantage, as the systems are self-protecting.

Although the autonomic computing paradigm has been around for some time, its applications to real computer applications and SCADA applications in particular have been very limited. With the current pace of development and adoption of techniques ultimately the promise of a self-protecting SCADA system will be realised. With a fully developed autonomic computing system, the technology itself would take over the decision-making from the human system administrators and operators. Ultimately the technology will blend within the system [6] as has happened for mobile phones, hiding the technical details of communication from anywhere and anytime.

Acknowledgment

The research is sponsored by London South Bank University and Firstco Ltd., London, UK, through Innovate UK funding.

References

[1] A. Amrein, V. Angeletti, A. Beitler, M. Német, M. Reiser, S. Riccetti, M. Ph. Stoecklin and A. Wespi, "Security intelligence for industrial control systems," *IBM J. Res. & Dev.* vol. 60 no. 4, Jul 2016.

[2] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access Special Section on the Plethora of Research in Internet of Things (IoT),* 2016.

[3] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," In IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society, 2011, , pp. 4490-4494.

[4] L. Constantin, "New Havex malware variants target industrial control system and SCADA users," *PC World*, Jun 2014.

[5] W. Mahoney, and R. A. Gandhi, "An integrated framework for control system simulation and regulatory compliance monitoring," *Elsevier Intl. Journal of Critical Infrastructure Protection*, vol. 4, no. 1, Apr 2011, pp. 41-53..

[6] J. Kephart and D. Chess, "The vision of autonomic computing," Computer, 36(1):pp. 41-50, Jan 2003.

[7] A. G. Ganek and T. A. Corbi, "The dawning of the autonomic computing era,". IBM Systems Journal. 2003, vol. 42, 1.

[8] M. Greer and M. Rodriguez-Martinez, "Autonomic Computing Drives Innovation of Energy Smart Grids" Elsevier Procedia Computer Science 12 (2012) 314-319.

[9] Q. Chen, and S. Abdelwahed, "Towards realizing self-protecting SCADA systems" 9th Cyber and Information Security Research Conference, 2014.

[10] Autonomic Computing Lab. http://acl.ece.arizona.edu/research.html

[11] Cloud and Autonomic Computing Centre: https://sites.google.com/nsfcac.org/home

[12] JADE - A framework for developing autonomic administration software. Available online: http://raweb.inria.fr/rapportsactivite/RA2009/sardes/uid40.html

[13] D. P. Cox, "The application of autonomic computing for the protection of industial control systems," PhD thesis, University of Arizona, 2011.

[14] W. Alves, D. Martins, U. Bezerra and A. Klautau, "A Hybrid Approach for Big Data Outlier Detection from Electric Power SCADA System," *IEEE Latin America Transactions*, vol. 15, no. 1, Jan 2017.

[15] M. C. Huebscher and J. A. McCann, "A survey of autonomic computing-degrees, models and applications", ACM Comp. Surveys, Vol. 40, Issue 3, August 2008.

[16] Symantec report "What you need to know about the WannaCry ransomware," May 2017. Available online: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

[17] D. Ranathunga, Matthew Roughan, H. Nguyen, P. Kernick, and N. Falkner, "Case Studies of SCADA Firewall Configurations and the Implications for Best Practices," *IEEE Transactions on Ntwork and Service Management*, vol. 13, no. 4, Dec 2016.

[18] J. Jiang and L. Yasakethu, "Anomaly detection via one class SVM for protection of SCADA systems," *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (CyberC), 2013.

[19] S. Singh, I. Chana, and M. Singh, "The Journey of QoS-Aware Autonomic Cloud Computing, *IEEE IT Pro*, 2017.

[20] M. Parashar and S. Hariri, "Autonomic Computing: An Overview," in Unconventional Programming Paradigms. Ecture Notes in Computer Science, vol 3566. Springer, Berlin, Heidelberg.

[21] L. Yang, X. Cao, X Gen, and J. Zhang, "A Knowledge expression method of SCADA network attack and defence based on factor state space," Journal of Theoretical and Applied Information Technology, 31 Dec 2012, vol. 46, no. 2, 2005.

[22] M. Crawford, "Utility hack led to security overhaul," Computerworld, 2006, pp.1-2.

[23] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSIT* , Mar 2013.

[24] D. Hadžiosmanović, D. Bolzoni, P.H. Hartel, "A Log Mining Approach for Process Monitoring in SCADA", *Int. Jour. of Information Security*, vol. 11, no. 4, pp. 231-251, 2012.

[25] Y. Wang, Y. Wang, S. Patel,and D. Patel, "A layered reference model of the brain (LRMB),". *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2006, 36(2)*, pp.124-133.

[26] Y. Wang and Y. Wang,"Cognitive informatics models of the brain" *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2006, 36(2)*, pp.203-207.

[27] SQL The Next Big Thing in SCADA, White Paper, Inductive Automation, 2012. Available online: https://www.automation.com/pdf_articles/inductive_automation/WhitePaper_SQL_The_Next_Big_Thing_in_SCADA.pdf

[28] J. Kirsch, S. Goose, Y. Amir, D. Wei, and P. Skare, "Survivable SCADA via intrusion-tolerant replication," *IEEE Trans. on Smart Grid*, vol. 5, no. 1, Jan 2014, pp. 60-70.

[29] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, May 2011.

[30] IBM. Autonomic Computing. Available online: ftp://public.dhe.ibm.com/systems/z/z_coursematerials/lscc/08_Autonomic_computing.ppt

[31] H. R. Ghaeini and N. O. Tippenhauer, "HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems," *in Proceedings of Workshop on Cyber-Physical Systems Security & Privacy* (SPC-CPS), 2016, Austria.