International Journal of Multimedia and Ubiquitous Engineering
Vol. 9, No. 11 (2014), pp. 75-84
http://dx.doi.org/10.14257/ijmue.2014.9.11.08

On Autonomic Self Healing Architecture for Resiliency in Cyber Physical System

Lokesh. M. R[1] and Y.S. Kumaraswamy[2]

[1]Department of Computer Science and Engineering, Sathyabama University, Chennai, India
[2]Department of MCA-VTU, Dayananda Sagar College of Engineering, Bangalore, India
[1]itlokeshmr@gmail.com, [2] yskldswamy@yahoo.co.in

Abstract

Disturbances to a system are inevitable. Resilience is thus utmost necessary to the system as it has to respond to the stresses and disturbances to keep the system stable. Cyber physical systems are physical engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing communication core which is expected to transform the physical world around us. This paper proposes an autonomic self healing architecture for improving resiliency in cyber physical system using autonomic computing self management properties. This is a layered architecture in which each stage has a mechanism to collect state information of the system and monitor the system behavior, if the performance of the system is degraded in comparison to the normal level, self healing module is activated to facilitate recovery from damaged state and restoring to normal state, thereby achieving resilience in the system.

Keywords: *Resilient System; State Awareness; Self healing System; Cyber-Physical System*

1. Introduction

The US National Science Foundation's new Cyber engineering Research program [1] approaches the future Internet as a networked embedded control system, referred to as 'Cyber-(Physical) System'. A cyber-physical system integrates computing, communication and storage capabilities with the monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and most importantly at real-time. This shows the development of cyber physical systems hence requires multidisciplinary fields like control systems, communication networks, sensors and actuators network to monitor and control entities in the real time physical world.

The real time world has diverse engineering applications spread across various domains like intelligent transportation systems (air and ground), smart power grids, structural monitoring and control of civil infrastructures such as bridges and dams; medical/healthcare systems (for assisted living, patient monitoring in hospitals, automated laboratories); smart spaces (buildings with surveillance and microclimate control); smart agriculture; flexible manufacturing systems (with self assembling structures); systems and processes used in defenses, homeland security and emergency response (ad hoc ground/airborne combat teams, intelligent firefighting, *etc.*)[2].

ISSN: 1975-0080 IJMUE

Cyber system basically evolves as a feedback control loop for the real-time physical world. Hence, it forms a critical infrastructure. In today's world networks can be categorized into three types based on the criticality of infrastructure, namely:

- Supply networks: transportation grids for electrical power, oil and gas; water distribution networks; transport/road tunnel systems; production flow supply chains; health care Systems.
- Cyber-networks: tele-control and SCADA (Supervisory Control and Data Acquisition) networks, e-banking/finance networks, *etc*.
- Managerial/organization networks where human resources supervise and/or utilize the services delivered by the above systems.

Given the fact that Cyber Physical Systems (CPS) are real time, criticality issues have to be taken care in order to make the systems more dependable, safe, secure, and efficient. This can however be achieved by targeting to non functional properties such as Reliability, Sustainability, Robustness and Resilience. Hence, the proposed architecture is designed to improve resilience in cyber physical Infrastructure, to ensure system dependability, safety, security, efficiency.

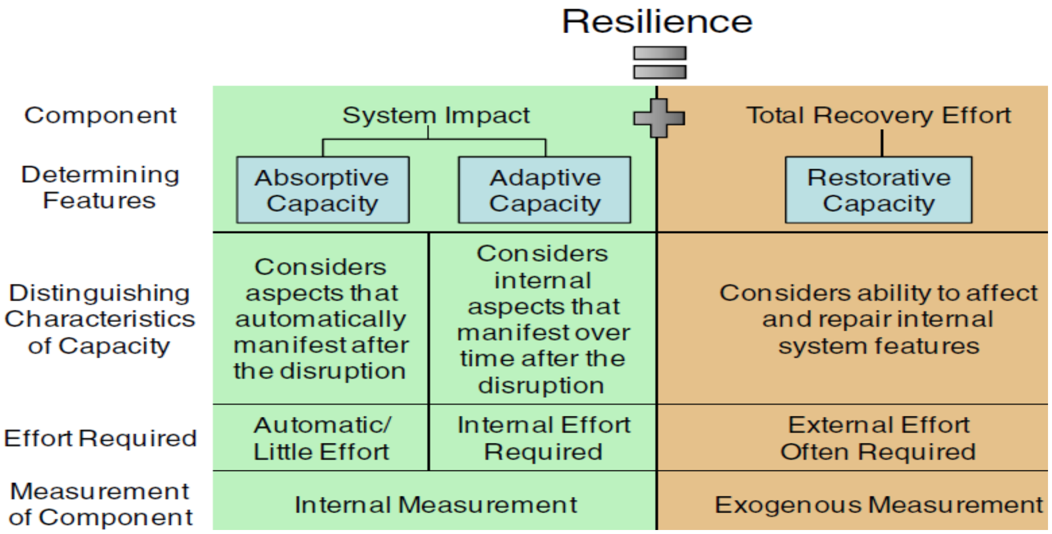
A CPS system requires improvement in the resilience, which can be achieved by following steps:

- Early warning and far-field detection of potential anomalies of the operational characteristics (*e.g.*, stability, livens, and performance) of the cyber-physical system;
- Fine-grained problem determination and containment within a CPS in order to quickly isolate the anomalies once they occur and ensure the problem area will be localized.
- Fast recovery of operational capabilities of a CPS from an incident to minimize the potential sustaining impacts.

Resilience is the virtue of a system which has the capability to withstand and recover back quickly from both known and unknown threats. Resilience refers to the maintenance of the system by creating awareness to handle unexpected threats and taking the right actions to handle them ensuring normal operation as fast as possible. Resilience has its roots from varies fields such as psychology, ecology and organizational behavior. This concept can be applied in various branches of engineering, namely aviation, nuclear power, oil and gas, transportation, emergency health care, and communication networks.

In any real time system, resilience can however be studied based on system capacities to formulate the resilience of the inherent properties of a system, specifically by reducing system impact and total recovery effort. The system capacities can hence be measured as absorptive capacity, adaptive capacity, and restorative capacity. These capacities are affected by resilience enhancement features, which refer to features of the system that can increase one or more system capacities [3].

Figure 1 depicts system impact and total recovery effort. System impact is achieved by proposing state awareness in each layer of the cyber physical system and the recovery is achieved by proposing self healing approach through this paper. This motivates us to propose State Awareness as an inner loop at component level and self healing module as an outer loop at the structural level.



Component	System Impact		Total Recovery Effort
Determining Features	Absorptive Capacity	Adaptive Capacity	Restorative Capacity
Distinguishing Characteristics of Capacity	Considers aspects that automatically manifest after the disruption	Considers internal aspects that manifest over time after the disruption	Considers ability to affect and repair internal system features
Effort Required	Automatic/ Little Effort	Internal Effort Required	External Effort Often Required
Measurement of Component	Internal Measurement		Exogenous Measurement

Figure 1. Resilience Capacities of a System [3]

Quanyan Zhu[4] developed Hybrid distributed reinforcement learning algorithms for defense systems with different levels of rationality and intelligence at different times and Games in- games frameworks are proposed for system-wide modeling of complex hierarchical systems, where games played at different levels interact through their outcomes, action spaces, and costs. Mohamed Mahmoud Mahmoud Azab [5]building a large scale, intrinsically resilient, self- and situation- aware, cooperative, and autonomous defense cloud-like platform that provisions adequate, prompt, and pervasive defense services for large-scale, heterogeneously-composed CPS. Ilsun Hong [6] proposed approach allows developers to implement autonomic CPS more systematically and validate through Home Surveillance Robot scenario. Andrew Jones [7] suggests an autonomic management system that enables an infrastructure to assess its real-time working environment and dynamically adjust its configuration for maximal resilience of the infrastructures composite parts. This existing work on resilience motivates this paper.

Tan Ying proposed prototype architecture of CPS [8] [9], but it lacks a comprehensive and deep description of the layers. Phan and Lee presented an approach towards a compositional multimodal framework of CPS [10], but composition analysis has been limited to uniprocessor processing elements and EDF/FP scheduling policies. Koubaa and Andersson provided a realistic vision to the concept of the Cyber physical Internet [11], but it does not solve the problem of real time for CPS. T. Erl provided a service-oriented architecture [12] of CPS, in which software and hardware of CPS are designed and developed in the form of interoperable services. This paper motivates to propose our layer approach for component and structural resiliency architecture for cyber physical system.

Part 1 gives broad introduction to cyber physical system and the requirement resilience in cyber physical system as well as Information technology resilience parameter with strong literature survey, Part 2 gives Autonomic Self Healing Architecture for Resiliency in Cyber Physical System along with state Awareness and self healing module. Part 3 Factors Affect on System Performance in Cyber physical system 4 conclusion and further work.

2. Proposed System Architecture

This architecture describes the formation of cyber-physical system along with improving resilience with self-healing approach. The architecture is represented in modular fashion, consisting of physical world integrated with cyber world with Monitoring and Actuation Infrastructure, Network Communication Infrastructure, and Distributed Centralized or Decentralized Control and Computation Infrastructure.

2.1 Proposed Layered Cyber-Physical Architecture

It is an integration of physical process system and cyber feedback loop along with state awareness and self healing to achieve resilience using autonomic management properties.

2.1.1. Physical Process System

The Physical entity refers to the mechanical, chemical, electronic elements of a system which are interconnected to perform a particular operation. Examples of this system are energy systems, power systems, nuclear power plants etc. Here resilience of such systems is achieved through improving features such as robustness and reliability.

2.1.2 Cyber feedback loop control system

The cyber world has various elements to monitor and control the physical process of the system. Depending on the functionality of the element, we propose, layered approach to distinguish the elements as follows with wide applications from health care to smart grid; each application uses it’s know sensing types and its network.

2.1.2.1 Monitoring and Actuation Infrastructure layer: This layer observes the physical entity status and acts as an interface between the physical and cyber world. This is done by various types of sensors, actuators device and it is networked to each other. As we know that cyber physical system having ECG, EMG, EEG, SpO2, accelerometer, & tilt sensors, ECG & PPG ,Video camera, audio, RFID, & smart, door lock Light, smoke, & temperature sensors, heat flux, gas(O2, CO,&CO2), GPS, accelerometer, magnetometer, Camera WiFi, and compass are some of the different types of sensors used in various application like medical application, electronics application, transport application, smart grids application , and game applications.

2.1.2.2 Network Communication Infrastructure Layer: This layer forwards the status information to Distributed Control and Computation Unit infrastructure. Based on the type of the application, Network communication infrastructure uses various technologies like switch, router and gateway with corresponding protocols. Body Sensor Network, GPRS, GSM, Wireless sensor Network, 3G, Bluetooth, WiFi Cellular and Internet are the different types of communication network are used between “Monitoring and Actuation” and “Control and Computation Unit” for different application.

2.1.2.3 Distributed control and computation Unit Infrastructure Layer: This layer is also called as Supervisory layer that offers human-machine interactions and capability of centralized decision-making. Doctors and nurses, data acquisition and storage component, agent-based command-control component, query manager agent and a set of Command, Control, Communication and Intelligence (C3I) user-interface agents to interact with users, an intelligent traffic signal control protocol to speed up car-crossing at intersections and smart user's phone are used as a control and computation unit in various applications.

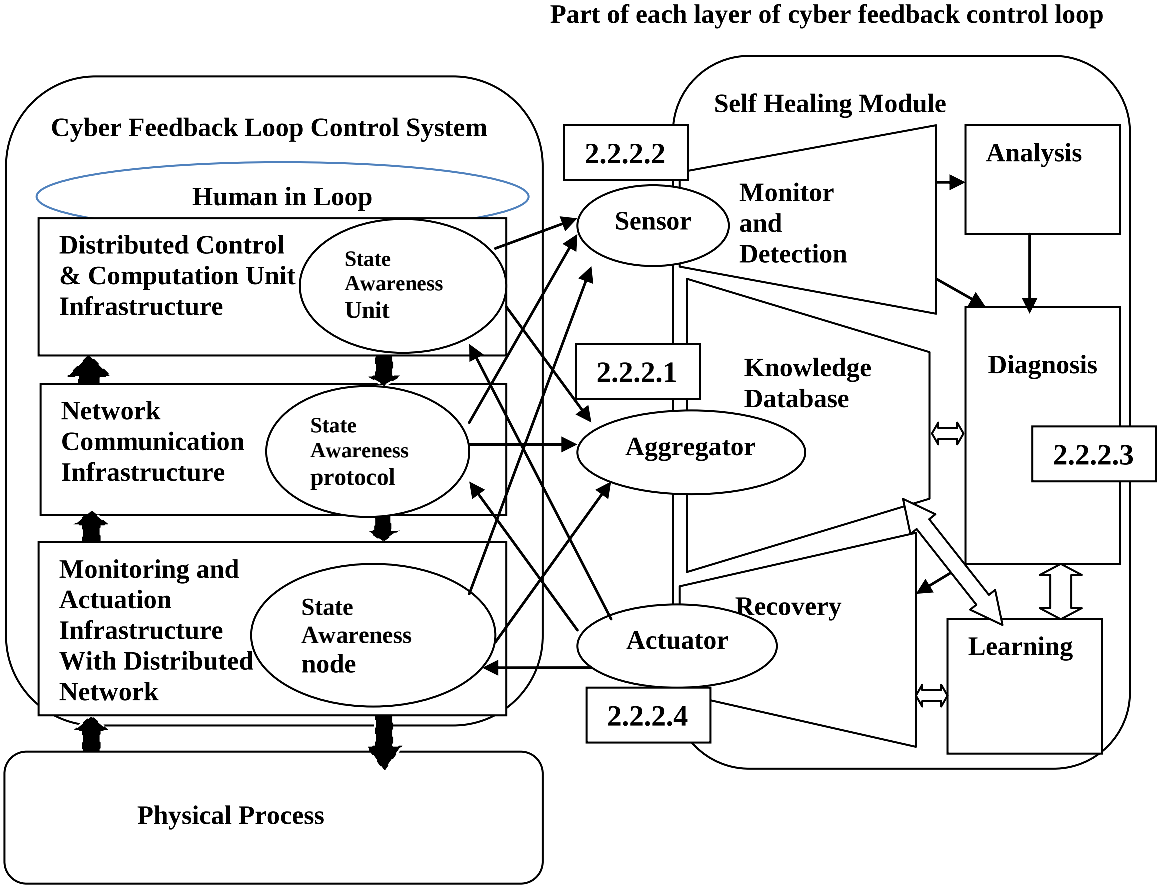

Part of each layer of cyber feedback control loop
Cyber Feedback Loop Control System
Human in Loop
Distributed Control & Computation Unit Infrastructure
State Awareness Unit
Network Communication Infrastructure
State Awareness protocol
Monitoring and Actuation Infrastructure With Distributed Network
State Awareness node
Physical Process
Self Healing Module
2.2.2.2
Sensor
Monitor and Detection
Analysis
2.2.2.1
Knowledge Database
Diagnosis
Aggregator
2.2.2.3
Recovery
Actuator
Learning
2.2.2.4

Figure 2. Autonomic Self Healing Architecture for Resiliency in Cyber Physical

2.2. Proposed State Awareness and Self healing Module

The State Awareness in each module along with Autonomic computing and self healing is proposed to improve resiliency in cyber physical system.

2.2.1. State Awareness Module

Existing approaches to gain cyber situation-awareness consist of vulnerability analysis (using attack graphs), intrusion detection and alert correlation, attack trend analysis, causality analysis and forensics (*e.g.*, backtracking intrusions), taint and information flow analysis, damage assessment (using dependency graphs), and intrusion response. These approaches however only work at the lower (abstraction) levels. Higher level situation-awareness analyses are still done manually by a human analyst, which makes it labor-intensive, time consuming, and error-prone [13]. A direct measurement of system state is often unavailable in control theory, and when this occurs, an observer or state estimator is often used. The state estimator is based on a model of the system and uses a combination of existing data and the model to estimate the current state and determine the desired state [14]. By this statement we are proposing our module and it is an inner loop in each layer of cyber physical system. It follows the following procedure to recognize system degradation performance before affecting the performance of the whole system.

1. Modeling behavior of the node through online and stores operational parameter to knowledge Database. This is in the self healing module.
2. Acts as an Intrusion Detection Node, if any change in the behavior of node which may degrade the system performance, then it is intimated to Monitoring and Detection module of self healing, for recovery and restoration action.
3. Acts as a Reconfigure node, after the corresponding action taken by the self healing module.
4. Acts as a standby node till the State of the system becomes stable.

2.2.2 Self Healing Module

Self healing module is a software module which is used to mitigate faults in the Infrastructure of cyber feedback control loop. It acts as outer loop in the system. It automatically detects diagnoses and repairs localized software and solve hardware issues. The system fixes faults through patch generation that automatically recover from faults.

Self-healing feature enables software systems to continuously and dynamically monitor, diagnose, and adapt themselves after a failure has occurred in their components. [15] Divides the self healing mechanism into three groups as 1) Internal adaptation mechanism, 2) Model-based mechanism and 3) Log-based mechanism and proposed Common Base Event (CBE).According the requirement of application one of the above mechanism is selected and following methodology is used to recover from faults.

2.1.2.1 Knowledge Database: In this module, generic fault model is stored. Fault model determines response strategy based on Fault duration, Fault manifestation, Fault source, Granularity, Fault profile expectations. All the operational parameters of the infrastructure component are stored in the knowledge database at deployment stage.

2.1.2.2 Monitor and detection: This module takes input from state awareness in each infrastructure and identify source/spot of faults which may occur in "Monitor", "Network communication" or "Control and Computation Unit" by using monitor methods like different granularities like Internal to the component (Self-checking software[16]), Supervisory checks (Recovery blocks [17]), Comparisons with replicated comoponents(Nversion[18]),andInstrumentation(Garlan[19],Debusmann[20],Valetto[21]) methods and detect corresponding fault using detection methods like Different levels of intrusiveness of detection [16] like Non-intrusive checking of results, Execution of audit/check tasks, Redundant task execution, Online self-tests/periodic reboots for self-tests and Fault injection methods.

2.1.2.3 Analysis and Diagnosis: This module is used for problem detection and to identify solution using knowledge database. Analysis block, analyzes the fault using Data correlation and inference technologies to support automated continuous system analysis over monitoring data [22] method and another method with reference points which use models and/or knowledge repositories to determine whether a problem exists or not. Diagnosis block diagnose the Fault by locating source of a fault after detection *e.g.,* Decision trees [23] Improve adaptation strategy selection methods.

2.1.2.4 Learning and Recovery: In this module the process of learning is done, along with diagnosis module. Recovery block recover the fault using methods like Degradation e.g. killing less important tasks (Koopman [24, 25]), Repair Adaptations (Dynamic updates [26], Reconfigurations [27, 28, 29, 30]), Roll forward with compensation (System-level undo [31]), Functional alternatives [20] and Requesting help from the outside (Philip Koopman [32]) methods.

3. Factors Affecting the System Performance in Cyber Physical System

As per the definition of "Resilient Control Systems (RCS), it is defined as a control system that maintains state awareness and accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature [14]. In the proposed concept in this paper it has to identify operational parameter when infrastructural component is deployed.

3.1. Human in loop: Human plays major role in giving higher level policies to efficient utilization of the application. More delay on response time occurs due to human error as well as lack of knowledge of using technology.

3.2. Control and Computation unit: Applications like mobile Operating System, supporting application in the mobile like Google map activation, proper browser applications, proper google account are complex in nature. Control and computation unit are distributed and delay will be due to computational capabilities, interconnection, overloaded etc example are smart Phones or cloud computing.

3.3. Network Communication: Various types and topology of network as well as components used in the applications like switch, router, and gateways and its corresponding protocol has to be aware and connected with each other for seamless communication.

3.4. Monitoring and Actuation: The main monitoring is performed through wireless sensor network, so constrains like battery, memory and data validity has to be considered.

To overcome the entire situation state awareness and healing module is used to improve resiliency. To the best of our knowledge, the proposal of self healing architecture to improve the resiliency through state awareness and self healing system is novel and first of its kind.

4. Conclusion & Further Work

We proposed an autonomic self healing architecture for resiliency in cyber physical system. We listed corresponding steps and methods available in the literature for state awareness and autonomic self healing to achieve resiliency in cyber physical system. Efforts are made to utilize them in the proposed architecture. Additional technical details, including a prototype implementation would be covered in the subsequent papers.

References

[1] NSF Workshop on Cyber-Physical Systems, Austin, Texas, October 16-17 **(2006)** (http://varma.ece.cmu.edu/cps/CFP.htm).

[2] G. Denker, N. Dutt, S. Mehrotra, M.-O. Stehr, C. Talcott and N. Venkatasubramanian, "Resilient dependable cyber-physical systems: a middleware perspective", Journal of Internet Services and Applications, vol. 3, no. 1, **(2012)** May, pp 41-49.

[3] E. D. Vugrin, D. E. Warren and M. A. Ehlen, "Infrastructure and Economic Systems Analysis Department", Sandia National Laboratories, Albuquerque, New Mexico, USA, **(2011)**.

[4] Q. Zhu, "Game-Theoretic Methods for Security and Resilience in Cyber-Physical Systems", PhD thesis **(2013)**.

[5] M. Mahmoud Mahmoud Azab, "Cooperative Autonomous Resilient Defense Platform for Cyber-Physical Systems", PhD thesis, **(2013)** January.

[6] I. Hong, H. Youn, I. Chun and E. Lee, "Autonomic Computing Framework for Cyber-Physical Systems", Proc. of Int. Conf. on Advances in Computing, Control, and Telecommunication Technologies, **(2011)**.

[7] A. Jones, M. Merabti and M. Randles "Resilience Framework for Critical Infrastructure Using Autonomics", International Journal of computer Applications, **(2012)**.

[8] Y. Tan, S. Goddard and L. C. Perez, "A prototype architecture for cyber-physical systems", ACM SIGBED Review, vol. 5, no. 1, **(2008)**, pp. 56–60.

[9] Y. Tan, M. C. Vuran and S. Goddard, "Spatio-Temporal Event Model for Cyber-Physical Systems", 29th IEEE International Conference on Distributed Computing Systems Workshops **(2009)**

[10] L. T. X. Phan and I. Lee, "Towards a compositional multimodal framework for adaptive cyber-physical systems," in Proceedings of the 17th International Conference on Embedded and Real-Time Computing Systems and Applications, , Toyama, Japan, **(2011)**. pp. 67–73.

[11] A. Koubaa and B. Andersson, "A vision of cyber-physical internet", Proceedings of the 8th International Workshop on Real-Time Networks, Porto, Portugal, **(2009)**, pp. 75–80.

[12] T. Erl, "Service-Oriented Architecture: Concepts, Technology, and Design", Prentice Hall PTR, Upper Saddle River, NJ, USA, **(2005)**.

[13] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin and S. Jajodia, Cyber SA: "Situational awareness for cyber defense. Cyber Situational Awareness", Advances in Information Security, vol. 46, **(2010)**, pp. 3–13.

[14] C. Rieger, Q. Zhu and T. Baszar, "Agent-based Cyber Control Strategy Design for Resilient Control Systems: Concepts, Architecture and Methodologies", 5th International Symposium on Resilient Control Systems, **(2012)** August.

[15] Park and Jeongmin, "Self-healing mechanism for reliable computing", International Journal of Multimedia and Ubiquitous Engineering, vol. 3, no. 1, **(2008)**.

[16] S. S. Yau and R. C. Cheung, "Design of Self-Checking Software", ACM SIGPLAN Notices - International Conference on Reliable Software, vol. 10, no. 6, **(1975)** June.

[17] B. Randell "System Structure for Software Fault Tolerance", Proceedings of the international conference on Reliable software, **(1975)**, pp 437–449.

[18] A. Avizienis, Fellow, IEEE, "The N-Version Approach to Fault-Tolerant Software", IEEE Transactions on Software Engineering, vol. SE-11, no. 12, **(1985)** December.

[19] B. Schmerl and D. Garlan, "Exploiting Architectural Design Knowledge to Support Self-Repairing Systems", Proceedings of the 14th international conference on Software engineering and knowledge engineering, **(2002)**, pp. 241–248.

[20] M. Debusmann and Kurt Geihs "Efficient and transparent Instrumentation of Application Components using an Aspect-oriented Approach", 14th IFIP/IEEE Workshop on Distributed Systems: Operations and Management, **(2003)**, pp. 209-220.

[21] G. Valetto and G. Kaiser, "Using Process Technology to Control and Coordinate Software Adaptation", International Conference on Software Engineering archive Proceedings of the 25th international conference on Software engineering Portland, Oregon, **(2003)**, pp. 262–272.

[22] L. Stojanovic, J. Schneider, A. Maedche, S. Libischer, R. Studer, Th. Lumpp, A. Abecker, G. Breiter and J. Dinger, "The role of ontologies in autonomic computing systems", IBM Systems Journal, Unstructured Information Management, vol. 43, no. 3, **(2004)**.

[23] M. Chen, A. X. Zheng, J. Lloyd, M. I. Jordan and E. A. Brewer, "Failure Diagnosis using Decision Trees", 1st International Conference on Autonomic Computing (ICAC 2004), New York, NY, USA, **(2004)** May 17-19, pp. 36-43.

[24] P. Koopman, "Elements of the Self-Healing Problem Space", ICSE Workshop on Architecting Dependable Systems, (**2004)**.

[25] C. Shelton and P. Koopman, "Using Architectural Properties to Model and Measure System-Wide Graceful Degradation", Accepted to the Workshop on Architecting Dependable Systems sponsored by the International Conference on Software Engineering, **(2002)**.

[26] M. W. Hicks, J. T. Moore and S. Nettles, "Dynamic Software Updating", Proceedings of the 2001 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), Snowbird, Utah, USA, **(2001)** June 20-22.

[27] R. S. Fabry, "How to Design a System in which Modules can be changed on the fly", International Conference on Software Engineering, **(1976)**.

[28] Mark E. Segal and Ophir Frieder, “On-The-Fly Program Modification: Systems For Dynamic Updating” IEEE Software, vol. 10, no. 2, **(1993)** March, pp 53-65.

[29] B. Rosenburg Ostrowski and J. Xenidis, “System Support for Online Reconfiguration”, Proceedings of the Usenix Technical Conference, San Antonio, TX, USA, **(2003)** June.

[30] S. B. Zdonik, “Maintaining Consistency in a Database with Changing Types”, Proceedings of the 1986 SIGPLAN workshop on Object-oriented programming Yorktown Heights, New York, United States, **(1986)**, pp. 120-127.

[31] A. Brown and D. A. Patterson. “Rewind, Repair, Replay: Three R's to Dependability”, 10th ACM SIGOPS European Workshop, **(2002)**.

[32] C. P. Shelton and P. Koopman, “Improving System Dependability with Functional”, Alternatives Proceedings of the **(2004)** International Conference on Dependable Systems and Networks (DSN'04) - Volume 00 Page: 295.

Authors

Lokesh M.R, received B.E degree in Electronics and Communication from Mysore University, India in 2001, M.Tech degree in Information Technology from Visvesvaraya Technological University (VTU), India in 2007. He currently research scholar in Computer Science and Engineering, Sathyabama University, Tamil Nadu, India. His has 13 year of teaching experience. His research include, Cyber-Physical System, Resiliency, Autonomic Computing, Self healing Methods and has also guided more than 30 projects in Computer Network, Wireless Sensor Network and Embedded System.

Dr. Y. S. Kumaraswamy, working presently as Sr.Professor and Head, Department of MCA (VTU) at Dayananda Sagar of College of Engineering, Bangalore. He has published more than 150 Research paper and guided 41 PhD students in the area of computer Science domain like Computer Network, Embedded System and also a selection committee member for ISRO/UGC/DSI profiles.