Cyber-Physical Systems Security: To Improve Independent Computing Capabilities of reliable Platforms and Tools

P.SalmanRaju[1]
Dr. M. Rama Bai[2]
T. Ashok[3]

1. Research Associate, Dept. of IT, Institute of Public Enterprise, Hyderabad.
2. Professor & HoD, Dept. of CSE, Mahatma Gandhi Institute of Technology, Hyderabad.
3. Asst.Professor, Dept. of CS, Adikavi Nannaya University, Rajahmundry.

Abstract:

In recent years, Cyber-Physical Systems has appear from conventional engineered systems in the areas of healthcare, aerospace, power and energy, automotive, entertainment, civil infrastructure, chemical process, transportation and power and energy. By introducing extensive transmission support in those systems, they have become more flexible in performance and response. In general, these CPS are also operation-expository: their availability and correct operation is essential. The **s**cope of this paper is to develop Independent system with novel health organization techniques for Reliable Platforms and Tools. It enables independent identification and re-designs when hardware or software fails to work as expected. In this paper outcomes are improved for intellect-identification, intellect-design and intellect-organization capabilities of Reliable Platforms and Tools.

Key Words: Intellect-Identification, Intellect-Design and Intellect-Organization, Independent Computing, Reliable and diagnosis.

1. Introduction

Cyber-physical systems (CPS) can be described as smart systems that encompass computational (i.e., hardware and software) and closely interacting with physical components, seamlessly integrated to sense the changing state of the real world. These systems involve a high at numerous spatial and temporal scales and highly networked communications integrating computational and physical components. Cyber-physical systems are enabling a new generation of 'good systems' – and the economic impacts could be enormous. The disruptive technologies emerging from combining the cyber and physical worlds could provide an innovation engine for industries, creating entirely new markets and platforms for growth. New products and services will bring the creation and retention of India jobs. The nation will also benefit through greater energy and national security, improved India. IT has become extensive in every way—from our phones and other small devices to our enterprise networks to the infrastructure that runs our economy. Cyber security standards are security quality which enables organizations to practice safe security techniques to minimization. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain degree, **cyber security certification** by an accredited body can be obtained. Cyber security depends on the institution, and there have been variation on older documents [1]. However, since the U.S. Federal Executive Order (EO) 13636 on the subject was spelled.

The history of Cyber security standards have been created recently because sensitive information now frequently stored on computers that are attached to the network. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security. A number of reports have focused on the importance of CPS and the need to pursue R&D that will establish U.S. leadership in the field and enhance competitiveness in global markets (PCAST 2012, PCAST 2011; PCAST 2010, NITRD 2009). Improving public health and safety is also a national priority where CPS can have a significant impact. The European Union is already investing $343 million per year for 10 years to pursue "world research and technology development related to CPS (include $199 million per year in public funds and $144 million year in private funds) (EU 2012). Cyber-physical systems are quickly becoming critical to the business success of many companies and the mission success of many government agencies.

In this way we studying and implementing some applications of CPS security for reliable independent systems. These are included in next section.

1.1. Applications of CPS

Manufacturing: Intelligent manufacturing equipment, processes, computerization, control, and networks; new product configuration.
Transportation: Intelligent vehicles and traffic control, intelligent structures and more.
Infrastructure: Intelligent utility smart and grid buildings/ structures.
Health Care: Body area networks and usable systems.
Emergency Response: Observation and extensive systems, transmission networks, and crisis response equipment.
Defense: Persist equipment systems, weapons systems, and engineering. In spite of these applications having availability rates in the 99% range, these systems do occasionally fail. As such, every operating entity has back-up, call-out, and response plans to rapidly identify and address the rare application crashes.

In this paper we have been included scalable reliable systems and how can address problems of reliable systems in next section. Table 1 representing summary of reliable systems.

leadership" through advanced strategic

2. Scalable Reliable Systems: What is the problem being addressed?

Reliable is a multidimensional measure of the extent to which a system is likely to satisfy each of multiple aspects of each stated requirement for some desired combination of system security measurements as integrity, system availability and extensibility, data confidentiality, guaranteed real-time performance, accountability, acknowledgement, usability, and other critical needs.

Extensible is the ability to satisfy given requirements as systems, networks and systems of systems expand in functionality, capacity, complexity, and scope of reliable requirements security, reliability, survivability, and improved actual time performance.

Capability is the ability to create systems and applications with predictably. Acceptable behavior from components, sub systems, and other systems. To enhance extensibility in complex distributed applications that must be reliable, high assurance systems should be developed from a

Set of capable components and subsystems, each of which is itself suitably reliable, within a system architecture that inherently supports facile capability [2].

There are three important aspects: (a) to provide a sound basis for capability that can scale to the development of large and complex trustworthy systems; (b) to stimulate the development of the components, analysis tools, and test beds required for that effort; and (c) to ensure that reliability evaluations themselves can be composed.

TABLE 1. Summary of Scalable Reliable Systems

Creativity: Development of reliable systems of systems (RSoS) experiment; ensure that even very complex and large systems can be built with predictable extensibility and provable reliability, using well-understood capable architectures and well designed, soundly developed, assuredly reliable components.

Tests: Many systems are built out of unreliable legacy systems using inadequate structures, development practices, and tools. We need appropriate theory, metrics of reliability and scalability, sound capable architectures, synthesis and analysis tools, and reliable building blocks.

Objectives: Maintain tools and sound basics that can relate device to strategies, threats to systems to requirements, enabling simplistic development of capable RSoS systematically enhancing reliability (i.e., making them more reliable than their weakest components); documented RSoS developments, from specifications to framework to deployed systems.

DISCOVERIES

Challenge/Rating: Identify measures of Reliability, capability, and extensibility, and apply them to real systems.

Change technology: Publish capable methodologies for developing RSoS with mix-and-match components. Release open-source tools for creating, designing, and organizing RSoS. Release open-source capable, reliable components. Publish successful, well documented TSoS developments. Develop profitable business models for public-private RSoS development partnerships for critical applications, and pursue them in selected areas.

In general, these CPS are also operation-expository: their availability and correct operation is essential. The scope of this paper is to develop Independent system with novel health organization techniques for Reliable Platforms and Tools. In this connection we have been implemented techniques for reliable platforms of cyber physical security systems. And also covered ranges of platform (see in next section).

3. Reliable Healthcare Platform

The Healthcare reliable Platform is a platform based on the reliable Cloud Technology that allows people to share health data while guaranteeing security and privacy [3]. It provide services such as providing an applications to access the user's health data, allowing for user registration, and allowing end users to manage their data and to specify a privacy policy with fine-grained access control. In this way healthcare business services communicating with data sharing control and user data within the healthcare reliable platform environment. And also connect with communication source, monitoring source, security source, and people groups. It is useful to develop health management techniques in reliable independent systems. Figure 1 shows reliable health care platform. Within the healthcare reliable platforms, healthcare business services connecting user data through data sharing control module. It has been proper module of both business and user data modules to reliable healthcare platform. In this way applications are supporting to various processes within the environment. Mostly it can be providing security to new technologies of reliable healthcare systems

3.1 Ranges of Platform

3.1.1 Isolation strategies

Distributing healthcare data may be-come a serious isolation issue? With our platform solution, users are enabled to manage every detail of their data and have the ability to query the system and see who has had access to user's data and why.

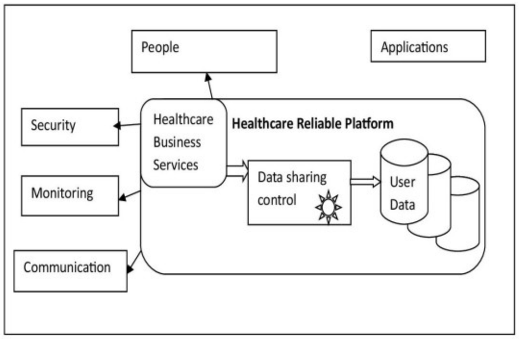


Fig. 1. Healthcare Reliable Platform connected with tools and apps

3.1.2 Reliable in-changed data

Combining applications and tools to PHR (Primary health record) data becomes easy with the Healthcare reliable Platform. Giving a doctor the permission to check your blood pressure trends or asking a friend to share his data is done in a reliable way since every single piece of data will be sent in an encrypted form to increase security of sensitive private data.

3.1.3 Legitimate submissions

PHR data can contain clinical i.e. Electronic Health Record (EHR) data. Although the patient is in full control, there are legal rules regarding handling this user has the ability to query the Log-as-a-Service functionality that provides a trusted overview of all the access to the data.

3.1.5 Reliability on Commodity Clouds

The Healthcare reliable Platform uses a resilient storage feature to store data on commodity clouds (unreliable by nature) in a secure way via fragmentation and encryption of the data.

3.1.6 Reliable Data Storage

Every activity of the Healthcare reliable Platform is encrypted, as well as every single piece of user‘s data. This ensures that no one (not even the cloud owner) can have access to and exploit the user‘s data. Share data.

In the next section, we have been improved and implemented Theoretical Model of Independent Evaluation System. And also improved characteristics of Independent Evaluation System.

4. Independent evaluation

Independent evaluation refers to the Intellect-organization characteristics of sharing evaluation resources, modify to uncertain changes while hiding inherent problem to operators and users [4]. Started by IBM in 2001, this initiative ultimately aims to develop computer systems capable of Intellect-organization, to overcome the quickly growing complication of evaluation, and to reduce the barrier that problem poses to further growth.

4.1 **Independent systems**

A possible solution could be to enable modern, networked computing systems to manage themselves without direct human intervention. The Independent Computing Initiative (ICI) aims at providing the data. For instance it may not be allowed to delete this data at any time.

3.1.4 Reliable Audits and Log

If a user thinks that an app, or another user, is misusing the data that the user gave access to, that

foundation for independent systems. It is inspired by the independent nervous system of the human body. This nervous system controls important bodily functions (e.g. respiration, heart rate, and blood pressure) without any conscious intervention.

In an Intellect-organization independent system, the human operator takes on a new role: instead of controlling the system directly, he/she defines general policies and rules that guide the self-management process. For this process, IBM defined the following four functional areas:

- *Intellect -Design:* Independent design of components;
- *Intellect -Mitigation*: independent discovery, and correction of faults [5];
- *Intellect -Development:* independent scanning and control of resources to ensure the optimal functioning with respect to the defined requirements;
- *Intellect -Preservation*: Proactive identification and protection from arbitrary attacks.

IBM defined five evolutionary levels, or the independent deployment model, for its deployment: Level 1 is the basic level that presents the current situation where systems are essentially managed manually. Levels 2 - 4 introduce increasingly independent organization functions, while level 5 represents the ultimate goal of autonomic, self-managing systems.

The design complexity of independent Systems can be simplified by utilizing design patterns such as the model view controller (MVC) pattern to improve concern separation by encapsulating functional concerns [6].

4.3 Theoretical Model of Independent Evaluation System

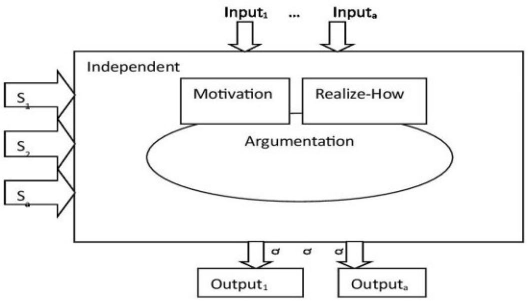


Fig. 2. Theoretical Model of independent system

A fundamental building block of an independent system is the sensing capability (*Sensors S_i*), which enables the system to observe its external operational context. Inherent to an independent system is the knowledge of the *motivation* (intention) and *realize-how* to operate itself (e.g., bootstrapping, design knowledge, explanation of sensory data, etc.) without external intervention.

4.4 Characteristics:

Even though the purpose and thus the behavior of independent systems vary from system to system, every independent system should be able to exhibit a minimum set of properties to achieve its purpose:

Independent

This is essentially means being able to restraint its internal functions and operations.

4.2 Restraint Curves

Basic concepts that will be applied in independent Systems are closed restraint curves. This well-known concept stems from Process Theory. Essentially, a closed restraint curves in a Intellect-Organizing system scanners some resource (software or hardware component) and independently tries to keep its parameters within a desired range.

Flexible

An independent system must be able to change its operation (i.e., its design, state and functions.

Aware

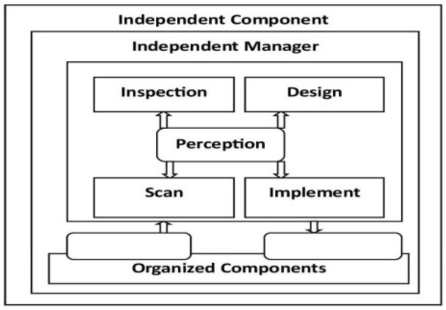
An independent system must be able to scan (sense) its operational context as well as its internal state in order to be able to assess if its current operation serves its purpose.

In this paper outcomes are improved for intellect-identification, intellect-design and intellect-organization capabilities of Reliable Platforms and Tools. In the next section, we have been Proposed System model of Independent Evaluation System. And also evaluated agent recognition, Terms of the record scanning Module, the Filtering & Translating Efficiency, and the mitigating Time.

5. Proposed System model of Independent Evaluation System

One of the fundamental components of IBM's vision of Independent Evaluation System is a reference model for independent restraint curves [7], which is usually referred to as the *proposed model* (scan, inspection, design, and implementation) adaptation curves, and depicted in Figure 3. IBM's vision of autonomic computing was influenced by agent theory, and the *proposed* model is similar to and was probably inspired by the generic model for intelligent agents proposed by Russell and Norvig [8]. In this way we have been implemented new Proposed System model of Independent Evaluation System.

Fig. 3. Proposed model of Independent Evaluation System



An independent system must be able to scan (sense) its operational context as well as its internal state in order to be able to assess if its current operation serves its purpose.

The data collected by sensors allows the autonomic manager to *scan* the execution of the managed element. For instance, we may be interested in monitoring such properties of deployed applications as CPU and memory utilization, response times to user requests, I/O operations frequency, up time, etc. Two types of monitoring are usually identified in the literature [7]:

- *Passive* monitoring, also known as *non-intrusive*, assumes that no changes are made to the managed element. This kind of monitoring is targeted at the context of the managed element, rather than the element itself.

- *Active* monitoring, also known as *intrusive*, entails designing and implementing software in such a way that it provides some entry-points for capturing required properties (e.g., APIs).

5.1 Recognition Agent (*Analysis and identification*):

The first major attribute of an intellect-mitigation system is self-identification [12]. The results of the diagnosis can be used to trigger independent reaction. Using the record service existing in the operating system, as shown in Table 2, it classifies the Error Event, and sets up the priorities. The results of the diagnosis recognize the situation level.

Fallacy Level	**Importance**
Crisis	1
Vigilance	2
Error	3
notify	4

TABLE 2. Rating of the Fallacy event

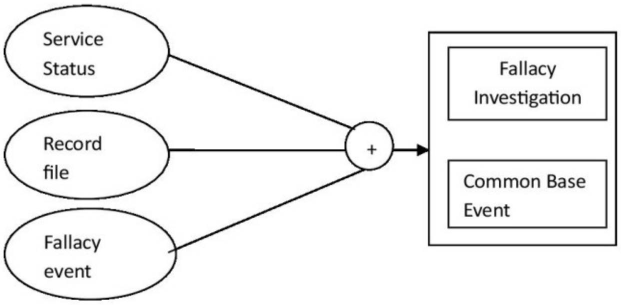


Fig. 4. Recognition Agent's behavior

As shown in Fig 4, the Diagnosis Agent generates the Error Report and modifies the CBE. The Error Report is an administrator document, and the common base event (CBE) is a document for the system. The following is the algorithm performed by the Recognition Agent Using the first-order logic; we can recognize the situation level of system and represent the policy for it. Figure 5 illustrates Factor Base and its example.

Factor Base
Find(MainObject, Object_Topology)
Condition(Error_Topology)
State(Resource Type,Usage)

MainObject: Windows, Unix, Linux, Oracle,…
Object_Topology: OS, DB,DBMS…
Error_Topology: Crisis, Elert, Error…

Example of Factor Base
Find(Linux, Oracle)
Condition(Crisis)
State(CPU,80)
State(RAM, 70)
State(Ma_Client, 70)

Find(Linux, Oracle)^ State(CPU,80) ^ State(RAM, 70
^ State(Ma_Client, 70)-> Condition(Crisis)
⇨ Code 1 (Oracle, Control Max_ClientNum)
⇨ Code 2 (Oracle, Kill NotUsedProcess)
⇨ Code 3 (Oracle, Restart)

Figure .5 Redesign of System level

5.2 Terms of the record scanning Module, the Filtering & Translating Efficiency, and the mitigating Time.

(a) *Record scan Test.* In the existing system, if the number of components is 1, the system has to have 1 process to monitor the record. In the proposed system, however, only one process is needed to scan the record, as shown in Figure 6.

(b) *Flow & move productivity Test.* In the system, the Component Agent searches for a designated keyword (such as “not”, “reject”, “fail”, “error”, etc.) in the log generated by the components. As a result of the filtering process, only about 20% of the logs were required for the healing process, as shown in Figure 6. Therefore, the proposed system reduces the number and size of the logs, which require conversion to the CBE format.

(c) *Mean Mitigate Time Computation***.** We measured the Mean Transformation Time arising in the existing intellect-mitigation system and the proposed intellect-mitigation system. And time arising in the existing resolving system and proposed resolving system and also time arising in existing scanning system and proposed scanning system. The detail evaluation was included below [13].

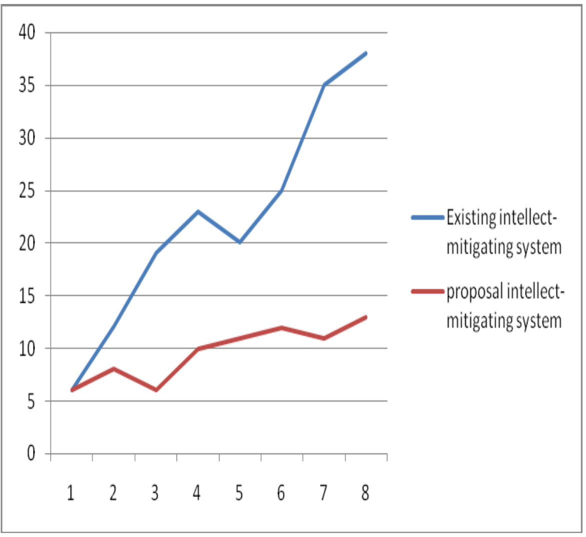


Fig. 6. Memory usage and similar of size and number of records

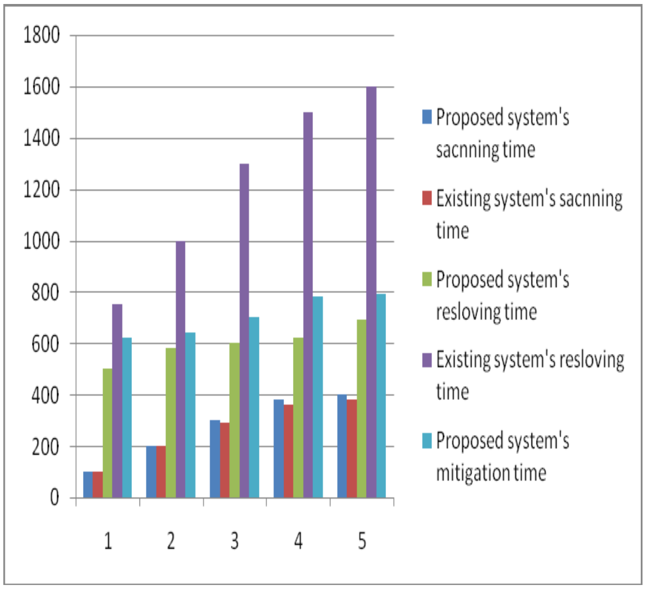


Fig. 7. Similarity of modification time

For each alteration time, as shown in Figure 7, we verified that the proposed systems resolving time and mitigating time are fastest than the existing systems, and rapidly responded problems arising in the urgent situation.

5. Conclusion

The performance of Independent Evaluation Capabilities of reliable Platforms and tools is improved by intellect-identification, intellect-design and intellect-organization capabilities using novel independent system health management techniques. This paper has described intellect-organization system for reliable system. The scanning layer consists of modules for scanning the information such as record context, resource, configuration parameters. In this paper we have presented a framework for introducing intellect-organization in Platform-as-a-Service environment. Devising this framework, we drew similarities between the problem domain of intellect-transformation in cloud platforms, and other problem domains where successful solutions have come from applying the Sensor Web technology, such as traffic supervision and environmental scanning.

References:

1. Department of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004).
2. [Can2001] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols (http://eprint.iacr.org/2000/067), 2005. An extended version of the paper from the 42nd Symposium on Foundations of Computer Science (FOCS'01) began a series of papers applying the notion of universal composability to cryptography. Much can be learned from this work regarding the more general problems of system composability.
3. http://tclouds.eservices4life.org:8080 and www.tclouds-project.eu
4. Padovitz, Amir; Arkady Zaslavsky; Seng W. Loke (2003). "Awareness and Agility for Autonomic Distributed Systems: Platform-Independent Publish-Subscribe Event-Based Communication for Mobile Agents". Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03): 669–673.
5. S-Cube Network. "Self-Healing System"
6. Curry, Edward; Grace, Paul (2008), "Flexible Self-Management Using the Model-View-Controller Pattern", IEEE Software 25(3):
   84, doi:10.1109/MS.2008.60
7. Huebscher, M.C. and McCann, J.A. 2008. A survey of autonomic computing—degrees, models, and applications. ACM Comput. Surv. 40, 3 (2008), 1–28.
8. Russell, S.J., Norvig, P., Canny, J.F., Malik, J.M. and Edwards, D.D. 1995. Artificial intelligence: a modern approach. Prentice hall Englewood Cliffs, NJ.
9. Hitzler, P., Krötzsch, M. and Rudolph, S. 2009. Foundations of Semantic Web Technologies. CRC Press.
10. Studer, R., Benjamins, V.R. and Fensel, D. 1998. Knowledge engineering: Principles and methods. Data & Knowledge Engineering. 25, 1–2 (Mar. 1998), 161–197.
11. Dautov, R., Paraskakis, I. and Kourtesis, D. 2012. An ontology-driven approach to self-management in cloud application platforms. Proceedings of the 7th South East European Doctoral Student Conference (DSC 2012) (Thessaloniki, Greece, 2012), 539–550.
12. B. Topol, D. Ogle, D. Pierson, J. Thoensen, J. Sweitzer, M. Chow, M. A. Hoffmann, P. Durham, R. Telford, S. Sheth, T. Studwell: Automating problem determination: A first step toward self-healing computing system, IBM white paper, October (2003)
13. Qianxiang Wang, Towards a Rule Model for Self-adaptive Software ACM SIGSOFT Software Engineering Notes Page 1 January 2005 Volume 30 Number 1 pp. 1-5.

ISSN: 2278 – 1323

Authors' Profile

Dr. M. Rama Bai received, her B.E degree from Bharathiar University, Coimbatore(T.N) and her M.Tech (CSE) from College of Engineering, Osmania University, Hyderabad. She received her Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University, Kakinada (JNTUK). She joined as Assistant Professor in the Dept of Computer Science & Engineering, Mahatma Gandhi Institute of Technology (MGIT) in 1999. At present she is working as Professor & HOD, Dept of IT, MGIT, Hyderabad, Telangana. Her research interests include Image Processing, Digital Water Marking, Information Security and Cyber Security. She has published 24 research publications in various National, International conferences, proceedings and Journals. She has a total teaching experience of 19 years. She is a life member of ISTE and CSI.

P.Salman Raju received his MCA degree from JNTU Hyderabad and his M.Tech (CSE) (pursuing) from JNTU Hyderabad. He joined as Faculty member in the department of computer science, Adikavi Nannaya University, Rajahmundry in 2010. At present he is working as Research Associate, Dept of IT, Institute of Public Enterprises, and Hyderabad. His research interests include Data Mining, Information Security and Cyber Security

T.Ashok received his M.Tech (CSE) degree from JNTU Kakinada. He joined as Faculty member in the department of computer science, Adikavi Nannaya University, Rajahmundry in 2010. At present he is working as Asst.Professor(Ad-hoc) , Dept of Computer Science. Adikavi Nannaya University, Rajahmundry

ISSN: 2278 – 1323